I+D+i, EN LA FUNCIÓN POLICIAL

PUBLICACIONES
DE LA FUNDACIÓN POLICÍA ESPAÑOLA
Colección Estudios de Seguridad

I+D+i, EN LA FUNCIÓN POLICIAL

PUBLICACIONES
DE LA FUNDACIÓN POLICÍA ESPAÑOLA
Colección Estudios de Seguridad

Con la colaboración de:

Obra Social "la Caixa"

CaixaBank

Edita: Fundación Policía Española
Conde de Aranda, 16, 3º Izq.
e-mail: info@fundacionpoliciaespañola.es
Coordinador Editorial:
Mario Hernández Lores
Equipo Editorial:
Mª Jesús LLorente Vega
Mª del Carmen Baz Crespo
David Blázquez Hernández
Imprime: Tecnología Gráfica
Diseño y Maquetación: Félix Gil
ISBN: 978-84-09-07664-2
Depósito legal: M-41354-2018

ÍNDICE

ÍNDICE

PRESENTACIÓN DEL CURSO

La idea de que "el mundo es cambiante y global" es una creencia instaurada y repetida frecuentemente; lo mismo ocurre con el pensamiento de que los cambios se producen cada vez más rápidamente. Cambio, globalidad y celeridad, bien administrados, pueden ser generadores de avances sociales que redunden en la mejora de la calidad de vida.

Por otro lado, siguiendo la analogía de que la conducción de un coche exige echar un vistazo al espejo retrovisor, pero sobre todo mirar hacia adelante, la buena gestión de este mundo cambiante debe tener en cuenta el pasado, pero sobre todo el futuro. Las mejores herramientas para ello son la investigación, el desarrollo y la innovación, el I+D+i.

Muchos retos de futuro están identificados a nivel europeo en el programa marco "Horizonte 2020" y a nivel nacional en el "Plan Estatal de Investigación Científica y Técnica y de Innovación 2017-2020"; de estos retos, muchos están relacionados con la seguridad. Algunas veces porque la innovación es necesaria para poder prestar seguridad (nuevas tecnologías, recursos logísticos, recursos humanos,...), otras porque sin seguridad no se podrían implementar las innovaciones globales (ciberseguridad, paz social, comercio seguro, movilidad, seguridad subjetiva,...).

Por ello, en este espacio de reflexión e intercambio que es la Universidad, diferentes especialistas de seguridad a nivel europeo, estatal, territorial y del sector privado, tomando como referencia la seguridad ciudadana, las fronteras, la seguridad judicial, la lucha contra el terrorismo, la ciencia forense, la logística, la movilidad... intentaremos analizar lo que se está haciendo y sobre todo lo que se puede hacer en el "ámbito de la seguridad" desde los postulados del "I+D+i."

Conferencia inaugural

MANUEL ÁLVAREZ JUNCO
Director de los Cursos El Escorial

Para mí es una satisfacción estar aquí, y les doy la bienvenida a este curso. Después de veinte años, esta es la vigésima edición, con lo cual ya es un absoluto clásico y un auténtico placer acoger un curso de esta importancia; además, en este caso y en este año, todo lo que es el I+D+i. Este curso es de una enorme importancia y siempre con alguna novedad, con alguna actualización de lo que es la problemática policial.

Les doy la bienvenida e intentaré asistir en alguno momento a ver si de alguna forma nutro un poco más mi conocimiento de la realidad en un tema tan fundamental como es la seguridad.

Así pues, que comience el curso.

MARIO HERNÁNDEZ LORES
Director Gerente de la Fundación Policía Española

Quiero dar las gracias a Manuel Álvarez Junco por habernos invitado una vez más a participar del mundo del saber, de este intercambio de conocimientos e inquietudes, que es la Universidad.

Como Director Gerente de la Fundación Policía Española, patrocinadora de estos cursos y al mismo tiempo como Director del curso, tengo una doble perspectiva y voy a empezar hablando como Director Gerente de la Fundación transmitiéndoles los saludos de D. Rafael del Río, Presidente de la Fundación. Rafael del Río es una institución en el Cuerpo Nacional de Policía, dado que es el único, actualmente, que ha sido al mismo tiempo Director General de la Policía y Comisario del Cuerpo Nacional de Policía. Es un representante de lo que es la Fundación, y que está compuesta por patronos que son todos antiguos Directores Generales de la Policía, antiguos Subdirectores o DAO que se han venido renovando y que posiblemente se vuelvan a renovar, como ha ocurrido últimamente, con la incorporación de un alto cargo del Cuerpo en activo, como es el propio José Manuel Pérez, que lleva poco más de un año de patrono. Esta es la Fundación Policía Española, una institución privada que tiene entre sus mayores objetivos dar apoyo a la trayectoria de la Policía, trayectoria que viene a ser la doctrina del sentir policial. Tiene como decía, entre sus patronos, a los Directores Generales de la Policía desde el año 1986; por ejemplo, Rafael del Río, Ignacio Cosidó… y nos imaginamos que en un lapso de tiempo no muy lejano se incorporará también D. Germán López Iglesias, el anterior Director del Cuerpo.

Como decía, esta es la Fundación y sus actividades. Yo les invitaría a que visitasen la página web de la Fundación en la que se van a encontrar con gran parte de las actividades que realiza. Impartimos cursos, entre los que destacan estos cursos de verano de El Escorial y el de Policía Científica en la Universidad Menéndez Pelayo. Se otorgan premios de novela policial,

también premiamos los valores humanos de los funcionarios del Cuerpo Nacional de Policía; se conceden becas de investigación para los funcionarios del Cuerpo que quieran incorporar nuevas ideas al acervo cultural y de gestión de la función policial; damos premios de investigación, abiertos a todas las universidades, premios de veinte mil euros para promover esto que llamamos I+D+i; premiamos asimismo producciones periodísticas que reflejan la actividad del CNP. Insisto, todas estas actividades se pueden ver en la página web oficial de la Fundación; y esto, lo voy a utilizar para enlazar con la segunda función que tengo, que es la de Director del curso.

La Fundación Policía Española lleva veinte años patrocinando los cursos de El Escorial; se han tocado temas muy variados. Empezamos en el año 1999, en aquel momento yo estaba en los inicios, dando apoyo como lo hacen hoy Mari Carmen, que es la secretaria de la actual edición, y María Jesús, que también colabora con nosotros, y que estarán en la gestión del libro que recogerá las ponencias que tendremos estos días; también está Alfonso que es el fotógrafo de la revista. A todos ellos podéis dirigiros para cualquier necesidad que tengáis. Por otro lado, y al hilo de lo que decíamos antes, quiero destacar que todas las ponencias que se han venido realizando durante estos veinte años están en formato PDF en la página web de la Fundación.

Os doy las gracias a todos por haber venido, a los ponentes que nos vais a ilustrar y a los compañeros, alumnos del Cuerpo Nacional de Policía, de Policía Municipal, de Guardia Civil, y a un número importante de personas que, sin ser policías, puedo decir que también son compañeros por la propia inquietud de estar aquí.

Otros años, por parte de la organización, se nos ha proporcionado un programa de mano. Este año, por responsabilidad ecológica, y porque al fin y al cabo es una innovación, se ha renunciado a los programas de mano en papel y se nos ha entregado una APP para poder consultar toda la dinámica de los cursos a través de los móviles; de esta forma, contribuimos a mantener un poco más la naturaleza.

Una vez expuestas estas cuestiones de organización, quisiera presentar lo que compete al curso. El curso de I+D+i en la Policía se debe a una cuestión: "la inquietud que ha tenido la Fundación de mirar siempre hacia adelante". Es importante tener noticias de lo que está sucediendo para saber dónde estamos, pero siempre mirando hacia adelante; con lo cual, dentro de esta vocación que tiene la Fundación de estar siempre dispuestos para los desafíos de futuro que se nos puedan producir y a los que tengamos que dar respuesta para los ciudadanos. Consideramos que estas reflexiones de lo que se nos viene encima en cinco o diez años para los profesionales de

este Cuerpo, van a ser importantes para tener una visión de cómo debemos prepararnos en un futuro.

La dinámica en la programación de las ponencias va a ser la siguiente: primero vamos a presentar una visión global de los conceptos tanto de innovación como de investigación. El desarrollo es evidente y a nivel teórico lo integraremos dentro de la función policial en la Unión Europea (Horizonte 2020) y también con las propias estructuras del Cuerpo Nacional de Policía que más responsabilizadas están en la materia. A continuación, pasaremos a presentar, conocer y reflexionar sobre aquellas organizaciones, dependencias, que conocemos nosotros -el Cuerpo Nacional de Policía- como son las grandes comisarías generales, o las grandes divisiones y sobre todo saber qué están haciendo en la materia. Continuaremos, también, con algún componente de carácter internacional; intentaremos ver algunos aspectos de organizaciones paralelas a nosotros, como Defensa o la propia Guardia Civil; y cerraremos el curso con un tema importante, las migraciones. Clausuraremos el curso con la presencia de la nueva Secretaria de Estado de Seguridad.

Quiero comentar que habrá algunos cambios y tendremos que actuar sobre la marcha, porque los momentos actuales en que estamos de cambios políticos nos han impedido que viniera el Director General de la Policía, como estaba previsto. Mañana tendremos que hacer algunos pequeños cambios en el orden de los ponentes; como bien sabéis, mañana es la presentación oficial del Director General de la Policía y dos altos cargos que tenían que estar como ponentes tienen que estar, como miembros de la Junta de Gobierno, en la presentación del Director.

Y creo que ya es hora de pasar a José Manuel Pérez Pérez, que va a ser el encargado de hacer la inauguración oficial.

JOSÉ MANUEL PÉREZ PÉREZ
Jefe del Gabinete Técnico de la Dirección General de la Policía

Buenos días, efectivamente, de los veinte cursos no he asistido a todos pero sí a unos cuantos. Tengo que empezar por disculpar la presencia del Ministro que hace dos meses no era el que es actualmente y que se había comprometido a inaugurar el curso. Lo ha explicado muy bien Mario, la situación es la que es y tanto el Ministro como la Secretaria de Estado están hoy en la línea de la Concepción con el problema que tenemos del narcotráfico.

Quería saludar a todos, Mario decía que erais el 85% de las Fuerzas y Cuerpos de Seguridad, yo no sé si tanto, pero sí que estáis aquí más del cincuenta por ciento porque os conozco, así que bienvenidos, quiere decir que estáis muy interesados en la formación y eso me alegra. De estas veinte ediciones en las que la Policía ha estado en los cursos de El Escorial se han tratado temas siempre candentes, siempre de actualidad: la trata de blancas, la seguridad en general, la Policía 3.0, la inmigración, el terrorismo…, pero todos los años procuramos que sea un tema candente, como lo es la investigación, el desarrollo y la innovación. Antes de continuar quiero agradecer por una parte a la Fundación Policía Española, aunque hoy los representantes somos Mario y yo, y muy especialmente a la Universidad Complutense, aquí representada por D. Manuel Álvarez Junco, Director de los cursos y que todos los años tiene la amabilidad de acompañarnos.

También tengo que agradecer a la Fundación La Caixa, a Caixabank y al Banco Santander, porque sin la financiación de ellos tampoco podríamos hacer estos cursos y, como habéis visto, este año se van a ir haciendo las ponencias y los capítulos del libro, porque es muy interesante tener en un libro todo lo que se ha tratado en el curso, independientemente de que esté colgado en la red.

También, agradezco a Luisa María Benvenuty Cabral, Comisaria Principal del CNP, Secretaria General de la Jefatura Central de Logística y que además tiene el tema de innovación en la ponencia, su presencia en estas jornadas porque su ponencia es precisamente la que indica el nombre del curso.

En el tema de formación, desde siempre, la Policía se ha caracterizado por estar abierta a la colaboración con los demás, con las universidades en concreto,y yo, ahora mismo, de memoria, no podría deciros la cantidad de convenios que, desde el gabinete, me ha tocado tramitar de todo tipo, desde los más sonados que son los de Policía Científica, hasta los de traducción e interpretación con la Universidad de Alcalá. Tenemos prácticas de criminología con muchas universidades incluida la Complutense; es decir, hay un afán por parte de la Policía de abrirse a la formación con cualquier institución, en este caso, lógicamente, con las universidades que serían las más representativas. Por eso, no solo serán veinte ediciones sino que entiendo que esto continuará hasta que haya por lo menos otras veinte.

La Policía Nacional es una organización abierta y, por lo tanto, tiene que estar en todos los temas, en la vanguardia de lo que se está produciendo en la sociedad. Actualmente, vemos que se producen los cambios a una gran velocidad, a veces, nos da hasta vértigo el pensarlo; y las organizaciones criminales siempre van un punto por delante, sea en los delitos, como he dicho antes, del narcotráfico en la Línea, donde vemos que tienen lanchas más rápidas que las nuestras; pero, sobre todo, en lo relacionado con la informática y la tecnología casi siempre van un paso por delante. Por eso, no nos queda más remedio que evolucionar y procurar avanzar al menos a la par que estas organizaciones criminales. Yo decía en un curso de inauguración hace dos, tres años, no recuerdo exactamente, en el que hablábamos de la delincuencia en general, que llegaría el momento en que no veríamos un atraco y muy difícil un hurto, porque no va a haber dinero físico. Desde el año 2011 hasta la actualidad, la delincuencia común, a pesar de la crisis económica -que fue sorpresa para nosotros-, ha ido descendiendo con carácter general, pero han ido aumentando todos los relacionados con Internet o la pornografía infantil, así como también los delitos económicos a través de la red. De ahí la importancia que tiene este curso.

Mario avanzó lo que era el programa del curso y que va a estar en esta mesa María Luisa, que es la representación mayor del cuerpo en materia de innovación, de la Jefatura Central; pero también vamos a tener conferenciantes que van a tocar temas desde otros puntos de vista, por ejemplo, de la Unión Europea en el Horizonte 2020, que es uno de los objetivos como lo es en nuestro plan estratégico 2017-2021; aunque ahora, por la situación

en que estamos, se retocará. Pero todo lo relacionado con investigación, desarrollo e innovación, seguro que no se va a reducir en tal caso, porque en todas las facetas, sea medicina o en este caso policial, lo que gastemos en investigación, desarrollo e innovación, yo no lo consideraría gasto sino más bien una recompensa; es decir, vamos a ser recompensados en nuestra eficacia, en todo lo que podemos ir desarrollando para ir combatiendo, en nuestro caso, ir cumpliendo lo que nos manda la Constitución y que es la de garantizar la libertad y seguridad de los ciudadanos y conseguir que cada día nuestro país sea más seguro en este tiempo que estamos de muchísima importancia, sobre todo en el turismo. Una de las claves de nuestro país por lo que es tan turístico es porque es uno de los más seguros de la Unión Europea y también a nivel global en el mundo. Y, para seguir en ese camino, no nos queda más remedio que invertir en esto. Estos días, también compartirán con nosotros sus experiencias miembros de la Guardia Civil, del Ministerio de Defensa, de la Policía Local y de organismos españoles que están trabajando dentro del marco de la Unión Europea.

Dicho esto, nada más, os deseo y me uno al deseo del Director del curso, Manuel Álvarez, de que además tengáis tiempo para disfrutar aquí de la buena temperatura y del buen clima que tiene El Escorial; y que hagáis vuestras aportaciones, que sea un curso interactivo, y que cada uno pueda contar su experiencia que también va a enriquecer a los que están aquí; que es de lo que se trata en estos cursos de verano.

A continuación comienza el contenido el curso, queda inaugurado el curso veinte de investigación, desarrollo e innovación.

Comentario de: Manuel Álvarez Junco.
Subdirector de los Cursos El Escorial

Se me ocurría al hilo de este curso comentar una cosa que a mí me parece muy importante, la relación que tenemos, y que tengo además el privilegio de estar en contacto con embajadas y con la visión de España desde fuera, una de las cosas que se destaca es que España es un país seguro. Es fundamental que lo sepamos, hablamos de la marca España y hablamos de una serie de cuestiones y no nos damos cuenta de que realmente estamos transmitiendo una sensación de seguridad que es el atractivo, o uno de los principales atractivos, que tiene nuestro país. Por eso, me parecía importarte decirlo, porque la gente de fuera de España, tiene esa impresión y eso es evidente, la seguridad es lo primero. Por supuesto que hay cosas fundamentales, pero lo primero que uno se plantea en la vida es si estás en un sitio tranquilo, seguro, donde realmente puedes actuar.

Creo que era el momento adecuado para decirlo, que sepamos que tenemos esa marca, por mucho que nos cuenten de eventos deportivos, de los que es mejor no hablar en este momento y de montones de cosas que son muy positivas, pero de pronto, que te venga un embajador y que te hable de eso, una persona que realmente se ha enterado, que está transmitiendo al mundo lo que es este país; desde fuera, esa visión externa me parece esencial que la conozcamos. Por eso no quería por menos de poner este añadido que me parece fundamental para que sepamos que lo estamos haciendo bien, tan sencillo como eso.

Primer panel: la globalización en investigación, desarrollo e innovación (i+d+i)

INNOVACIÓN EN EL CNP, RETOS DE FUTURO

LUISA MARÍA BENVENUTY CABRAL
Comisaria Principal del CNP, Secretaria General de la Jefatura Central de Logística e Innovación de la Dirección General de la Policía

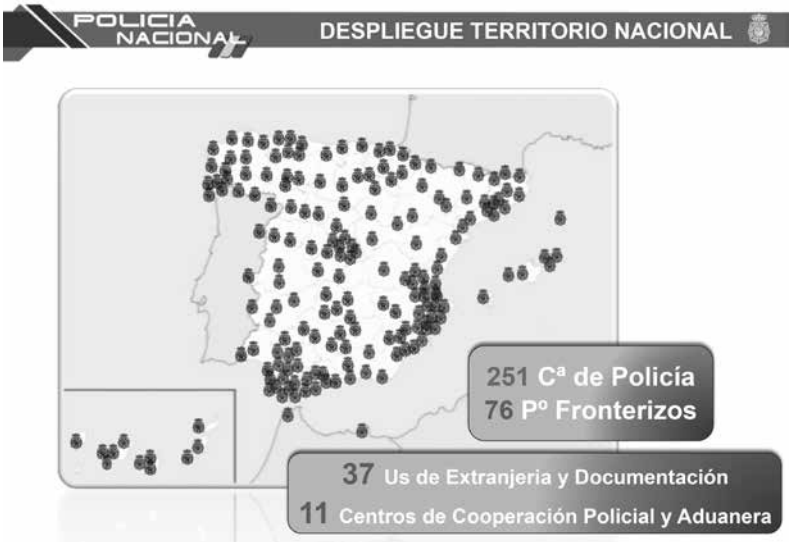
Cuando me propusieron hacer esta ponencia, mi idea fue dar una visión global de lo que es, primero, el Cuerpo Nacional de Policía, en qué momento estamos, dónde estamos posicionados y cómo está estructurada la innovación en nuestro Cuerpo así cómo en un futuro debería seguir la estela de los modelos de otras policías, en el ámbito de la Unión Europea.

Ha pasado mucho tiempo desde que el Rey Fernando VII publicara un 13 de enero de 1824 la Real Cédula por la que se crea la Policía General del Reino, siempre, desde el primer momento, a las órdenes de un magistrado. Ha habido muchas denominaciones a lo largo de la historia, muchas vicisitudes, la Policía es una de las instituciones nacionales más valorada por los ciudadanos españoles; además, está reconocida en el mundo como una de las mejores policías a nivel mundial en cuanto a eficacia e investigación.

Pero si algo caracteriza precisamente a lo largo del tiempo esa visión, esa función, el ADN policial, es la función de investigación. que data de primeros del siglo XX con los antiguos gabinetes de identificación y de criminalística, siguiendo las líneas de Vucetich, el creador de la dactiloscopia.

Esto, unido con una administración de recursos siempre precarios y escasos, ha hecho que la creatividad y la imaginación en el Cuerpo de Policía, haya sido una necesidad -una razón de ser-.

Hay un mensaje importante que quiero trasladarles aunque sea obvio; el Cuerpo Nacional de Policía es un servicio público, su vocación, su necesidad y su justificación es prestar un servicio público al ciudadano en el ámbito de la seguridad, un concepto lo más amplio posible. Todas sus acciones van dirigidas a ese objetivo, por eso, valores como la ética, la trasparencia y la equidad, que generan valor al ciudadano, también tienen que presidir la actividad de innovación en el Cuerpo Nacional de Policía.



Este es el mapa de la distribución territorial del Cuerpo Nacional de Policía. El número de población a los que damos cobertura, y las ciudades más importantes donde prestamos nuestros servicios.

POLICIA NACIONAL

DATOS DE POBLACION

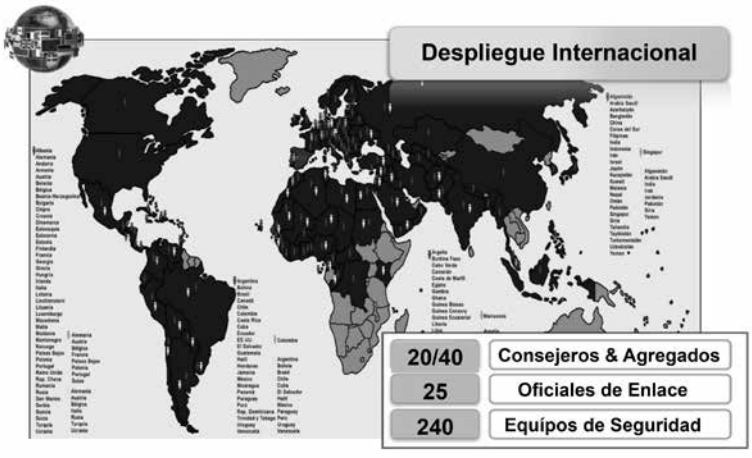
Nº habitantes de las 100 ciudades mas importantes: 21.715.571

CUERPO POLICIAL	Habitantes	Porcentaje %	Presencia en ciudades
Policía Nacional	16.598.597	76,43%	73
Guardia Civil	515.752	2,37%	6 (68,69,80,83,84 y 94)
P. A. Cataluña	3.644.047	16,78%	16 (2, 16, 22, 23, 26, 47, 48, 51, 56, 60, 63, 71, 75, 87, 96 y 97)
P A. P. Vasco	957.175	4,40%	5 (10, 17, 34, 62 y 93)

Posición	Ciudad	Habitantes	Posición	Citudad	Habitantes
1	Madrid	3.182.981	11	Alicante	329.988
2	Barcelona	1.620.809	12	Córdoba	325.916
3	Valencia	787.808	13	Valladolid	299.715
4	Sevilla	689.434	14	Vigo	292.986
5	Zaragoza	664.938	15	Gijón	272.365
6	Málaga	569.002	16	Hospitalet de Llobregat	257.349
7	Murcia	443.243	17	Vitoria	246.976
8	Palma de Mallorca	406.492	18	La Coruña	244.099
9	Las Palmas Gran Canaria	377.650	19	Granada	232.770
10	Bilbao	345.110	20	Elche	228.675

POLICIA NACIONAL

COOPERACION INTERNACIONAL



En el ámbito de cooperación internacional, pueden ver el despliegue que tenemos del Cuerpo Nacional de Policía, en el que también colaboran otros cuerpos policiales. Este es el mapa global de la Policía tal como está organizado según el Real Decreto 770/2017, donde está desarrollado el servicio de innovación en el Cuerpo Nacional de Policía.

Me corresponde el reto y el honor de dirigir el Servicio de Innovación y el Servicio de Fondos Europeos, íntimamente relacionado con todo lo que supone innovación en la Policía; porque toda innovación necesita de un presupuesto para llevarla a cabo y si no hay presupuesto, o es escaso, difícilmente podremos efectuar su desarrollo.

El Real Decreto 770/2017, atribuye a la Jefatura Central de Logística e Innovación, el impulso, la dirección y la coordinación de todas las actividades en esta materia de innovación, en materia de la dirección del impulso de la promoción del control y seguimiento de los proyectos que en materia de innovación, sobre todo de tecnología y de seguridad.

Radica en nuestra estructura la obligación y el mandato de la gestión y el seguimiento de los proyectos y subvenciones que en materia de fondos europeos y del proyecto Horizonte 2020, corresponde a la Dirección General de la Policía.

Estas son las diferentes áreas. Aunque le corresponde a la Jefatura de logística e innovación, liderar y coordinar, las grandes áreas policiales no solo en investigación, sino también en formación y perfeccionamiento, gestión económica y técnica, han desarrollado unidades especializadas que gestionan y lideran proyectos y grupos de trabajo en el ámbito de la Unión Europea.

Innovación no es solo innovación tecnológica; hay muchas clases de innovación y está orientada y enlazada en la gestión de cambio en todo proceso creativo. El término " innovación" a veces es confuso, ambiguo, y quería dar unas pinceladas al respecto antes de avanzar. La innovación está asociada a una idea de progreso, de mejora continua; pero lo importante en innovación son tres elementos: las personas a quienes va dirigida; la novedad que supone; y el valor, el beneficio que va a generar para la sociedad.

Esto es lo que enlaza la ética con la innovación. Ciencia, tecnología e innovación, a veces, suelen ir unidas, pero no se confunden, porque ni toda innovación es tecnológica, ni toda tecnología es necesariamente innovadora. Las clases de innovación más usuales, las tipologías, las tenemos aquí: tecnológica, científica, que son las más habituales, pero tenemos empresarial, innovación en educación, del cual la división de formación de perfeccionamiento es pionera, existe innovación financiera; hay innovaciones que tienen un carácter deductivo para la sociedad y hay muchísimas clases de innovación que no se basan exclusivamente en eso.

A veces se mezclan creatividad e innovación ¿qué es lo que las diferencia básicamente? La innovación requiere de la creatividad de forma continua, pero igual que la creatividad se mueve en el plano del pensamiento, la innovación se mueve en el plano de acción. Para resumir, citando la frase de William J. Coyne "La creatividad es pensar en ideas nuevas y apropiadas", mientras que "la innovación es la aplicación con éxito de las ideas dentro de una organización". La creatividad es el concepto y la innovación es el proceso. Esa es la gran diferencia, pero evidentemente, si no hay creatividad no puede haber innovación.

¿Cómo vivimos en la función policial la innovación? Estamos en la edad del cambio acelerado, con un futuro V.U.C.A: volátil, incierto, ambiguo y complejo, con fenómenos disruptivos en una sociedad para nosotros como los cambios migratorios, la globalización, el ciberespacio, el Big Data, el Internet de las cosas, la robótica y la interconexión y la inter operatividad.

Por eso, para el Cuerpo Nacional de Policía, institución en continua transformación, no solo para afrontar los retos en materia de seguridad

sino para adaptarnos a otro factor de nuestro entorno, es imprescindible desarrollar una innovación, sobre todo tecnológica para responder a las demandas en investigación.

Deben existir unos referentes legales en esta materia de innovación para afrontar los problemas de seguridad, porque los referentes legales, las leyes, siempre van por detrás de los hechos, es lo que llaman en el ámbito jurídico, "el poder normativo de lo fáctico", el hecho hace el derecho y muchas veces los legisladores van muy por detrás de todas las innovaciones tecnológicas y, sobre todo, no existen los medios financieros, ni los recursos que el mundo del crimen organizado posee. Es evidente que este siempre irá muchos pasos por delante.

La última modificación de la Ley de Enjuiciamiento Criminal, supuso un avance importante para dar cobertura en medios técnicos y tecnológicos, para la investigación, a las Fuerzas y Cuerpos de Seguridad.

¿Cómo tenemos estructurado y cómo entendemos que tiene que estructurarse la innovación en cualquier organización policial? La primera la función del departamento de innovación es conectar a todos los usuarios, tanto los internos de la organización como los externos. Detectar la necesidad para poder innovar y lanzar retos, pero para eso es importante tener el apoyo total de la dirección de la organización, no solamente de nuestra organización sino de cualquier organización que se precie.

El primer escalón para crear una estructura de innovación es la concienciación en esta materia; esa concienciación está conectada continuamente con la gestión del cambio y del cambio cultural, y ese cambio cultural tiene que venir, también, del liderazgo de los directivos policiales o de cualquier otra organización pública o privada, de los directivos. La innovación es un proceso continuo y tiene que discurrir de abajo-arriba y de arriba-abajo, en todos los procesos de la organización.

Por eso, es muy importante que la concienciación en cualquier innovación, ya sea educativa, tecnológica, o en materia de investigación; venga unida del consenso y del diálogo dentro de la organización porque los usuarios, es decir, los policías son los encargados de implantar todas las medidas y de recibir las medidas que tengamos, no solamente en tecnología de seguridad, sino en otros tipos de innovación como, por ejemplo, en la formación. Y eso, es importante para que cualquier proceso innovador llegue a cabo con éxito y llegue, por supuesto, al ciudadano que es el usuario final.

En segundo lugar, es muy importante, igual que otras policías europeas, crear las comunidades de innovación. Las comunidades de innovación trascienden a la estructura formal, su función, a nivel interno, es crear comunidades de usuarios, fomentar buenas prácticas de innovación en todas las áreas policiales y que esa función de coordinación y de comunicación -gestión del conocimiento-, fluya entre todas las áreas y cree sinergias pero, sobre todo, nacionales, con otros entes públicos o privados y sobre todo internacionales.

¿Qué función importante enlaza con las funciones de la innovación en la Unión Europea? La creación de un radar tecnológico.

El radar tecnológico en la Policía está a cargo de servicios de innovación a través de proyectos y grupos de trabajo, y detecta los panoramas. Es el encargado de rastrear el panorama de las nuevas tecnologías, sobre todo orientadas a ver posibles brechas en seguridad y las nuevas realidades delincuenciales. Esto enlaza con el mundo del ciberespacio, de la ciberseguridad y de la ciberdelincuencia.

Toda innovación tiene que tener una proposición matemática, un problema que hemos detectado, una idea para solucionarla y un presupuesto para ejecutarlo. Solo así podremos materializar ese proyecto y que ese pensamiento se traduzca en una acción. Si no lo tenemos, nosotros, un cuerpo imaginativo, buscamos soluciones, incluso con escasez presupuestaria y la creamos renovando lo que ya tenemos, modificando los procesos y los procedimientos que ya están implementados. Otras veces, tenemos que recurrir a la financiación externa.

Dentro de las comunidades se están creando, y me voy a referir al plano internacional, en otros cuerpos policiales, los ecosistemas de innovación, a nivel interno y a nivel externo, para dar respuesta y tener en cuenta esa proposición matemática que acabo de mencionar.

Interno, porque tiene que influir, modificar el comportamiento cultural de la organización, porque tiene que enlazar con la gestión del cambio y porque fomenta el intercambio de habilidades y capacidades individuales y grupales. En la Policía, dentro de las áreas que a veces están trabajando en forma paralela, a veces sin cooperar unos con otros.

Externo, por supuesto, con la colaboración público-privada; la creación de asociaciones con entidades no solamente ciudadanas, con empresas, administraciones públicas, universidades o equipos de investigación.

En el plano internacional me tengo que referir al centro de innovación de Interpol con sede en Singapur con muy pocos años de andadura, está formado por cuatro estructuras de laboratorio: de futuro y de prospectiva; de adaptación policial de ciberespacio; de nuevas tecnologías y laboratorio digital forense.

En este aspecto, en junio del año 2018 tuvo lugar la primera reunión de jefes de innovación de las policías representadas en Interpol, reunión en la que se creó una plataforma, que está en fase de implementación y de prueba, de jefes de innovación policiales que engloba Interpol y que está abierta a la incorporación de otros futuros cuerpos policiales a nivel no solamente europeo sino a nivel mundial.

En nuestro plan estratégico policial está mencionado el I+D+i y la investigación, pero yo quiero hacerles llegar que la innovación debe tener un eje estratégico exclusivo dentro de cualquier plan estratégico y que, cara al futuro de la Policía, tiene que ser transversal a todas las áreas. En efecto existen grandes planes estratégicos a nivel del Estado, pero el presupuesto de la Dirección General de la Policía debería contemplar, aunque sea una pequeña partida, dedicada a innovación en I+D+i y a otros tipos de innovación que no sean solamente tecnológicos.

¿Qué es fundamental para desarrollar y avanzar en el tema innovación? La colaboración público-privada, entre entes públicos, empresas privadas, universidades; es necesario desarrollar los *clusters*. Precisamente en innovación tenemos la figura de la asociación empresarial innovadora, dentro de INCIBE, muy focalizada en temas de seguridad.

Estos *clusters* representan agrupaciones de empresas en tecnología ¿Cómo funcionan? Las policías y otras administraciones públicas se dirigen a ese *cluster* a través de INCIBE para proponer soluciones, detectar alguna necesidad y obtener una solución tecnológica de esas empresas.

Es necesario que tengamos un modelo, un *cluster* más a nivel de seguridad policial porque, efectivamente, están en la actualidad más enfocados a seguridad y defensa, y a seguridad industrial.

Exclusivamente, como seguridad policial, está orientada precisamente la asociación empresarial innovadora actual, dentro de INCIBE, más al ámbito de la innovación en la ciberseguridad; la Comisaría de la Policía Judicial, en la unidad de investigación tecnológica o de ciberdelincuencia, es un colaborador continuo de ese trabajo.

¿Qué modelo policial se propone? El modelo holandés, que está regulado normativamente, es un *cluster* de grandes empresas en tecnología en Holanda y radica en una empresa "TINOU" encargada legalmente de colaborar con las Fuerzas y Cuerpos de Seguridad en Holanda en todo tema de innovación, ciberseguridad, en robótica, en tecnologías de la imagen, en drones etc.

Colabora en investigaciones que han culminado con éxito en ciberdelincuencia, en la darkweb, en criptomonedas y en otras especialidades.

¿Qué fórmula de desarrollo tecnológico e investigación tecnológica estamos tratando todas las administraciones? La PCP es la compra pública pre comercial y el PPI es la compra pública innovadora.

La PCP consiste en la adquisición de productos de I+D, es decir, de productos que hasta la fecha no tienen una solución tecnológica o no existen en el mercado.

La PPI, compra pública innovadora: son las administraciones públicas adjudicadoras quienes actúan como cliente principal mediante la adquisición de "soluciones innovadoras"; son productos o soluciones que ya están en el mercado pero que no están disponibles a escala comercial

¿Qué Skateholders, en especial para nosotros, tiene la Policia Nacional? Por supuesto, la Secretaría de Estado de Seguridad a través de la Subdirección General de Comunicación para la Seguridad, CDTI (Centro para el Desarrollo Tecnológico Industrial), e INCIBE (Instituto Nacional de Ciberseguridad de España)

LA INNOVACIÓN Y LA FUNCIÓN POLICIAL.
Desarrollo y limitaciones

¿Cuáles son las limitaciones que nos encontramos? Un presupuesto limitado, la Policía no tiene una partida presupuestaria dedicada exclusivamente a innovación. Siempre existe la prioridad de las necesidades urgentes, cotidianas y operativas. Necesitamos, al igual que otros cuerpos policiales a nivel mundial de socios externos para la financiación; un aumento del *cluster* en innovación ¿Dónde tenemos que recurrir? Evidentemente a la financiación de la Unión Europea. El Ministerio del Interior es líder en proyectos del marco Horizonte 2020; también a los fondos Feder.

¿Qué fondos son los que nos interesan? El Fondo de Seguridad Interior (FSI): cooperación policial internacional, fronteras y visados; los Fondos

Feder, Fondos FAMI de Asilo a la Migración e Integración y los Proyectos de Horizonte 2020.

LA INNOVACIÓN EN LA POLICÍA NACIONAL Y EUROPA: Grupos Europeos. Horizonte 2020

El grupo ILEAD: red de fuerzas de seguridad europeas, cuenta con un radar tecnológico con la finalidad de hacer prospectiva y análisis de mercado de tecnologías relativas a 25 temáticas diferentes, en los que se pretende identificar las necesidades tecnológicas para la seguridad dentro de la Unión Europea.

El grupo ENLETS: red de servicios tecnológicos de fuerzas policiales de 26 países de la UE, dependiente de los Grupos de Aplicación de la Ley del Consejo de la UE; encargado de un sistema de prospectiva tecnológica y análisis de tecnologías de seguridad para todos los miembros de la red a nivel nacional y siempre alineado con las estrategias europeas en seguridad.

España forma parte del grupo dirigente de la red en la que se toman todas las decisiones. El Cuerpo Nacional de Policía, a través del Servicio de Innovación y Desarrollo, es colider. La Policía Nacional está participando o ha participado en grupos como: parada de vehículos, inteligencia en fuentes abiertas, contratación de tecnología y estudio forense de electrónica.

HORIZONTE 2020

Programa Marco (H2020) en el período 2014-2020 mediante la implantación de tres pilares, contribuye a abordar los principales retos sociales, promover el liderazgo industrial en Europa y reforzar la excelencia de su base científica. El presupuesto disponible ascenderá a setenta y seis mil ochocientos ochenta (76.880)M€. Las Fuerzas y Cuerpos de Seguridad, presentan proyectos en el programa "Sociedades Seguras".

RAMSES: pretende crear una plataforma para la investigación forense de evidencias en Internet fundamentalmente desde el punto de vista financiero y análisis de ramsonware y banking troyans.

TITANIUM: desarrollo de tecnología para la investigación de criptomonedas fundamentalmente en darkweb y sobre todo con la finalidad de recogida de evidencias digitales.

VICTORIA: pretende una plataforma de video análisis que sea capaz de automatizar el análisis de grandes cantidades de video mediante un fuerte componente de la capa de inteligencia y de forma automatizada a través de la definición de parámetros de análisis.

BROADWAY: sistema inter-operable de radio para que cada país miembros pueda utilizar sus sistemas de comunicación-radio en el resto Presupuesto estimado para el Ministerio del Interior de ciento treinta y dos mil (132.000)€, de los que treinta mil (30.000)€ son para Policía Nacional).

COPKIT: establecimiento de alarmas tempranas sobre amenazas relevantes en el uso de tecnologías que pueden ser utilizadas por el crimen organizado y las organizaciones terroristas, a partir de las que se mejoran las decisiones estratégicas y operativas para dar respuesta a las mismas. Presupuesto para el Ministerio del Interior de ciento ochenta y seis mil ciento veinticinco (186.125)€ (pendiente por determinar la cantidad asignada a Policía Nacional y Guardia Civil)

PROYECTOS PRINCIPALES DE LA POLICÍA NACIONAL EN LA ACTUALIDAD

Proyecto DNI-Express. La competencia de documentación para la Policía es muy importante ya que es una de sus funciones desde el año 1950, la tiene en exclusividad y es la única entidad oficial de certificación gratuita. El DNI español se encuentra reconocido por el reglamento EIDAS de reconocimiento, certificación e identidad digital de todos los países de la Unión y supone que todos los países de la Unión Europea reconozcan el DNI electrónico la validez como identificación y firma en cualquier transacción que cualquier ciudadano haga dentro del marco de la Unión Europea.

Consiste en el desarrollo de un procedimiento automatizado de renovación del DNI; supondrá un incremento de la seguridad (captura imagen in situ) y un fuerte descenso de los tiempos de espera, paralelo a un aumento en la producción de documentos.

Partes de Intervención de Patrullas de Seguridad Ciudadana. Su finalidad es crear y generar inteligencia e interconexión con todas las bases de datos policiales, inteligencia no solo a nivel criminal, sino a nivel de información de todos los tipos, para optimizar no solo los recursos, las patrullas de seguridad ciudadana, sino mejorar cualquier tipo de investigación.

Proyecto de Movilidad. Consulta de bases de datos policiales, fotografías y otras funcionalidades a través de smartphones securizados, destinados en especial a la Policía del Transporte y operativos de patrullas a pie. Finalizada la fase piloto en la Comisaría General de Seguridad Ciudadana. Ultimadas las funcionalidades y características técnicas para integración en los automóviles destinados a las patrullas de seguridad ciudadana.

Séneca. Conversión de las Salas del 091, en centros de integración de inteligencia procedente de las actividades de seguridad ciudadana.

INTEROPERATIBILIDAD. SIENA Y UFM3 (Europol) ETIAS, ECRIS EE

La Comisaría General de Policía Científica lidera un grupo de trabajo en la Unión Europea.

Pretende la interconexión de las bases de datos, sobre todo en Europol.

PROYECTO UFM3, va a permitir un acceso con distintos niveles de usuario, directamente a las unidades policiales sin tener que pasar en primera instancia por las funciones de enlace.

ETIAS, es un sistema de entrada y salida de la Unión Europea.

ECRIS EE, es un sistema de interconexión de las bases de datos de antecedentes penales y policiales a nivel de la Unión Europea.

VERIPOL, es un sistema detección de denuncias falsas. Optimización de los recursos policiales y reducción de estadísticas de delitos violentos.

DRONES: la competencia del Servicio de Medios Aéreos en coordinación con el servicio de innovación. En la actualidad está en fase de desarrollo un Plan de de RPAS. Sistemas de detección e inhibición. Utilización en espacios confinados y búsqueda de personas en subsuelo.

PROYECTO SURVEIRON en colaboración con la SES y Unión Europea.

BIG DATA: "I-3".

BLOCKCHAIN.

APLICACIONES.

COMISARÍA VIRTUAL.

CONCLUSIONES

- La Policía Nacional es un servicio público al ciudadano y tiene una adaptación al cambio acelerado.

- La innovación supone concienciación y cambio cultural a todos los niveles de la organización. Conexión con la Gestión del Cambio.

- Necesidad de Estrategia en innovación orientada a las mejoras de las capacidades.

- Coordinación interna y colaboración público-privada esencial.

- Fundamental la colaboración y cooperación internacional.

- El presente y futuro de las organizaciones pasa por su capacidad en I+D+i y su creatividad.

- Necesidad de soluciones imaginativas para adaptarse al cambio acelerado de la sociedad.

- Ante un escenario de restricción presupuestaria. es imprescindible fórmulas como la financiación de la Unión Europea. PCI, PPI.

PROGRAMAS EUROPEOS DE INNOVACIÓN

ANABELA GAGO
Jefa de la Unidad de Innovación e Industria para la Seguridad de la Dirección General de Interior de la Comisión de la UE

Es un placer para mí poder dirigirme a los asistentes a este curso de verano sobre la investigación en la función policial organizado por la Universidad Complutense de Madrid, la Fundación Policía Española y el resto de colaboradores; y mi sincero agradecimiento a los organizadores por haberme invitado a participar en esta sesión, pero también por llevar a cabo esta iniciativa en un momento en el que se ha adoptado la propuesta Horizonte Europa, que va a sustituir a partir del año 2021 el programa Horizonte 2020. Esto nos ayuda a mantener la inercia positiva generada en el seno de la Unión de la Seguridad.

El hecho de que estemos hablando de la I+D+i en la función policial pone de manifiesto cómo la investigación en seguridad puede ser un factor decisivo en el ámbito operativo al plantear nuevas soluciones, nuevas herramientas para hacer frente a las amenazas cambiantes, pero también en facultar mejor entendimiento de estas amenazas, de los comportamientos y del impacto de las nuevas herramientas.

En España esto es bien conocido, al tratarse de uno de los Estados Miembro con una participación más activa en los programas de investigación en seguridad de la Unión Europea. Si hablamos en términos de beneficiario, en relación con la contribución europea para la investigación en el marco de la seguridad, España se sitúa en la primera posición. En el marco del Horizonte 2020, España ha recibido contribuciones de la CE en torno a los noventa y dos millones de euros a través de su participación en ciento

quince proyectos y su papel de coordinador en unos cuarenta y ocho. Esto es muy significativo. Es decir, representa el once coma cinco por ciento de todo el presupuesto de Sociedades Seguras en el marco europeo, motivo por el cual me complace aún más poder dirigirme a ustedes en el marco de esta jornada.

La amenaza terrorista en la Unión Europea sigue al alza, y los desastres naturales, a menudo relacionados con fenómenos climáticos extremos, siguen causando numerosas bajas a lo largo y ancho de nuestro continente, teniendo costes económicos y medio ambientales enormes.

El programa de sociedades seguras centra su actividad en la investigación en la función policial, siendo así pertinente para el trabajo de todo tipo de cuerpos y fuerzas de seguridad, incluyendo las actividades llevadas a cabo por las autoridades aduaneras, Cuerpo Nacional de Policía y Guardia Civil, cuerpos de protección civil, etc. Esta investigación abarca campos como la lucha contra el terrorismo y contra el crimen organizado, la protección de las fronteras, la protección de las infraestructuras críticas, así como la resiliencia frente a desastres naturales, incluyendo entre otros fenómenos los fuegos extremos o las inundaciones.

El último Eurobarómetro (otoño del año 2017) mostró cómo el terrorismo es claramente la principal preocupación de los europeos (38%), pero también lo es el crimen (10%). Esto significa que los temas relacionados con la seguridad están en lo más alto de las prioridades de los ciudadanos europeos. Pero más allá de la percepción de los ciudadanos, como ya han mencionado otros dos ponentes, la situación cambia constantemente de una forma acelerada en todo lo relativo a las amenazas.

Si hablamos de crimen organizado, por ejemplo, desde mi anterior puesto en la Jefatura de la Unidad de Crimen Organizado, del Crimen y de la Corrupción, recuerdo datos que hablaban de tres mil seiscientas (3.600) organizaciones de crimen organizado a nivel europeo bajo investigación. En el informe de Europol publicado en el mes de marzo, el Socta 2017 (Serious and Organized Crime Threat Assessment) actualmente se habla de cinco mil (5.000) organizaciones de crimen organizado bajo investigación a nivel europeo. Es decir, la función policial progresa en temas como la inteligencia, en la investigación, etc., pero estas cifras son también un reflejo de la evolución y de la adaptación a las nuevas tecnologías por parte de estas organizaciones, haciéndolo en ocasiones más rápido que la propia policía.

La complejidad de las amenazas transfronterizas requiere una respuesta concertada y multi-nivel. Esa respuesta es asimismo compleja y conlleva un

alto coste. La capacidad de responder de manera eficiente normalmente no está al alcance de un Estado Miembro solo, con lo cual, solamente a través de un enfoque conjunto europeo podremos encontrar soluciones para salvaguardar la seguridad de nuestros ciudadanos.

Los ciudadanos esperan una respuesta unificada a la situación actual por parte de la Unión Europea, y la Comisión ha asumido esta expectativa estableciendo como objetivo una Unión para la Seguridad (Security Union). La investigación en seguridad nos permite desarrollar herramientas que pueden mejorar la protección a los ciudadanos de la Unión Europea y podemos decir con orgullo que durante los últimos años hemos luchado por estructurar lo que llamamos una "Comunidad Europa para la Investigación en Seguridad".

En términos generales, la investigación financiada con fondos de la Unión Europea representa entre el 8% y el 10% del total de la inversión pública en investigación. Pero este saldo es muy diferente en el ámbito de la seguridad civil, donde los fondos de la Unión Europea representan el 50% de la financiación pública global de la Unión. Estos números bien podrían reflejar el caso de España, pero lo cierto es que solo ocho Estados miembros tienen su propio programa nacional de investigación en materia de seguridad, mientras que la mayoría dependen casi totalmente de los fondos europeos para poder hacer alguna investigación en materia de seguridad.

Del año 2014 al 2016 el presupuesto para las sociedades seguras europeo en el Horizonte 2020 ronda los seiscientos cuarenta y ocho millones de euros (648). En el futuro cercano tenemos previstos, para el año 2018, doscientos once (211), para el año 2019 doscientos cuarenta (240), y para el año 2020, para cuya programación estamos empezando a identificar las prioridades en colaboración con los Estados Miembro, doscientos sesenta y cuatro millones (264). Con lo cual, cuando un Estado Miembro como España se decide participar, no solo en la determinación de la programación a nivel europeo, sino también a participar de una forma tan activa en los proyectos implicando a los usuarios, es fundamental.

En referencia a los aspectos financieros, permítanme enfatizar que durante el próximo Marco Financiero Multianual (MFF) del año 2021 al 2027, que recoge todo el presupuesto para la Unión Europea, se prevé un refuerzo sustancial de las actividades de seguridad; por ejemplo, en la gestión de fronteras. El paquete del Marco Financiero Multianual 2021-2027 refleja a las claras la visión del Presidente Junker de una Europa que protege, empodera y defiende.

Asimismo, la relevancia de la investigación se confirma mediante el nuevo Programa de Investigación e Innovación, Horizonte Europa, que será el mayor programa de financiación de la investigación y la innovación que jamás haya existido, alcanzando la suma de noventa y siete mil (97.000) millones de euros, [Horizonte 2020 = setenta y siete mil (77.000) millones de euros]. Horizonte Europa se sustentará sobre nuestro deseo de garantizar el impacto de la financiación europea y eso es fundamental: la prioridad es, sobre todo en el área de la seguridad, tener un impacto real, que sea útil a los usuarios finales. En el área de seguridad y con la falta de presupuestos públicos que hay actualmente sería un lujo que no se aprovechara en el ámbito operativo lo que se desarrolla en el marco de la investigación y de la innovación.

Algunos puntos fundamentales del Horizonte Europa:

- Asegurar una inversión esencial que pueda estimular la inversión privada.

- Adecuar los marcos regulatorios o referentes legales a las necesidades de la innovación.

- Convertirse en un promotor de la innovación para la creación de mercados.

- Reconectar la investigación y la innovación con la ciudadanía a través de misiones pan-europeas.

- Apoyar la diseminación de la innovación a lo largo y ancho de la Unión.

En lo que al ámbito de seguridad se refiere, si bien en cuanto a contenido Horizonte Europa mantendrá cierta continuidad con las estructuras actuales del programa de trabajo Sociedades Seguras, en lo que se refiere a procesos se prevé más agilidad, más flexibilidad y más posibilidad de que tenga impacto. De este modo, el futuro programa buscará:

- Asegurar una clara separación entre la investigación en seguridad y la investigación en defensa, canalizada a través del Fondo para la Defensa, para así proteger nuestro presupuesto de seguridad civil, estando al mismo tiempo atentos a la simetría para que no hay duplicaciones o pérdidas.

- Mantener unidas bajo el mismo paraguas a las dimensiones de ciberseguridad y seguridad física.

- Habilitar las sinergias apropiadas con otros programas de financiación relacionados, como por ejemplo, el futuro Fondo para la Gestión Integrada de Fronteras, el Fondo para la Seguridad Interior -la Comisión hizo nuevas propuestas en junio- y el Programa Digital Europe. Me alegro de haber mencionado los Fondos Estructurales FEDER y el Fondo Social Europeo y el fondo para la seguridad interior también, porque yo no venía del mundo de la investigación sino del mundo de la Policía, de la lucha contra el crimen organizado. En un momento se me planteo cómo alinear el presupuesto dedicado a los Estados bajo el Fondo para la Seguridad Interior con los desarrollos en el marco de la investigación e innovación europea, así como el papel que pueden jugar instrumentos como la compra publica pre-comercial o la compra publica innovadora. Bien, pues con las nuevas propuestas para el programa Horizonte Europa, la base legal prevé este alineamiento y la sinergia entre fondos. También con los fondos estructurales, algo que pude comprobar durante su negociación. Existe mucha complementariedad entre los fondos FEDER y lo que se hace en H2020 bajo, por ejemplo, el área de fronteras. Estoy muy interesada en saber cuáles son las áreas que España habrá utilizado con FEDER

El futuro programa Horizonte Europa también busca:

- Garantizar una estructura orientada a Misión, en la que los requisitos del usuario final tengan un papel principal.

- Prever la flexibilidad necesaria para lidiar con el cambiante panorama de seguridad. Más flexibilidad, en explorar más sencillamente la compra pública pre-comercial, o sea, que pueda hacer unas acciones más rápidas. Esto también está en la legislación, que son las reglas para la participación en los proyectos bajo Horizonte Europa.

- Asegurar una mejor diseminación y explotación de los resultados a través de mecanismos específicos

Por supuesto, desde las políticas europeas, siempre necesitaremos tomar precauciones para que el dinero público dedicado a investigación se invierta de una manera eficaz y eficiente. Para maximizar el impacto de la investigación, nuestros esfuerzos deben estar totalmente integrados en un proceso de desarrollo de capacidades de mayor alcance, permitiéndonos así una mejor interacción con los actores relevantes en el proceso de co-creación. Parece muy idealista pero debe ser así.

El primer grupo que es clave por su orientación estratégica es el de los facultativos (practitioners). Cuerpos y fuerzas de seguridad, protección civil, centros forenses, etc. Necesitamos seguir estructurando las comunidades de facultativos que nos permitan consolidar de manera sistemática los requisitos de usuario a nivel europeo para que luego haya interés en desarrollar las herramientas que permitan responder o contestar a esas necesidades. La Señora Benvenuty habló de nuestras redes de facultativos, y eso sí es algo que se está desarrollando cada vez más. Proyectos como I-lead, vinculado también a la red Enlets, son redes de facultativos integrados por autoridades policiales. También financiamos redes de centros forenses y, ahora se están desarrollando otras áreas como la de bomberos y servicios de protección civil en el proyecto FIRE-IN. Esto es muy importante porque trabajan juntos determinando lo que es necesario y luego lo comunican a nivel europeo para que la investigación pueda desarrollarse y así canalizar la la innovación.

Otro punto muy importante para el futuro es el papel de las agencias europeas como Europol y la Agencia Europea de Guarda Costas y Guardas de Fronteras (Frontex). Estas agencias deben tener un papel significativo en el ciclo de los proyectos de investigación, agregando y contrastando las necesidades de los usuarios finales, como son los cuerpos de policías y las guardias fronterizas, y proporcionándolas como entrada al ciclo de programación de la investigación.

De este modo, contribuirán a garantizar que los resultados de esta investigación sean efectivamente útiles en el campo operativo. Es un trabajo que lleva mucho tiempo, por ejemplo, Frontex acaba de reestructurar un departamento de investigación mucho más importante para poder llevar a cabo este nuevo papel.

En cualquier caso, los usuarios finales no deben encontrarse solos en los procesos de creación de soluciones innovadoras. Necesitamos, por tanto, reflexionar internamente sobre cómo mejorar su colaboración con científicos, investigadores, académicos y, por supuesto, con la industria. Sin la involucración, el compromiso y la inversión de la industria europea, las soluciones innovadoras no llegarán al mercado y se eternizarán en un ciclo de investigación alejado del ámbito operativo.

Pero, incluso si conseguimos hacer un uso eficiente de la experiencia de todos los actores mencionados en un enfoque integral, aún queda un último reto: la comunicación. Es muy habitual que los resultados de la investigación en seguridad no se comuniquen o se diseminen entre las comunidades de interés, impidiendo que se acelere su tránsito al mercado o se les dé un uso apropiado sobre el terreno de operaciones. España, por ejemplo, participa en

muchos proyectos, pero también hay otros proyectos en los que no participa, a lo mejor, hubiera sido necesario saber que hay proyectos que conducen a un resultado X y que también lo podrían aprovechar; y los Estados miembros que participan mucho menos que España en proyectos, todavía más interés tendrían en saber lo que pasa.

En esta misma línea, no me gustaría dejar pasar la oportunidad de mencionar el próximo gran evento de diseminación, organizado por la Comisión Europea en colaboración con la Presidencia Austriaca de la Unión. Se trata del Security Research Event 2018 que tendrá lugar en Bruselas los días 5 y 6 de diciembre, y donde trataremos de profundizar en cómo mejorar la comunicación y la diseminación de los proyectos de investigación en seguridad. Este es un factor crucial para reducir el hueco existente entre la investigación y su aplicación práctica.

La ciencia y la investigación se fundamentan en la colaboración, en construir puentes y en descubrir intereses comunes. Se trata de desarrollar soluciones tecnológicas innovadoras que puedan prevenir o hacer frente a las amenazas y a los retos del mañana. Se trata de mejorar el entendimiento de los miedos de nuestra sociedad y el impacto que producen en ella. Todos deberíamos ser conscientes de una cosa: necesitamos aprovechar cada oportunidad que surja durante la implementación del próximo programa marco para mejorar la cooperación entre todos los actores y para abordar de manera conjunta los retos y problemas que identificamos en común.

Estas jornadas son un claro ejemplo de este modelo de colaboración y nuestra intención es seguir prestando nuestro apoyo. Permítanme, para finalizar, desearles unas jornadas exitosas y altamente productivas durante el resto del curso. Confío en que las ideas que surjan de este foro nos permitan reforzar nuestros objetivos y progresar hacia una investigación en Seguridad Europea en beneficio de las necesidades de todos los ciudadanos.

TURNO DE PREGUNTAS

Pregunta en sala: soy Comisario de Policía en Melilla, y mi pregunta es: los proyectos en materia fronteriza, como están en la actualidad.

Responde: Anabela Gago

Es una de las partes más importantes de nuestro trabajo. Todo lo que vaya a los proyectos de vigilancia de fronteras, que cubre no solo fronteras de tierra sino también marítima, son muy importantes. Tenemos muchos proyectos, algunos de gran éxito, como por ejemplo el proyecto CLOSEYE, en el que España está implicada como uno de los actores más activos. CLOSEYE ha permitido desarrollar herramientas de vigilancia marítima, pero también de interoperabilidad entre sistemas de distintos estados. Este proyecto, en el que hay autoridades de España, Portugal e Italia, bajo la coordinación de la Guardia Civil , ha llevado al desarrollo de varias herramientas y soluciones específicas. Este proyecto ha permitido alcanzar un grado de madurez tecnológica alto para la comercialización de productos que ya están siendo utilizados en varios países, algunos fuera de la Unión Europea, donde debemos recordar, también hay demanda. Más aun, CLOSEYE ha conseguido explotar sinergias con el fondo de seguridad interior, con una propuesta presentada de forma conjunta por Guardia Civil y la Guarda Nacional Republicana de Portugal para la adquisición de equipamiento de vigilancia. Pero tenemos otros proyectos, por ejemplo, SAFESHORE, muy importante y que implica a varios Estados miembros, pero también países asociados como, por ejemplo, Israel. Una de sus partes más interesantes tiene que ver con la demostración conectada a drones de vigilancia, y a la amenaza de su utilización. En definitiva, es una de las áreas de investigación más extensa y el año pasado en nuestro evento anual de seguridad, que fue en Talín, la mayoría de los proyectos que estuvieron en demostración fueron en el área de la protección de fronteras. No hablo de migración, porque investigación en migración no se enmarca en el reto social "Sociedades Seguras" sino que está en otro ámbito del programa marco que no trata sobre seguridad. Por el contrario, la propuesta del nuevo programa de investigación e innovación Horizonte Europa, contempla que ambas estén juntas en un *cluster*, aunque con áreas de intervención diferenciadas. En el informe que vi de Europol una de las cinco mil organizaciones criminales de mayor crecimiento es el crimen de fraude de documentos que está conectado con el fenómeno de la inmigración. Y, ahí se dirige la investigación en el área de la seguridad, a crímenes que están creciendo. El fraude de documentos es un área estratégica.

Pregunta en sala: ¿Cuál es exactamente el papel que se ha propuesto para agencias como Frontex o Europol?

Responde: Anabela Gago

En el papel solo Frontex, pero también EU-LISA, tienen en su nuevo mandato un artículo que describe el papel que deben tener en materia de investigación. Europol, no lo tiene pero la filosofía es que las agencias estén trabajando cotidianamente al lado de los usuarios, de las fuerzas de Policía, que son los que saben lo que es necesario en el plano operativo; pueden tener un trabajo de identificación y agregación de las necesidades y pueden ayudar a decir dónde dirigir la investigación. El papel de las agencias no debería ser el de beneficiario de un proyecto, formando parte de un consorcio, es que tengan un papel como el que tenemos nosotros desde la dirección general de asuntos de interior y que es dar una orientación a las necesidades, a congregar a los usuarios, y acompañar la evolución del proyecto. Posteriormente, pueden tener un papel fundamental en la adquisición de tecnología, por ejemplo implementando proyectos de compra publica pre-comercial o dando apoyo a las autoridades nacionales en la utilización de otros fondos, no de investigación, sino mas operativos, como los fondos FEDER o el futuro Fondo de Gestión Integral de Fronteras. Ese es el papel, y ahora estamos trabajando mucho con Frontex para definirlo. Luego tenemos Europol, que está muy interesado en desarrollar ciertos proyectos y nos preguntan si pueden ser parte del proyecto. No es esa la orientación que queríamos, no es que sean beneficiarios, porque es una agencia europea, lo que queremos es la otra filosofía; pero si acaso hay algún proyecto que sean parte y que sea muy prometedor, no está prohibido que participen, aunque nosotros no lo estamos fomentando.

LA SEGURIDAD EN EL PLAN ESTATAL DE INVESTIGACIÓN CIENTÍFICA Y TÉCNICA Y DE INNOVACIÓN

JUAN CARLOS CORTÉS PULIDO
Director de Programas Europeos, Espacios y Retornos Tecnológicos del Centro para el Desarrollo Tecnológico Industrial (CDTI) del Ministerio de Economía, Industria y Competitividad

Quería hacer unos comentarios derivados de las intervenciones precedentes, uno realizado por José M. Pérez. Al principio del curso ha hablado, acertadamente, de un tema fundamental, que la innovación no es un gasto es una inversión, es decir cuando yo vuelvo a casa, pago el parking eso es un gasto, pero si compro acciones de la empresa, eso es porque tengo una expectativa de futuro, de tener dividendos, eso es la innovación; es una inversión porque queremos tener un retorno a esa inversión en años venideros y básicamente se traduce en un crecimiento económico y a la postre en mejorar la vida del ciudadano, pero en particular, y ese es el objetivo.

Y otro comentario que creo es importante, Luisa Mª Benvenuty ha dicho que la financiación es fundamental para la I+D+i; sin ninguna duda, es absolutamente fundamental. Sin fondos no hay I+D+i, pero es condición necesaria, no suficiente. Saben ustedes ¿cuál es una característica, una necesidad de I+D+i? aparte de la financiación la estabilidad; es decir, nosotros cuando hacemos seminarios tenemos la obligación de hacer proselitismo tecnológico y siempre decimos que el tema del I+D+i, Horizonte 2020, lo que tiene que ver con programas nacionales, son complejos, y se necesitan unos recursos delicados, desde luego, con una estabilidad importante. Es la única forma de tener éxito de cara al futuro. Por eso les digo que hacen falta

fondos pero también estabilidad en la gestión de los fondos, sino realmente la participación no es buena.

Dicho esto, voy a pasar a comentarles cuatro ejes que quería compartir con ustedes.

CDTI Y EL NUEVO PLAN ESTATAL

El primer punto es el CDTI y su papel dentro del plan estatal de I+D+i, para luego continuar con la financiación que ofrecemos desde el centro, tanto en su vertiente nacional como internacional y al final también quería compartir con ustedes ciertas ideas relativas al espacio y la seguridad. El CDTI desde el año 1986 es la delegación de España en la central europea y ahora mismo hay varias iniciativas que creo serán de su interés, en el campo espacial en particular. El Gobierno es propietario de un satélite, el satélite Ingenio, que se va a lanzar creo que en el último cuarto del año 2019, la Comisión Europea ha lanzado un programa de comunicaciones por satélite y también ha lanzado un programa de seguimiento de basura espacial que también tendrá un impacto muy fuerte en la seguridad.

En el año 2013, se redactó y publicó la estrategia española de Ciencia Tecnología e Innovación que es el documento madre elaborado entonces por el Ministerio competente en este tema y del que luego emanan los diferentes planes estatales para su desarrollo en paralelo con el Programa Marco Europeo, que en su edición actual lo conocemos como Horizonte 2020. El plan de investigación científica, técnica e innovación del año 2013, acabó el año pasado, y a continuación se ha empezado a trabajar en el siguiente, que es el que está vigente, el plan estatal 2017-2020. Estos son documentos que redacta el Ministerio, con el concurso de todos los actores, documentos con un componente político, porque los hace el Ministerio correspondiente, y después se ejercitan básicamente a través de dos agentes preferentes, que son la Agencia Española de Investigación y el CDTI, que es por ley la agencia española de innovación. Son los dos órganos preferentes para implementar la gestión del plan.

¿QUIÉNES SOMOS?

Centrándonos en la parte que tiene la encomienda de ejecutar el I+D+i del plan Estatal, CDTI, para quien no nos conoce estamos en el centro de Madrid, al lado de la puerta de Alcalá, somos trescientas (300) personas y llevamos desde el año 1977 acuñando el tema de I+D+i, de hecho nacimos con un crédito de cuarenta millones (40) del Banco Mundial. Nuestra misión es clara y transparente, traducir el conocimiento científico-técnico

en crecimiento económico y en crecimiento sostenible, ese es básicamente nuestro objetivo de primer nivel y pueden entender que, para nosotros, el I+D+i es un elemento instrumental, no es un fin en sí mismo, es instrumental.

La misión del CDTI es la de conseguir que el tejido empresarial español genere y transforme el conocimiento científico-técnico en crecimiento sostenible y globalmente competitivo.

Esta misión que fue fijada hace ya muchos años coincide plenamente con los objetivos del Plan Estatal que entre otros son:

- Activar la inversión privada en I+D+i y la capacitación tecnológica del tejido productivo; en España está por debajo de la media europea.

- Impulsar el potencial impacto de la Investigación y la Innovación en beneficio de los retos de la Sociedad.

- Coordinación de sinergias e implementación eficiente de políticas de I+D+i y financiación a nivel regional, estatal y europeo.

INSTRUMENTOS DE FINANCIACIÓN DEL CDTI

¿Qué hacemos en el CDTI? Hacemos financiación, tenemos varias fuentes de financiación: los presupuestos generales del Estado, el fondo FEDER; este año pasado también tuvimos el fondo marítimo de pesca, delegación del Ministerio correspondiente y también fondos CDTI. Una parte de nuestras ayudas son créditos que el CDTI mantiene circulando en el sistema desde el principio de los tiempos. Pero, no solamente hacemos eso, también tenemos una actuación clara promoviendo la internalización de I+D+i. Tenemos una red exterior de treinta y un nodos de diferentes países, desde Australia a Canadá y desde Chile hasta Corea, que están generalmente localizados, o bien en la embajada, o en la oficina comercial; y cuyo objetivo es apoyar a las empresas y usuarios para poder establecerse o colaborar con el país de destino. Aparte de esto, la característica fundamental del CDTI es que no solo financiamos, sino que damos asesoramiento experto y servicios complementarios a las empresas y otros actores del panorama de I+D+i. Es fundamental, nosotros no funcionamos con una convocatoria donde las empresas, los usuarios, presentan sus proyectos, se evalúan y luego dan su resultado; nosotros tenemos una interacción constante con los agentes de la I+D+i, entendemos qué necesitan y a partir de eso, montamos un programa; es decir, ese es el elemento diferenciador del CDTI, no solo financiamos sino que también damos asesoramiento experto.

ÁREAS DE ACTIVIDAD. EL CDTI Y LA I+D+I

Tenemos cuatro áreas fundamentales de actividad en la acción del I+D+i.

• Financiación de proyectos de I+D+i.

- Evaluación y financiación.
- Emisión de informes motivados para deducción fiscal.

Es nuestra área frontal, puede ser un 70% de la actividad en cuanto a función directa. Ahí evaluamos proyectos y, sobre la base de la valoración técnica y la valoración financiera, se da ayuda a la empresa con un tramo no reembolsable que puede andar entre el 20 y el 33%. Muy importante, emitimos informes motivados para deducción fiscal. En esta área de actividad se financian proyectos sobre la base de sus méritos tecnológicos, no tenemos ningún sector de actividad privilegiada, es decir, se financian de abajo-arriba a propuesta de la empresa o del actor que presenta el proyecto.

• Apoyo a la creación y consolidación de empresas de base tecnológica.

- NEOTEC
- INNVIERTE

Aquí se financian empresas, evidentemente nosotros somos un ente público y eso significa que tenemos la obligación de recuperar los créditos que asignamos y eso para muchos actores de I+D+i no es posible. Imagínense un emprendedor que tiene una idea brillante y que realmente no tiene ningún tipo de capital, ni ningún tipo de activo que pueda actuar de garantía para un crédito. Eso lo entendemos y por eso creamos esa parte que tiene que ver con la financiación de empresas de base tecnológica y que tiene que ver también con la participación en empresas de base tecnológica, donde el CDTI participa en el capital de la empresa. En este caso no se financian proyectos, sino empresas con un proyecto.

- Gestión de programas internacionales.

  - Cooperación tecnológica (Programa Marco, Eureka, Iberoeka, Eurostars, etc.).

  - Apoyo a la transferencia de tecnología (Red Exterior) .

Un tercer ámbito de actividad es la gestión de programas internacionales donde pretendemos internacionalizar la I+D+i y, por supuesto, generar crecimiento económico a través de la exportación de tecnología española y el apoyo a la transferencia tecnológica a través de nuestra red exterior de treinta y un puntos.

- Aeronáutica, Espacio y Retornos Tecnológicos.

  - I+D+i aeroespacial.

  - Suministros tecnológicos (CERN/ESRF, Hispasat /Eumetsat/ Spainsat).

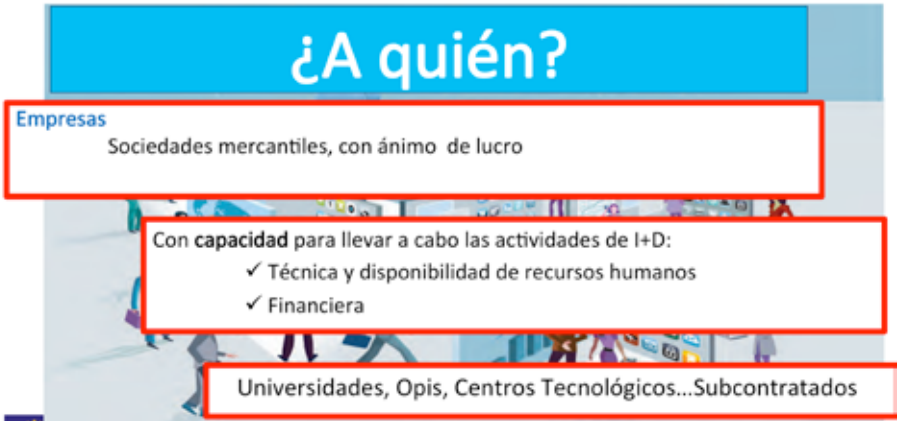
Y por último, la parte analógica de espacio y retornos tecnológicos que es la única parte vertical. Aquí no se financian los proyectos sobre la base de sus méritos tecnológicos sino sobre la base de un sector vertical que es la actividad aeroespacial y dentro de aquí, evidentemente, se financian aquellos que tienen unas tecnologías y unas características mucho más avanzadas. Porque, para poner límites, el CDTI, hasta la fecha hemos financiado más de trece mil empresas (13.000) y hemos aportado y movilizado más de veinticinco billones (25 b) de euros, sobre todo en la última etapa del centro. En el año 2017 se financiaron con financiación directa del orden de mil doscientos (1.200) proyectos con ochocientos cuarenta millones (840) de aportación. Y para este año 2018 la previsión es de llegar casi a los mil mi-

llones de euros (1.000 m) de proyectos de financiación con mil seiscientos cincuenta (1.650) proyectos financiados.

En cuanto a la financiación directa, la previsión de retornos en este año, está en el entorno de los setecientos millones (700) de euros, de los cuales –casi quinientos- vendrán de la gestión de los pilares dos y tres de Horizonte 2020 y el resto vendrá de diferentes programas relacionados con el espacio y la industria de la ciencia, que son grandes instalaciones científicas tipo ITER, tipo CERN, donde el CDTI participa obteniendo contratos industriales.

¿A QUIÉN FINANCIAMOS?

Básicamente a empresas y consideramos la mayoría de los proyectos, y consideramos también a universidades, centros tecnológicos, OPIs como subcontratados de estas empresas. La empresa tiene que tener una capacidad de poder llevar a cabo técnicamente el proyecto, y disponer de una capacidad financiera que le permita acometer el proyecto que nos presenta.



¿CÓMO FINANCIAMOS LAS EMPRESAS?, ¿CÓMO FINANCIAMOS LOS PROYECTOS DE FORMA GENERAL?

1. A través de la filosofía de ventanilla abierta, tratamos de que las empresas vengan a CDTI con una idea de proyecto y, entre las empresas y el actor que corresponda y el CDTI, montar un proyecto que después se evaluará en todo el centro. Aquí veo una colaboración con usuarios en el sentido de que, y son casos reales, muchas veces viene el usuario con un problema concreto, quiere un inhibidor para teléfono móvil, por ejemplo, o quiere una antena que quepa en el tapacubos de un coche;

viene el usuario directamente, nosotros entendemos las necesidades operativas del usuario y buscamos la empresa para montar el proyecto. Evidentemente la empresa tiene que tener interés en tecnología, de otra manera el esquema es complicado.

2. También trabajamos con convocatorias cerradas, porque al haber subvenciones nos obligan a ello en algunas circunstancias y aquí la participación es diferente; la interactuación con la empresa es más limitada y el CDTI hace básicamente una labor de evaluación y financiación de proyectos.

3. Evaluación técnica y financiera. Evaluación de la empresa y del proyecto. Tenemos una dirección de evaluación que evalúa los proyectos desde una perspectiva técnica y financiera y como resultado del proceso se asigna una ayuda, que básicamente corresponde a crédito más subvención, o en el caso de convocatorias generalmente es subvención para el proyecto con el que tratemos. Estamos en todos los sectores, desde el aeronáutico al de la seguridad, al de la producción y como les decía antes, se financian los proyectos sobre la base de sus méritos tecnológicos, esto siempre es una discusión bastante amplia, en el sentido de que si desde el CDTI se debería tener una orientación bastante más sectorial o más orientada a un sector actividad, pero por el momento, la actividad es horizontal; se financian todos los sectores.

El esquema fundamental de un proyecto CDTI es la transparencia, la flecha roja es para mí uno de los elementos troncales de nuestra actividad, es la interacción con la empresa, con el usuario para entender su necesidad y poder traducir esa necesidad en un proyecto de I+D+i. Esa fase puede llevar varios meses, es decir, tratamos de, una vez entendidos los requisitos de la empresa o del usuario, convertirlos en un proyecto robusto que pueda ser financiado por CDTI. A partir de ahí, hay un periodo de evaluación que puede ser de mes o mes y medio, y una ejecución que es típicamente empresarios entre los cuales hay un periodo de carencia y a partir del cual se

empieza a devolver la ayuda; y hay una parte que es la subvención. Yendo al plan estatal de I+D+i, el plan estatal se vertebra en diferentes programas, que se vertebran en subprogramas y a su vez en acciones estratégicas. La parte donde el CDTI es activo son estos dos que tienen que ver con el mundo empresarial y con la I+D+i orientada a retos, donde por cierto en el reto ocho figura la seguridad, protección y la defensa que me imagino es una de sus prioridades.

En el programa del plan estatal es donde figura específicamente el tema de seguridad y se vertebra a través de proyectos de I+D+i, acciones de dinamización, acción estratégica en salud en el caso del ISCIII y acción estratégica economía y sociedad Digital como en el caso de la antigua SESIAD.

Como les decía, hay ocho retos que van desde la salud, cambio climático, todos ellos modulados por estrategias sectoriales en los diferentes ámbitos hasta llegar al número ocho que es el reto de seguridad, protección y defensa sobre la base de la estrategia de tecnología e innovación para la defensa. En

4 PE I+D+i Orientada a los RETOS DE LA SOCIEDAD		
Proyectos I+D+i	Proyectos I+D+i C	AEI
Proyectos I+D+i	Proyectos I+D+i para la realización de **Pruebas de Concepto**.	AEI
Proyectos I+D+i	Proyecots de I+D+i **Retos Colaboración**	AEI + CDTI
Proyectos I+D+i	Proyectos para la incorporación de **Jóvenes Investigadores** (JIN)	AEI
Proyectos I+D+i	Proyectos de I+D+i **"Programación Conjunta Internacional"**.	AEI
Proyectos I+D+i	Consorcios de Investigacion Empresarial Nacional (CIEN)	CDTI
Acci. de Dinamización	Ayudas a **Plataformas Tecnológicas** y de Innovacion	AEI
Acci. de Dinamización	Ayudas para el fomento de **la Cultura científica y de la Innovacion**	FECIT + AEI
Acci. de Dinamización	Ayudas de **Colaboración Científico-Tecnica Internacional**	AEI
Accion Estratégica en SALUD 2017-2010		CIII
Accion Estratégica en ECONOMIA y SOCIEDAD DIGITAL 2017-2010		METyAD

resumidas cuentas hace referencia a la estrategia de tecnología e innovación para la defensa, a la estrategia de seguridad nacional, a la estrategia de ciberseguridad y a la acción preparatoria de investigación en defensa de la Unión Europea. Es un elemento fundamental, saben ustedes que en los últimos años hay alrededor de noventa millones (90) para esta acción preparatoria y el órgano de contacto por la Comisión Europea es la Dirección General del Ministerio de Defensa y para el siguiente periodo se lanzará un programa para dotar las capacidades de defensa, un elemento fundamental donde hay del orden de quinientos (500) millones al año en la ventana de capacidades y unos doscientos cincuenta (250) para la ventana de tecnología.

RETO 8: SEGURIDAD, PROTECCIÓN Y DEFENSA PRIORIDADES

- Intercambio y explotación inteligente, segura y masiva de información.
- Nuevos conceptos y prestaciones mejoradas de vehículos y plataformas.
- Mitigación de nuevas amenazas en materia de seguridad pública.

Reto 8: Seguridad Protección y Defensa

Objetivo: Reforzar la seguridad pública y capacidades de defensa:

Referencias a:

- Estrategia de Tecnología e Innovación para la Defensa
- Estrategia de Seguridad Nacional
- Estrategia de Ciberseguridad
- Acción preparatoria de investigación en defensa de la Unión Europea

- Seguridad y resiliencia de infraestructuras críticas.

- Metodologías y herramientas avanzadas de modelado y simulación, y de gestión integral de la seguridad.

- Investigación en ciencias jurídicas asociadas a los avances tecnológicos registrados y de futuro.

FINANCIACIÓN CDTI EN SEGURIDAD Y DEFENSA (2015-2017)

En el periodo 2015-2017 se han financiado con nuestros instrumentos: veinte proyectos, con una ayuda CDTI por encima de los trece (13) millones de euros, con un presupuesto global de los proyectos de dieciocho con sesenta y seis (18,66) millones de euros, lo cual supone un 0,55 % de la financiación CDTI

Estas cifras son realmente bajas y desde luego no corresponden a la importancia que tiene la seguridad dentro de la sociedad y estamos a su disposición para poder incrementar esta cifra que insisto, nos ha sorprendido por lo baja.

INTERNACIONALIZACIÓN DE LA I+D+I CON EL CDTI

Dentro de la Internacionalización tenemos dos canales:

- Financiación directa: donde hay una financiación descentralizada de las diferentes agencias de I+D+i.

- Financiación indirecta: que básicamente es la gestión de retornos y H2020; programa Horizonte Europa.

Existen treinta y un puntos de contacto por todo el mundo, y cada delegado del CDTI cubre su zona geográfica, por ejemplo, tenemos uno en la punta sur del continente africano, pero esta persona cubre otros países del entorno Kenia. Estos delegados son un apéndice de CDTI, están a disposición para cualquier tipo de contacto o consulta que quieran. Conocen perfectamente los sistemas de I+D+i del país de destino.

Tenemos un proyecto de I+D+i internacional; e imagínense que tenemos interés en colaborar con un país determinado: Colombia, Argelia,.. Y existe también un interés del país de destino. Lo que hacemos es entrar en contacto con la agencia de destino y montar un proyecto donde cada agencia financia la parte correspondiente a su empresa, usuario, etc. Es una financiación descentralizada, cada país paga su parte y, también, es una aproximación de abajo-arriba. No hay, a priori, una distribución de actividad, sino que la actividad se propone directamente en cada una de las convocatorias o programas. Hay una solicitud, habría un sello de aprobación que ratifica que la actividad tiene un carácter internacional y, después, cada agencia financia su parte del programa correspondiente. Es una actividad muy interesante porque permite a empresas españolas instalarse en países extranjeros, en países donde hay intereses comerciales y también permite que los usuarios entren en contacto con usuarios de otros países para poder montar proyectos de I+D+i conjuntos.

FINANCIACIÓN INDIRECTA

La financiación indirecta el H2020, es una financiación sin igual a nivel nacional:

Subvención:

- Acciones de I+D: 100% del total de costes elegibles.
- Acciones de Innovación: 70 %.
- Tarifa plana para costes indirectos: 25%.

No van a encontrar nunca un programa nacional de esta intensidad de ayuda porque los Estados nacionales estamos sometidos a la reglamentación o ayuda del Estado y la Comisión no; y eso le permite subir el tipo máximo de ayuda hasta esos límites que son inalcanzables.

Esta es la distribución:

Sociedades seguras tiene mil setecientos (1.700) millones de euros en números redondos, y desde CDTI ofrecemos dos tipos de servicios:

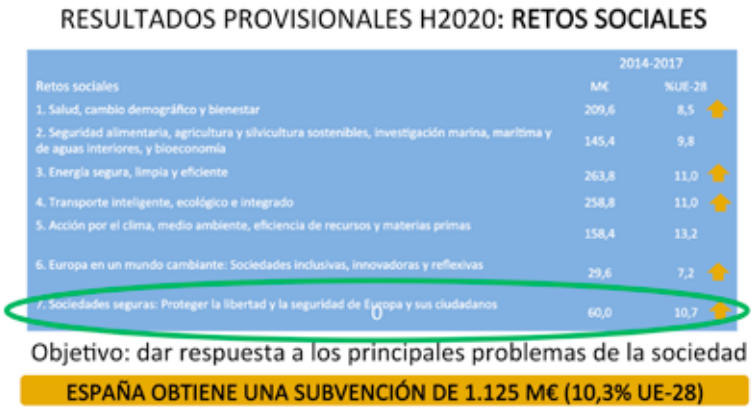
- Un asesoramiento y orientación a través de los MPTs que les ayudan a votar propuestas y que actúan con ustedes de forma continua.

- Una representación en el comité de gestión donde tratamos de influir en los diferentes aspectos de gestión del programa, plan de trabajo, etc.

Tenemos una participación realmente satisfactoria, hasta la fecha, somos el cuarto país en cuanto a retorno y hemos movilizado más de dos mil ochocientos (2.800) millones de euros. Ahora mismo, el nivel de retorno ronda el 10%, el 11,7% si tenemos en cuenta los pilares dos y tres que son los que se gestionan directamente. También tenemos un papel importante de liderazgo, aparte del retorno industrial que se pueda derivar de la participación en el H2020, hay un retorno relacional; establecer relaciones con otros usuarios, con otros Estados miembros, con otras empresas que de cara al futuro permiten montar propuestas conjuntas. Y, ese retorno relacional tangible lo tenemos en cuenta a la hora de apoyar propuestas en el marco del H2020.

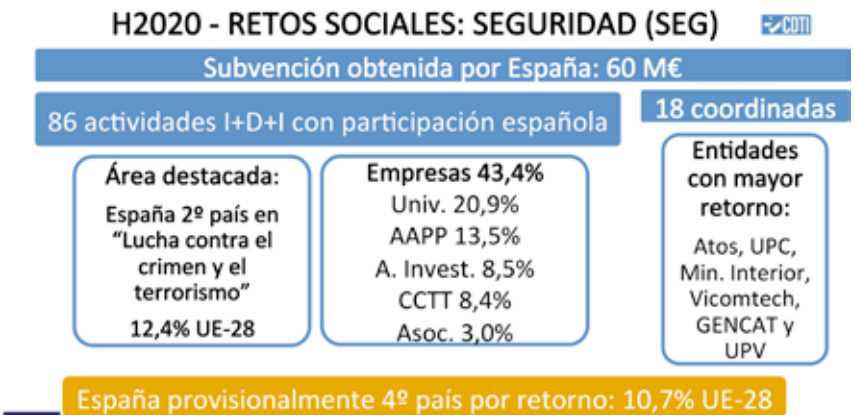
H2020. RETOS SOCIALES: SEGURIDAD

La imagen, presenta los retornos del H2020 por áreas temáticas, y en el caso de seguridad, segmentado por tipo de actor. En particular, en el caso de asuntos sociales y seguridad, la subvención obtenida por España hasta la



fecha es bastante relevante, sesenta (60) millones de euros, lo cual supone un 10,7 en términos de retorno. Somos el segundo país de la Unión en este programa en el *topic* de lucha contra el crimen y el terrorismo un 4% de participación; y tenemos una distribución segmentada en cuanto a actores que es la siguiente:

Empresas, casi un 45% que es el actor que más participa, seguido de universidades con casi un 21%; administraciones públicas, 13,5%; acciones de



investigación 8,5% y centros tecnológicos 8,4 % y asociaciones 3%. En cuanto a las entidades, España coordina dieciocho de estas iniciativas y las entidades con un mayor retorno son Atos de Cataluña, UP de Cataluña, el Ministerio del Interior,Vicomtech, que lidera un programa, siendo esta una de las razones por las que está ahí la Generalidad de Cataluña y la UPV del país vasco.

Este es el H2020, se acaba prácticamente pasado mañana y se está planteando ya la siguiente iniciativa de programa europeo, que se va a llamar Horizonte Europa. El motivo sigue siendo el que disparó el H2020 y es que Europa tiene un 7% de población mundial, tenemos el 20% de la inversión mundial en investigación y desarrollo, tenemos 1/3, el 3%, de las publicaciones de investigaciones científicas y, sin embargo, en el tema de I+D+i, en el tema del emprendimiento, en el tema de convertir este conocimiento en negocio fracasamos; estamos por debajo de Corea, Japón, EEUU y tenemos una inversión de un 1,3 % en temas de RD dedicado a negocios. Estas cifras, realmente están configurando la estructura del nuevo programa marco de Horizonte Europa. En números redondos, cien millones (100) dependen también de las condiciones económicas, cien millones sin Reino Unido, es decir, el incremento ha sido superior al que se esperaba, de unos ochenta mil (80.000) a cien (100.000) mil, pero quitando una participación del orden del 12% de Reino Unido.

¿Dónde va a estar seguridad? Se está discutiendo pero el planteamiento actual es que va a estar en los *clusters*. Hay un *cluster* que tiene que tratar con sociedades inclusivas y seguras y ahí parece que va a estar. A nosotros, básicamente no nos gusta que un tema como la seguridad, que tiene una personalidad propia, esté en un *cluster* con sociedades inclusivas; creemos que el protagonismo de la seguridad debe ser mucho más patente y estamos trabajando en los canales adecuados a través de los contratos de la Comisión, para tratar de revertir la situación actual que es esta.

El 7 de junio de 2018 salió la propuesta para Horizonte Europa y desde aquí hasta finales del año 2021, se estará negociando con unos milestones para preparar los borradores. El calendario es bastante ajustado.

ACTUACIONES DEL CEDTI EN MATERIA DE ESPACIO

Somos la delegación de España en la ESA desde el año 1986, y hacemos tres tipos de actividad:

- Estrategia y punto focal institucional para Espacio. Tenemos una parte de estrategia donde además actuamos de consultores de diferentes unidades de la Administración.
  - Plan Estratégico 2007-2011. Agenda 2020 (en preparación).
  - Defensa intereses de España en la UE.
  - Presidencia de España en ESA.
  - Acuerdos con otras agencias espaciales .
  - Consejo al Parlamento.
  - Coordinación con otras unidades de la Administración: Mº Fomento, Mª Defensa, MAPAMA, Autoridades autonómicas, locales.

- Gestión programas
  - Programas de la ESA.
  - Programas de la UE.
  - Acuerdos Cooperación.
  - AEMET/Eumetsat.
  - Hispasat.

- Gestión Proyectos Espaciales

En el año 2004, el Ministerio de Industria, encargó al CDTI el desarrollo y puesta en operación de un satélite; han pasado catorce años y el satélite está ya construido, se lanza el año que viene y tiene como característica la de servir de catalizador del desarrollo espacial. Realizado porque un contratista principal español, desarrollará, en el mercado público, aplicaciones con datos de satélite y, en estos momentos está por hacer. Se ha planteado de la siguiente forma, a partir del lanzamiento, finales del año 2019, los datos de este satélite serán gratuitos para las administraciones públicas y, desde el CDTI se tratará de financiar las aplicaciones de forma que las diferentes administraciones puedan utilizar, en el desarrollo de sus políticas, datos y aplicaciones derivadas del satélite. Satélite nacional óptico con 2,5 metros de resolución y con un alcance de 60 kilómetros por ocho coberturas completas de la península ibérica.

Además, se gestiona por delegación de la Comisión Europea, el programa Spece, programa de vigilancia y seguimiento espacial, que tiene un importante componente de seguridad y, también, financiamos otros programas que tienen que ver con la Comisión.

Ahí hay una representación de los diferentes orígenes de fondos de la actividad espacial en España; y lo que figura en esa sección es la parte que gestiona CDTI, un 85% del total de la actividad. Desde este punto de vista de actividad relacionada con la seguridad, el primer punto del satélite Ingenio que estará volando el año que viene, tendrá datos gratis para las administraciones durante al menos tres años. La idea es que ustedes puedan utilizarlo para hacer aplicaciones que les sirvan en su operativa del día a día.

El sistema SST que tiene que ver con el seguimiento de basura espacial, donde se ha desarrollado unos sensores ópticos, da tres servicios:

- Servicio de colisión en órbita.

- Servicio de fragmentación en órbita. Hace año y medio, cayeron en Murcia una serie de elementos, de basura espacial, y trozos de un cohete. Con este sistema se puede anticipar su caída; de hecho, este mes de marzo 2018 se seguirá, con este sistema SST, la reentrada de la estación espacial china Tiangong-1.

- Y el tercer elemento es el de los programas que está desarrollando la Comisión que son: Galileo, Copernicus -que es un programa dedicado a la observación de la tierra- y el programa Govsatcom, que es un programa que está orientado a las comunicaciones de defensa y seguridad.

En esta etapa actual, lo que la Comisión está haciendo es definir una serie de necesidades que los usuarios están listando: Ministerio del Interior, M. Exteriores, M. Defensa… y con esos requisitos lo que se hará es un catálogo de servicios. Se utilizarán todos los medios actuales, es decir, la filosofía de juntar y compartir, para dar servicios de defensa, seguridad y protección de infraestructuras críticas, a todos los usuarios. Es un tema que ahora está en fase de definición pero que, en pocos meses, empezará a tomar forma.

El satélite Ingenio d133, son ochocientos (800) kilos de satélite, con un instrumento cromático en bandas rojo, verde y azul; el infrarrojo dará imágenes de una resolución PAN de 2,5 m, con un anchura de pasada de 60 km.

El S Espacial, es una iniciativa de la Comisión que ha delegado en cinco agencias espaciales: la francesa, la alemana, la inglesa, la italiana y el CDTI.

En cuanto a las infraestructuras que se han desarrollado hasta la fecha, podemos mencionar el radar de Santorcaz, que está en Guadalajara y el radar S3TSR que se está desarrollando en Morón de la Frontera. Es un radar escalable y del que queremos desarrollar una segunda generación antes del año 2020. Es una iniciativa de la Comisión con la filosofía de dar servicios a todos los usuarios gubernamentales para la seguridad y defensa. En España tenemos dos operadores de satélites de comunicaciones y ellos serán el menú de servicios que ofrecerá este programa.

En el año 2007, el CDTI se embarcó en el desarrollo de una UVE que se situó en la escuela de Salamanca y que lo está gestionando el Ejército del Aire. Está previsto que tenga un programa de mejoras con diferentes características, en particular el control vía satélite y, desde luego, la intención es que se ponga al servicio de todas las Fuerzas de Seguridad del Estado.

TRUNO DE PREGUNTAS

Pregunta en sala: José Francisco López, jefe del servicio de innovación y desarrollo de la Policía Nacional.

Quería hacer una pregunta doble: la primera es relativa a qué interacción tiene el CDTI en relación con la compra pública innovadora, que para nosotros los policías es un tema que está muy valorado. Se ha hecho algún intento pero hemos fracasado y nos interesaba saber cuál es exactamente el sistema de financiación o qué aporta el CDTI a la compra pública innovadora o cómo podemos beneficiarnos de ello.

La segunda parte de la pregunta es relativa a los fondos CDTI, las administraciones públicas ¿podemos acceder de alguna forma a esos fondos CDTI? y luego la pregunta de curiosidad es relativa al tema satélite, ha dicho que el Ingenio va a tener tres años de uso para las administraciones públicas de forma gratuita con la finalidad de desarrollar aplicaciones o de interés nuestro; esto ¿cómo se va a gestionar? ¿se va a gestionar a través del centro de Torrejón, con el contacto directo con las administraciones públicas o cómo se va a hacer?

Responde: Juan Carlos Cortés Pulido

Nosotros en CDTI lanzamos en el año 2009-10 la Compra WIT Innovadora, entendiendo como tal aquella que iba a cubrir una necesidad en las administraciones. La idea era tener un instrumento financiero que supusiera cubrir una necesidad operativa y a su vez permitir a la empresa tener un cliente lanzador. Trabajamos mucho con la Comisión Europea, de hecho, la Comisión metió este instrumento en su portfolio de actividades y tenemos dos instrumentos, el CDTI y el Ministerio. El CDTI financia la parte de I+D+i que tiene que ver con la compra pública innovadora a través de un programa que se llama Innodemanda y que trata de utilizar un Fastrac, un pasillo rápido en CDTI para acompasar la necesidad operativa de las administraciones con el modus operandi de CDTI, de manera que se llegue a un calendario de evaluación compatible con los calendarios de la administración para este tema.

Es importante decir que, hasta la fecha puede haber habido cifras en el campo de la salud pública y también en el campo de la seguridad, de hecho, ha habido programas de compra pública con defensa; ha habido un radar modulable y escalable, realizado hace cuatro años; y donde falla este instrumento es en el procedimiento, la licitación que tiene que lanzar la administración. Cuando se lanza, el tema va sobre raíles, pero no podemos hacer

nada si no hay una iniciación y que es la que tratamos de coordinar. Decía que en el CDTI tenemos un instrumento que Innodemanda y otro en el Ministerio; el del CDTI financia la I+D+i de la empresa en este ámbito y el del Ministerio que se llama Innocompra, lo que se hace es financiar al comprador; y se hace a través de créditos; el Ministerio financia al comprador, es decir, tenemos la doble actuación. El CDTI a través del desarrollador y el Ministerio a través del comprador.

Segundo cuestión, fondos CDTI, las administraciones únicas pueden participar en los programas CDTI en la mayoría de ellos a través de subcontratación de empresas y esto es un esquema que ha funcionado y lo que comentaba antes es un caso real, aquí viene un operativo: Guardia Civil, Policía Nacional, de Defensa, con un problema operativo y nosotros tratamos de buscar una empresa a la que le puede interesar el desarrollo de tecnología en temas de encriptación, en temas de comunicaciones; y ahí si funciona. Pero, directamente en la mayoría de los programas de financiación directa, las administraciones tienen que venir de subcontratados de las empresas. En otro ámbito, como puede ser el programa marco o de retornos indirectos, está abierto a cualquier actor, y ahí las administraciones pueden ir, de hecho, como participantes. En el caso del reto 8 de seguridad, hay una parte de retorno que es un 13% que son administraciones públicas y que es el Ministerio del Interior.

Y por último, el tema del satélite no está cerrado, la situación actual es que ha habido muchos problemas de desarrollo, muchos problemas con el instrumento, nunca se había hecho en España y ha retrasado el programa bastantes años; la operación se va a delegar a Hisdesat que lo va a operar por delegación del CDTI, y la idea es que esos datos sean accesibles a través de un portal de administraciones. Tendremos que hacer una labor de comunicación para que todas las administraciones sean conscientes de esta posibilidad, pero el proceso todavía no está cerrado, aunque se parecerá mucho al siguiente, un portal donde tendréis acceso a los datos, donde tendréis acceso a decir qué actividad, qué datos, a qué hora, de qué territorio lo queréis y luego una serie de aplicaciones, que eso sí puedo anticipar que lo financiaremos, será dentro de los fondos de la Unión Europea con el objeto de convertir esos datos en información; pero el procedimiento todavía no está habilitado.

Pregunta en Sala: en lo relativo a Ingenio ¿cómo casa Ingenio con Copernicus? Porque ahora mismo hasta Frontex, en breve, empezará a ofrecer imágenes Copernicus, entonces ¿será en la misma red?

Responde: Juan Carlos Cortés Pulido
Sí, Copernicus es a nivel nacional, de capacitación industrial, tecnológica

y de utilización de aplicaciones. Copernicus se ha lanzado en el marco europeo hace años, da los datos gratis, que imagino tu pregunta va por ahí, pero los datos ópticos equivalentes a los de Ingenio, son de veinte metros. Nosotros tenemos una mayor resolución, son dos metros y medio. No obstante, en Copernicus hay dos tipos de misiones, las precursoras y las colaboradoras. Ingenio tiene el sello catalogado de una misión que contribuye a la iniciativa Copernicus; es decir, parte de los datos que venda Hisdesat como operador; y el cliente último será la Comisión dentro de sistema Copernicus.

PLANES DE ACCIÓN DE TRANSFORMACIÓN DIGITAL EN EL MINISTERIO DEL INTERIOR

JORGE ÁLVARO NAVAS ELORZA
Subdirector General de Calidad de los Servicios e Innovación del Ministerio del Interior

Mi incorporación en el Ministerio del Interior ha sido en enero de este año 2018, y lo que me confiaron fue la realización de la planificación estratégica de la transformación digital del Ministerio. Mi primer objetivo ha sido hacer un plan de transformación digital, y hoy lo que os voy a contar es esta experiencia que llevamos en el plan de transformación digital y que funciona en dos fases. Desgraciadamente, para lo que es esta ponencia, la fase que hemos empezado es la transformación digital civil del Ministerio, está fuera por ahora todo lo que es la transformación digital de todos aquellos medios y servicios que afecten a la seguridad del Estado.

TRANSFORMACIÓN DIGITAL

Lo principal es saber qué es la transformación digital: es el proceso por el cual las empresas reorganizan sus métodos de trabajo y estrategias, para obtener más beneficios gracias a la implementación de las nuevas tecnologías. En el caso de las empresas privadas obtener más beneficios consiste en obtener más dinero.

En el caso de las organizaciones, los beneficios que se obtienen son beneficios para el Estado o para el ciudadano.

¿Cómo se hace la transformación digital? Se intenta, básicamente, aplicar las innovaciones digitales a la búsqueda y el aprovechamiento de oportunidades que antes no se incluían. Ejemplos:

- La automatización de los procesos, la informática. Desde que empecé a estudiar informática siempre te decían que los ordenadores son tontos pero muy rápidos, capaces de hacer muchas cosas rápidamente. Con la inteligencia humana se definen una serie de procedimientos, los famosos algoritmos y, con ellos, se puede hacer que un ordenador haga un montón de cosas repetitivas a una gran velocidad. Esa automatización es una clave en la transformación digital.

- Minimizar costos. Cosas que antes necesitaban días para completar un proceso, con la automatización y la innovación se pueden hacer en segundos; con lo cual se minimizan costes.

- Maximizar la eficiencia. El objetivo de la transformación digital no es aplicar innovación o aplicar tecnología, por aplicar, sino es aplicar tecnología para tener gran ventaja y para hacer las cosas más rápidas.

- Inteligencia artificial. Al principio, se hablaba de la inteligencia artificial como la gran panacea, luego ha habido varios años en que no ha estado muy de moda y el año 2018 es, otra vez, el año de la inteligencia artificial. Cualquiera de las innovaciones que tenemos se basa en la inteligencia artificial, ahora está de moda. La inteligencia artificial si se mezcla con los avanzados sensores que tenemos para procesar todo tipo de información, ya sea en el caso policial -imágenes, videos, sonido, etc.- con esa inteligencia artificial, se pueden tener una serie de oportunidades que antes no existían, que ni siquiera se imaginaban, con lo cual, la transformación digital significa reorganizar los métodos de trabajo y las estrategias basadas en estas nuevas tecnologías.

TRANSFORMACIONES DISRUPTIVAS GLOBALES

Tenemos ejemplos en el mundo que son lo que llaman en innovación, la innovación disruptiva o las transformaciones disruptivas. Hay fenómenos impresionantes en el mundo que si hace cinco o seis años en una de estas charlas se cuenta, no se podría creer:

- La entidad que más pagos tramita no tiene ninguna oficina bancaria. (PayPal).

- La compañía que más personas aloja no tiene ni una sola habitación de hotel(Airbnb).

- La empresa que más viajeros traslada no es propietaria de ningún vehículo (UBER).

- La empresa que más productos vende en el mundo no tiene tiendas físicas (Amazon). Actualmente, Amazon está empezando con pilotos de tiendas físicas. En EEUU tiene algunos, son tiendas en las que se entra y directamente, o presentando un carnet o por bluetooth, te identifican, te llevas todo lo que quieras sin pasar por caja, y al llegar a casa llega el recibo con el importe a pagar. Son tiendas experimentales y toda una revolución. Con las primeras ha habido mucha polémica porque al principio como toda tecnología, no todo es perfecto, pero, es una revolución.

PERDER EL TREN DE LA TRANSFORMACIÓN DIGITAL

¿Qué pasa cuando se pierde el tren de la transformación digital? Que es un desastre, ejemplos:

- Las empresas líderes en fotografía (KODAK) no fueron capaces de adaptarse a la fotografía digital, aún siendo ellas las propietarias de las patentes técnicas.

- Las empresas líderes en los reproductores MP3 perdieron el tren del mercado frente al fenómeno iPod (SONY, llevaba años haciendo MP3, de repente aparece Apple, el IPOD; y se come un mercado enorme en cuestión de semanas). Estos ejemplos son para demostrar que el que pierde el tren de la transformación digital, se queda atrás y fuera del negocio.

- La mayor parte de las tiendas de discos y videoclubs tuvieron que cerrar tras el fenómeno del Streaming de audio y video. Antes en la Gran Vía, había tiendas enormes de discos, Discoplay, Escridiscos; ahora con el Streaming, la gente tiene las listas de spotify, youtube ..., usa lo que quiere y no compra discos y con los videoclubs pasa lo mismo.

TRANSFORMACIÓN DIGITAL EN LA ADMINISTRACIÓN GENERAL DEL ESTADO: ESTRATEGIA TIC

En la Administración General del Estado se siguen las pautas de la Unión Europea, que es la que va liderando las estrategias y se ha creado el plan de transformación digital de la Administración General del Estado y sus Organismos: la Estrategia TIC que constituye el marco estratégico global para avanzar en la transformación de la Administración. Es un documento que:

- Establece sus principios rectores, los objetivos y las acciones para alcanzarlos para que todas los Ministerios, todos los departamentos ministeriales lo implementen.

- Establece los hitos para el desarrollo gradual de la Administración Digital con un horizonte temporal hasta 2020.

- Incorpora las recomendaciones de la OCDE y se alimenta de la estrecha relación con los actos, políticas y servicios de la Unión Europea; alineándose con la agenda digital para España y la nueva estrategia de la Comisión Europea para el Mercado Único Digital.

La Estrategia TIC de la Administración General del Estado en España es un claro instrumento para la aplicación de las nuevas leyes 39/2015, de 1 de octubre, sobre el Procedimiento Administrativo Común de las Administraciones Públicas, y el 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público.

- Estas leyes vienen a configurar un nuevo escenario en el que la tramitación electrónica debe constituir la actuación habitual de las Administraciones en sus múltiples vertientes de gestión interna, de relación con los ciudadanos y de relación de aquellas entre sí.

¿Cuál es la clave de estas leyes? Que es un cambio radical; antes, utilizar la tecnología para hacer un tema de administración era algo que estaba tolerado, paralelo, se podía hacer y estaba admitido, y los que nos dedicábamos a hacer transformación digital y hacíamos procedimientos electrónicos, estábamos siempre con la legalidad de que esto tiene el mismo valor que el procedimiento papel y siempre apoyándonos en normativa.

¿Qué pasa ahora? Estas nuevas leyes dicen que por defecto todo es digital, todo es tramitación electrónica y lo raro va a ser el papel, es un cambio muy grande.

TRANSFORMACIÓN DIGITAL: LEYES 39 Y 40/2015

¿Y qué nos obligan las Leyes 39 y 40? En principio toda la tramitación tiene que ser electrónica tanto con el ciudadano como entre las empresa. Actualmente, todo se firma de forma electrónica, pero entre una administración y otra todavía se mueve mucho papel, y hay que transformarlo.

El Plan de Transformación digital de la Administración General del Estado y sus Organismos Públicos (Estrategia TIC 2015-2020) se elaboró teniendo muy presente en su momento los proyectos de las leyes 39/2015 y 40/2015, de forma que los principios rectores, los objetivos estratégicos, las líneas de acción y los hitos recogidos en el plan, persiguen facilitar la realización de las previsiones establecidas en las citadas leyes. Para ello, la

gobernanza de la administración digital en España, que lo lleva la Dirección General de Tecnologías de la Información y Comunicaciones, ahora se llama Secretaría General de Administración Digital, y con el cambio político, a lo mejor, dentro de unos meses cambia de nombre.

PLANES DE ACCIÓN DEPARTAMENTALES (CMAD)

- Para poner en marcha e implantar la Estrategia TIC es imprescindible que todas las Comisiones Ministeriales de Administración digital, elaboren un plan de acción departamental para la transformación digital que, siguiendo las líneas establecidas en la estrategia general, defina las pautas para la digitalización de sus servicios y el rediseño integral de sus procesos.

- Debido a la casuística particular del Ministerio del Interior, la CMAD ha decidido elaborar dos planes de acción de transformación digital (PATD) con dos ámbitos diferentes:

  - Medios y servicios específicos que afecten a la defensa, consulta política, situaciones de crisis y seguridad del Estado y todos los sistemas que manejen información clasificada, de acuerdo con lo dispuesto en la legislación reguladora de los secretos oficiales y en los Acuerdos internacionales. Este va a ser el ámbito de seguridad, en Defensa es el ámbito militar.

  - Resto de medios y servicios -que es el administrativo- .Yo entré en el Ministerio a mediados de enero de este año, empezamos los primeros grupos en febrero y este viernes, 13 de julio 2018, con la presencia de la Subsecretaria, se presenta para su aprobación por parte de la CMAD del Ministerio del Interior. Este plan es el primero que se ha abordado y va a suponer gran cantidad de cambios para la Policía, Guardia Civil, tráfico, para todos los centros directivos; porque van a tener que digitalizar muchos de sus procesos.

CENTROS DIRECTIVOS INVOLUCRADOS EN EL PATD

- Con unidades con infraestructuras TIC propias:

  - Secretaría de Estado de Seguridad.
  - Dirección General de Policía.
  - Dirección General de la Guardia Civil.
  - Dirección General de Tráfico.

- Secretaría General de Instituciones Penitenciarias.
- Dirección General de Protección Civil y Emergencias.

• Sin unidades TIC con infraestructuras propias (a las que da servicios TIC la Secretaría de Estado de Seguridad).

- Subsecretaría del Interior.
- Secretaría General Técnica.
- Dirección General de Política Interior.
- Dirección General de Apoyo a las Víctimas del Terrorismo.

METODOLOGÍA DE LA ELABORACIÓN DEL PATD

¿Cómo hemos definido el plan de acción?:

• Se han identificado diez áreas de trabajo, cada una de ellas liderada por un Centro Directivo. Por ejemplo, el área de identificación y firma electrónica la ha liderado la Dirección General de la Policía, porque son los más avanzados en temas de identificación electrónica.

• Se han definido encuestas para describir el grado de madurez actual de cada una de dichas Áreas de Trabajo en los distintos Centros Directivos del Ministerio del Interior.

• Con los datos de las encuestas se ha establecido un diagnóstico para cada Área de Trabajo. En las encuestas se preguntaba en qué estado se encontraba cada uno de los objetivos que teníamos que cumplir de las leyes 39 y 40.

• Y en función de ese diagnóstico, se ha generado un plan de acción, se han definido actuaciones (más de mil) encaminadas a mejorar el diagnóstico de modo que:

- Por una parte se consiga homogeneizar el nivel de administración digital de los distintos Centros Directivos, y

- Por otra parte, se avance en la transformación digital de todo el departamento y se adecúen los procedimientos a las Leyes 39 y 40/2015.

PRINCIPIOS RECTORES Y OBJETIVOS ESTRATÉGICOS

• Alineados con los principios rectores y objetivos estratégicos del PTD AGE 2015-2020:

- Orientar las acciones mejorando los aspectos de accesibilidad, usabilidad, simplicidad y seguridad, generando procesos homogéneos, interoperables y digitales de principio a fin.

- Buscar la integración de servicios o el desarrollo de proyectos comunes que proporcionen una imagen homogénea del Departamento.

- Monitorizar, evaluar y difundir de manera continuada los resultados y objetivos alcanzados como mecanismo de control y transparencia.

PATD "ADMINISTRATIVO" DEL MINISTERIO DEL INTERIOR

• Como temas importantes, en cumplimiento de la ley 39/2015:

- Derecho y obligación de las personas de relacionarse electrónicamente con las AA.PP. No puede haber un solo procedimiento administrativo, por ejemplo, un permiso de armas, que no se pueda hacer de manera electrónica.

- Asistencia en el uso de medios electrónicos de los interesados (OAMR, funcionarios habilitados), esto va a ser complejo y complicado para todos los organismos, por ejemplo, Policía o Guardia Civil; porque se supone que tienes que tener unas oficinas de asistencia en materia de registro, de manera que cuando alguien no sepa utilizarlo o no tenga medios para utilizarlo de manera telemática y hacer una petición electrónica para entrar en una portal web, pueda ir a una oficina de registro y un funcionario habilitado le tiene que ayudar a hacer ese trámite.

- Registros. Representación y registros electrónicos de apoderamientos. Todos lo conocen ¿Cuándo se utilizan? Cuando se quiere ascender y se presentan a un concurso, lo hacen en el registro; o para hacer un recurso, etc. Todo esto tiene que ser electrónico, hay que tener un registro de manera que de cualquier unidad de la comandancia más pequeña a cualquier subdirección del Ministerio, pueda ir la información electrónicamente.

- Uso de medios de identificación y firma.

- Solicitudes de iniciación, comparecencia de las personas, obligación de resolver y cómputo de plazos.

- Notificaciones electrónicas. Cuando alguien inicia un procedi-

miento, las leyes dicen que hay que personarse en la sede electrónica para obtener la respuesta.

- Emisión de documentos y sus copias, expediente y archivo electrónico.

PATD "ADMINISTRATIVO" DEL MINISTERIO DEL INTERIOR

En cumplimiento de la ley Ley 40, también unos temas que cumplir.

• Como temas importantes, en cumplimiento de la ley 40/2015

- Funcionamiento electrónico del Sector Público (sede electrónica, Portal de internet, sistemas de identificación de las AA.PP., actuación administrativa automatizada, sistemas de firma para la actuación administrativa automatizada, firma-e del personal al servicio de las AA.PP., aseguramiento e interoperabilidad de la firma-e, archivo electrónico de documentos).

- Gestión compartida de servicios comunes (sistemas de información y comunicaciones).

- Técnicas de colaboración (suministro de información, sistemas integrados de información administrativa).

- Intercambio de datos en entornos cerrados de comunicación, transmisiones de datos entre AA.PP. Hay una plataforma de intermediación de datos de manera que todos los Ministerios pueden ser consumidores o productores de información.

- Esquema Nacional de Interoperabilidad.

- Esquema Nacional de Seguridad.

- Reutilización de sistemas y aplicaciones de propiedad de la Administración y transferencia de tecnología entre Administraciones. Con la nueva ley salió un reglamento que especificaba que no se puede desarrollar nada que ya haya desarrollado la administración, con lo que se potencia intentar reutilizar desarrollos de otras administraciones y compartirlos. En general, la estrategia que se está llevando es que la Secretaría General de Administración General, elabora una serie de servicios comunes para que los use tanto Poli-

cía, guardia civil, interior, agricultura, política territorial, o sea, todos los ministerios que puedan utilizar esas aplicaciones comunes.

• Áreas de trabajo del PATD:

1. Registros. (Oficialía Mayor Subsecretaría)
2. Sitios Web (DGT)
3. Identificación y firma (DGP)
4. Intercambio de información (SES-SGSICS)
5. Tramitación electrónica de procedimientos (SES-SGSICS)
6. Gestión documental y archivo (SGAAD-SGT Subsecretaría)
7. Seguridad de la información (DGGC)
8. Infraestructuras y medios (SES-SGSICS)
9. Gestión de la información (SGCSI-Subsecretaría)
10. Formación (SGRRHH-Subsecretaría)

Es muy importante la seguridad en la continuidad de negocio ¿Qué es la continuidad de negocio? Que si un día por un tema de terrorismo vuelan El Escorial, y lo vuelan de verdad, al día siguiente o en unas horas, pueda estar funcionando la identificación de pasaportes, o lo que sea, en otro centro de respaldo. Y no solo que las máquinas funcionen, sino que si las personas se indisponen tiene que haber personas de reserva que conozcan los procedimientos y puedan hacer los trámites. La continuidad de negocio es algo muy complejo y que el Ministerio del Interior está aún por desarrollar, porque es un tema muy serio y donde creo que tenemos una debilidad grande; esto entronca con los sistemas de seguridad del Estado.

Por ejemplo, el sistema integral de vigilancia del Estrecho, tiene estaciones base que son radares, hay puestos cada x kilómetros y en esos puestos hay cámaras con infrarrojos, hay sensores, hay radares, hay de todo; y entonces, ahí y desde un centro de control se puede ver llegar una patera, si hay un narcotraficante, o cualquier otra cosa.

A estos equipos lo que les pasa es que la gente, "los malos", los tirotean con pistolas, con armas largas y a veces se estropean, y la tramitación administrativa es lenta, pasan tres meses sin arreglarse y en este tiempo se pueden ahogar los que vienen en una patera o se puede colar un terrorista. Son temas muy importantes los que atañen a asegurar la resiliencia de todos los servicios de seguridad.

PATD "SEGURIDAD DEL ESTADO"

- El siguiente plan a realizar cubrirá los medios y servicios específicos que afecten a la defensa, consulta política, situaciones de crisis y seguridad del Estado y los que manejen información clasificada, de acuerdo con lo dispuesto en la legislación reguladora de los secretos oficiales y en los Acuerdos internacionales.

- No existe aún un marco definido para este Plan, tenemos que lanzarlo. Yo tengo una serie de ideas, es lo que os he comentado aquí y es que los "malos" también han hecho transformación digital, entonces: los "malos" también se transforman y utilizan las tecnologías. Alguien que está muy de moda es Sito Miñanco, que utilizaba, hace poco, unos teléfonos móviles con encriptaciones, que por mucho Sitel que tengas, o lo que sea, es muy difícil encontrar la información. Hay que trabajar mucho en cifrado de comunicaciones y dispositivos e ir a la misma velocidad que los "malos".

- Cifrado de comunicaciones y de dispositivos.

- Blanqueo mediante criptomonedas. Es otro de los problemas grandes, y habrá que trabajar en las transacciones no solamente por el asunto fiscal, sino por el tema de seguridad.

- Manipulación de redes sociales (Elecciones). Que en las elecciones en EEUU, el Brexit, en Rusia, inyecten treinta mil tuits retuiteando un mensaje, es un fraude.

- Ciberataques. Con el 1 de octubre 2018, nunca ha estado el Ministerio del Interior tan atacado como los días cercanos al 1-O ante el ciberataque, hay que hacer ciberdefensa.

- Ciberterrorismo. Para esto hay dos soluciones la ciberdefensa y la informática ofensiva (es utilizar las mismas técnicas de los hackeres en su contra). Esto eufemísticamente en los contratos los llamamos agentes de control -meter un virus al malo y hackearle las comunicaciones en el teléfono o en el dispositivo que sea, antes de que él las cifre-.

Estos son los temas que estamos tratando y en la transformación de la seguridad:

- Formación: capacitación técnica del personal. Es muy importante porque no sirve de nada tener tecnología si no tengo personal formado.

- Enriquecimiento de soluciones en movilidad pero con la adecuada seguridad (Bastionado de equipos, identificación segura en equipos móviles, encriptación de dispositivos y comunicaciones).

- Aumento de la resiliencia ante fallos y ataques (ej. SIVE) Separación de entornos por nivel de seguridad, depende en qué entorno trabajes tendrás una seguridad u otra, hacer los some boxes, las cajas de arena, que es separar entornos de trabajo. La ofimática no tiene nada que ver con el entorno policial.

- Separación de entornos por niveles de seguridad.

- Gestión de datos y videos. Se necesitan máquinas potentes para poder gestionar todo tipo de información proveniente de los sensores, y esos datos hay que manejarlos en tiempo real para detectar problemas de seguridad.

- Inteligencia artificial: automatización de análisis de datos en tiempo real para detección de problemas potenciales de seguridad (integración y visualización de sensores):

  - Cámaras (reconocimiento facial, google glasses, …).

  - Sonido (Policía NY).

  - Vehículos conectados (reconocimiento de matrículas, etc.).

  - Predicción de criminalidad (mapas de tendencia de delitos).

  - Monitorización de redes sociales.

- Colaboración entre centros de mando y control.

MESA REDONDA: LUCHA CONTRA LAS AMENAZAS A LA SEGURIDAD

Modera: Luisa Maria Benvenuty Cabral.
Participan: Juan Carlos Cortés Pulido; Jorge Álvaro Navas Elorza; Anabela Gago

Interviene: Luisa María Benvenuty Cabral

Buenas tardes y gracias por tu interesante ponencia Jorge, algo conocíamos nosotros porque como bien saben la Unidad de Informática y Comunicaciones, de la Dirección General de la Policía, colabora estrechamente con vosotros y ha tenido su granito de arena en el plan de transformación digital.

Proyectos de los que has hablado, como la Ciencia de Datos de Nueva York (New York data science) la Policía, a través del inspector Camacho, autor del proyecto Veripol (sistema para la detección de denuncias falsas) ha estado trabajando con la Policía de Nueva York en ese proyecto de policía predictiva, que aunque parezca un poco ciencia-ficción, no lo es, estamos avanzando bastante.

Esta mañana he hablado del proyecto movilidad (en el que nos movemos la Policía): estamos definiendo los diseños de coches patrulleros donde se van a integrar, en las pantallas de navegación, todos los datos de la base de datos; se están definiendo los software, el parte de intervención que hace el patrullero que va a generar la inteligencia a pie de calle; se va a transformar la información de inteligencia para las unidades de investigación; y trabajamos en todos esos temas tan importantes como la firma digital, el reglamento europeo que va a tener un impacto fundamental en las transacciones; todo ello

con el fin de facilitar la vida a los ciudadanos europeos; porque, además, el DNI es la única certificación oficial de identidad digital. Es muy interesante, estamos avanzando sobre todo en el proyecto Redpol. Aquí hay representantes de la unidad de informática, y pueden imaginar que nos está costando, además, el cambio del papel cero implica un cambio de mentalidad cultural tremendo; yo que soy una fiel defensora de la firma electrónica me costó trabajo este cambio cuando llegue a la Jefatura Central de Logística; desde entonces hemos definido las unidades de registro, estamos avanzando pero nos va a costar mucho trabajo.

En esta mesa redonda con título "Lucha contra las amenazas a la seguridad", yo entiendo la seguridad como seguridad pública global, la seguridad no es solo la seguridad ciudadana global, que incluye la seguridad humana implica la seguridad ante catástrofes, no solo ante los grandes riesgos en materia de ciberdelincuencia, el ciberterrorismo, sino en todo lo que afecta a la seguridad de los ciudadanos. Y quería preguntar a Jorge ¿cómo nos va a afectar, o nos está afectando ya, el nuevo reglamento de protección de datos en estas actividades, porque es algo que nadie quiere tocar pero como ya estamos en él, queramos o no, el plazo ha llegado, y ya hay una valoración de una serie de riesgos. Las Fuerzas y Cuerpos de Seguridad del Estado estamos exentos, pero tenemos bases de datos que sí nos afectan, como la base de datos del DNI, por ejemplo, y tenemos bases de datos de gestión como Electra, que es toda la documentación de los ciudadanos extranjeros y comunitarios que son bases de datos documentales.

¿Cómo está incorporando tu departamento el reglamento?

Interviene: Jorge Álvaro Navas Elorza

Este tema me tocó en marzo de 2018, el Subsecretario me dijo que había que hacer algo al respecto, nos reunió a la Abogada del Estado, a la Secretaria General Técnica y yo tuve la idea de comentar que en el pasado había realizado auditorías de cumplimiento de la ley orgánica de protección de datos y me lo asignaron.

¿Y qué hemos hecho? Lo primero una estructura. El reglamento de protección de datos tiene una figura clave que es el delegado de protección de datos, por lo que hemos formado una estructura organizativa, de manera que los grandes organismos, los grandes centros tienen un delegado de protección de datos. La policía tiene un delegado de protección de datos, Guardia Civil tiene un delegado, Tráfico también e Instituciones Penitenciarias. Y, para todo el resto, hemos establecido que haya un delegado de protección de datos coordinador que, además coordina los otros cuatro, que soy yo. Nosotros lo que hacemos es que tenemos un rol de intentar hacer la mayor parte de la documentación y de proponer guías y directrices para la adecuación al reglamento.

Por ahora, hemos celebrado tres reuniones, hemos generado bastantes documentos y hay una hoja de ruta que la proporciona la Agencia Española de Protección de Datos para saber qué se debe hacer para adecuar el reglamento de protección de datos a una administración pública. Tiene una serie de puntos y los hemos llevado a cabo prácticamente todos, el primero es el de nombrar los delegados de protección de datos oficialmente y luego hay varios más, por ejemplo, con el Reglamento de Protección de Datos se pasa del concepto de fichero de datos personales a tratamiento de datos personales. Esto es un cambio fundamental. El fichero era básicamente que, una vez al año, los Ministerios o los grandes organismos, publicaban en un BOE los ficheros que utilizaban con una descripción genérica, y se olvidaban hasta el año siguiente. Así era cómo se trataba la protección de datos personales, declarándolos a la agencia y publicándolos en el BOE, indicando que la base datos del DNI incluye un campo de nombre, sexo, dirección y, por ejemplo, de grupo sanguíneo, con decir los campos que había y alguna información más, era suficiente.

Ahora, de acuerdo con lo que indica el Reglamento de Protección de Datos eso ya no vale. No tenemos que comunicar nada oficialmente a la Agencia Española de Protección de Datos pero es responsabilidad de cada Ministerio, o de cada organismo, o de cada empresa, generar una base de datos de tratamientos y ¿qué son los tratamientos?, todas las cosas que se hacen con los datos. Y aquí hay varios cambios porque no son solo tus datos; por ejemplo, para la Policía sería el DNI, que son también los datos que tú utilizas, pero que no son tuyos, ni se guardan en el sistema. Por ejemplo, en Policía se tienen datos de funcionarios de cuerpos generales que están en el registro central de personal. Antes, esos datos del registro general de personal los declaraba el Ministerio de Hacienda o Función Pública, era su fichero y aunque la Policía los utilizara, la Policía no tenía que declarar. Ahora sí, cada organismo, cualquier consulta que haga, de cualquier dato, ya tiene la responsabilidad y tiene que definir un tratamiento: simplemente consulta, cotejo, consulta de antecedentes del registro de personal; es decir, cualquier cosa que utilicemos tenemos que definir un tratamiento y para ese tratamiento hay que rellenar una base de datos y responder a una serie de preguntas.

¿Qué datos tiene, son datos ordinarios, o datos de clasificación especial? Porque hay datos de clasificación especial como puede ser: opiniones políticas, preferencias sexuales, también temas biométricos; en fin, hay que definir una serie de tratamientos y donde antes teníamos un fichero puede que afloren seis o siete tratamientos distintos y para cada tratamiento hay que decir lo que se hace con los datos, a quién se ceden, etc. Además, hay que hacer un análisis de riesgo y ver qué impacto sobre la privacidad tendría el robo de alguno de esos datos; porque, en el caso de robo hay una serie de niveles, cada dato tiene un nivel de riesgo, por ejemplo: un daño menor a la persona,

o un daño grave en la reputación de la persona, o un daño irreparable, o incluso daño físico en la persona; y en función de esto elaborar el análisis de riesgo. Si el tratamiento maneja quinientos datos, eso es cinco millones de datos, lo que supone que la labor es diseccionar todo lo que hace una organización y generar la base de datos de tratamientos. En el Ministerio hemos utilizado una aplicación, que por ahora tenemos en plantillas Excel, que nos ha venido del antiguo Ministerio de Empleo y Seguridad Social, que tiene unas plantillas con una serie de preguntas y respuestas con las que, por un lado, defines cada tratamiento: la legitimación, la base jurídica para hacer ese tratamiento, a quién se ceden los datos..., y luego hace una serie de preguntas sobre el análisis de riesgos y evaluación global y, automáticamente, genera una hoja de resultados con las medidas de seguridad que hay que adoptar en función del análisis de riesgos que se ha generado.

Es una tarea bastante grande, nosotros tuvimos una reunión la semana pasada, teníamos definidos por completo con los análisis de riesgos y la evolución de impacto, ochenta y cuatro tratamientos en el Ministerio. En la Policía llevan relativamente pocos y ha habido un problema porque el delegado de protección de datos ha pedido la dimisión por la responsabilidad que implica, con la organización y con la dirección como dice la agencia y el reglamento europeo; y en su caso alega que no se cumple.

Guardia Civil, sé que han empezado a trabajar, tienen un equipo humano grande y por ahora no han dado ningún tratamiento. Secretaría de Estado de Seguridad ha definido bien los que entran en el paraguas de la directiva de seguridad, y los que entran en la directiva de protección de datos del DNI. Porque el DNI puede ser por un lado de seguridad, para mi entra dentro del reglamento y han definido ya unos cuantos tratamientos y el de subsecretaría va bastante avanzado. Toda la política interior, víctimas del terrorismo, Secretaría General Técnica ..., han definido los tratamientos, se han analizado y se saben las medidas de seguridad a tratar.

Paralelamente, tenemos varias actividades, y una de las más importantes del reglamento es la información al ciudadano. El artículo 13 del reglamento dice que cuando se recaba cualquier acto de personal se tiene que informar al ciudadano de quién va a tratar los datos, cómo se puede reclamar y evitar que se utilicen los datos. El máximo exponente de esto ha sido la aplicación móvil de la liga de futbol, lo voy a explicar: desde el 25 de mayo 2018, es obligatorio informar, entonces ahora, los ciudadanos, al llamar a los servicios de información para contratar un seguro o hacer una gestión con su ayuntamiento lo primero que se escucha son cinco minutos de locución en los que se informa del procedimiento de protección de datos, se van a tratar sus datos en el Ayuntamiento; si continúa se considera que está dando el consentimiento, si quiere reclamar tiene que llamar a un número de teléfono

que le proporcionan o a un correo. Es obligatorio en cada aplicación, en cualquier página web, se tiene que exponer la información de lo que se hace con los datos. La aplicación de la liga, llevaba seis o siete meses funcionando, una aplicación móvil que se descarga y en teoría sirve para ver los resultados de los partidos y noticias de futbol. Y los que hicieron la aplicación y al publicar la información, aparece que ellos, sin que se supiera, arrancaban el micrófono del móvil, arrancaban la localización del móvil, se conectaban con un servidor y mandaban una grabación, con la localización del móvil, a un servidor de la liga para saber qué canal se estaba emitiendo, si canal plus, o gol TV, o un partido codificado en un bar.

El motivo era saber si se estaba transmitiendo el partido desde un local sin licencia; en definitiva, estaban utilizando a la gente para ser inspectores. Este tipo de prácticas, en caso de que se informe claramente llevaría a que un gran número de personas rechazaría utilizar la aplicación y el tema ha sido revelado a la opinión pública por el reglamento. Hay muchos ejemplos más, que utilizan nuestros datos para un montón de cosas y el reglamento obliga a que se comunique. Hay una inspección, viene la agencia de protección de datos a la liga y les pide la base de tratamientos, y qué hacen, y no dicen que están activando el micrófono.

Actualmente, cualquier portal, cualquier cosa que se haga, hay que comunicarla al usuario, un ejemplo que suelo poner es que cuando se llama a un operador móvil para una consulta, el operador móvil lo primero que hace es una segmentación: mira el número de teléfono, si el gasto al mes es menor de diez euros te pone al final de la cola con el operador que acaban de contratar la semana pasada; si gastas entre diez y treinta euros te pone más o menos y si gastas más de treinta euros te ponen a un operador con doctorado.

Eso es totalmente válido, pero ahora hay que informar. En todos los sistemas de información cada vez que se hace una segmentación, o un tratamiento, hay que informar. En el reglamento cualquier cosa que se haga, se informa, ¿por qué? Porque si se hace algo que no se debería, hay que dejar de hacerlo. Esta es la política de la Unión Europea.

¿Trabajo que hay que hacer en el Ministerio? Para los temas civiles nada de esto, pero cualquier cosa que se haga se informa. El reglamento lo que pide es un análisis de todo lo que se haga con los datos personales de la gente, en cualquier ordenador que se utilice, que se documente y en función de los riesgos que pueda tener que se protejan de la manera que sea.

Y, el ejercicio de derechos, cualquier ciudadano puede ejercitar sus derechos del reglamento de protección de datos y puede decir que se borren. A lo mejor no se pueden borrar datos de que alguien ha estado en la cárcel,

pero si se puede pedir "el derecho al olvido" si hay algo malo, a Google se le puede decir que cuando se busque su nombre, se olvide de esa información. Es lo que se ha hecho con gente famosa y con este tipo de cosas.

Interviene: Luisa María Benvenuty Cabral

Yo quería hacer un inciso sobre la Google glass. La Policía china esta utilizando una tecnología muy barata, con un router,visiona las caras y manda la imagen contra la base de datos policiales y si tiene un mac, un antecedente policial, se pone en rojo y lo detienen. Funcionan muy bien porque tienen un margen de error muy escaso, no es una tecnología cara. Aquí, podemos chocar con el tema de privacidad de datos en algún aspecto, tendríamos que ver los referentes legales.

Interviene: Jorge Álvaro Navas Elorza

Una empresa privada sería siempre ilegal, un Estado estaría legitimado y de hecho en las fichas que hacemos de tratamientos hay una serie de preguntas como ¿almacenas datos biométricos como reconocimiento facial? Contesta SI o NO. En caso afirmativo hay que cumplir una de las condiciones, que seas una de las Fuerzas de Seguridad del Estado.

Interviene: Luisa María Benvenuty Cabral

Pero dependiendo de en qué momento esté la sociedad española, a lo mejor es más o menos sensible a esto, y por lo tanto ya entra en otras cuestiones políticas.

Quisiera hacer una pregunta a Anabela o Juan Carlos, sobre una de las prioridades estratégicas en materia de seguridad y de los retos más importantes que tenemos en materia de seguridad, que son, indiscutiblemente, los movimientos migratorios. España es una gran frontera Schengen, no solamente una frontera aérea sino una frontera mediática. Jamás habíamos visto una avalancha tan grande de movimientos migratorios y de entradas por la vuelta a las rutas tradicionales, a la veda del Estado Libio. Estamos volviendo a ver esa hilera humana desde Argelia hasta Marruecos; y también es una cuestión política porque no es nada extraño que Marruecos presiona a España a través de la Unión Europea para que les den más dinero, más cooperación. Esto es una llamada de atención cuando ha habido un cambio político. La situación está ahí y aunque muchos de estos emigrantes vienen de paso, porque no es su fin quedarse en España, pero es una realidad importante. La Unión Europea, la Comisión, ha reajustado los fondos y ha dotado de un mayor fondo a la parte de fronteras, al fondo de Seguridad Interior, al FAMI también, ha habido una acciones de emergencia, como que en el FAMI a la Policía se le ha asignado una serie de proyectos y son de los pocos que hemos tenido la Unión Europea, la Comisión nos lo ha pedido.

Y quisiera saber, qué soluciones tecnológicas, con independencia de la Red satélite Copernicus que todavía está en desarrollo y que tiene un margen de unas horas hasta que las imágenes llegan en tiempo real; este satélite, Ingenio, cómo puede combinar medidas tecnológicas con las medidas políticas de la Comisión europea, porque es una prioridad en materia de seguridad de la Unión.

Interviene: Juan Carlos Cortés Pulido

Creo que es un problema global y necesita una solución global, pero existe lo que se llama el tiempo de revisita de los satélites. Ahora mismo, Copernicus creo que puede traer imágenes con una diferencia de días pero es imposible tener un sistema que pueda localizar en tiempo real la zona que interese. Esto se está tratando en estos momentos y se habla de constelaciones. Las constelaciones son grupos de treinta, cuarenta, cuatro mil satélites en varios ámbitos, tanto en el de las telecomunicaciones como en el de la tele atención para poder monitorizar zonas en tiempo real. Ahora mismo, la solución tecnológicamente es posible, los temas relaciones con diseño, puesta en órbita, instrumentos, gestión de fotos, son posibles; pero no hay un plan de sistema. En el futuro ya veremos, pero ahora es una idea, debe de haber más de mil satélites operativos y se están proponiendo constelaciones que alcanzan los ocho mil satélites. En estos momentos, la solución tecnológicamente más viable sería un sistema mixto con drones, con infraestructuras terrenas, con radares tipo SIRE, lo que existe ya en España, integrado y que pudiera monitorizar en la zona que interesa.

Interviene: Anabela Gago

Sin entrar en los detalle tecnológicos de los proyectos. Punto primero, que tiene que ver con el posicionamiento político, en el nuevo marco financiero que es el MFF -Multiannual Financial Framework- (2021-2027) tuvo una importancia enorme la seguridad en general, mucho más que en el marco actual que el MFF, y que se termina en el año 2020, y con un gran enfoque la protección de las fronteras. Reflejado en la revisión de los nuevos reglamentos y el fondo para la gestión integrada de las fronteras, que tuvo mucha mayor importancia que el actual, así como el Fondo de Seguridad Interior Policíal. Pero, para las fronteras es políticamente muy importante el nuevo cuadro financiero y muy importantes los fondos de apoyo a los Estados miembros para la gestión integrada de las fronteras, y también un apoyo increíble para todo lo que es el futuro de la Agencia Europea de Guarda de Fronteras y Costas (Frontex), y el plan de la investigación Horizonte Europa. Nosotros lo que argumentamos es que si hay esa importancia a nivel político para todo lo que es fronteras y para todo lo que es seguridad en términos más generales, el presupuesto para la investigación también tiene que crecer en paralelo, pero no creció. En la propuesta de la Comisión se quedó más o menos lo que era ahora. Hay argumentos de Estados miembros que lo vie-

ron no igual, sino al contrario, en disminución. Teóricamente, debería haber acompañado la misma importancia porque la investigación es un apoyo a la política.

Ahora, en términos de proyecto, es verdad que Horizonte 2020 da una parte muy importante a los proyectos de fronteras y hablé del *cloud side*, una de las aplicaciones para la detección de pequeñas embarcaciones en el mar. Ahora, lo estamos intentando, en cuanto Dirección General, en cuanto unidad responsable del impacto de nuestra investigación, y sabemos que es un proyecto bueno, aunque algunos lo ven como pasado y, por ejemplo, cómo convencer a la agencia Frontex de que haga la mejor utilización de las aplicaciones tecnológicas que salieron de *cloud side*; porque las investigaciones hacen el futuro y lo que se ha desarrollado ahora ya está pasado, pero a lo mejor hay posibilidad de utilizar lo que se hizo para mejorar. Luego hay interferencias de carácter político sectorial, porque hay varios tipos de entidades implicadas y en cuanto, por ejemplo, la Dirección General del Mar, ve interés en desarrollar ciertas aplicaciones del proyecto, la que trabaja indistintamente con la Dirección General de Transporte, no lo ve así, y hay que encontrar un campo común y utilizarlo en el interés de todos. Para algunos el objetivo es de unidad, para otros es distinto; unos trabajaron con Copernicus, otros están preocupados en que su ambiente de comunicación no sea alcanzado por otros. Por ejemplo, la Marina y la Guardia Aduanera, las aplicaciones que desarrollaron permiten que cada uno no tenga que cambiar su sistema, pero que los sistemas puedan ser utilizados. Eso tiene un potencial enorme; luego hay otros proyectos como el U-VISA que está todavía en curso, se lanzó en año 2014 y se termina en el año 2019. Su objetivo es mejorar la gestión de los flujos de migración ilegal a la frontera terrestre, con una mejor situación del contexto y de capacidad de reacción de las autoridades responsables de la seguridad. Ese proyecto está desarrollando un sistema en que las técnicas de análisis de video serán combinadas para mejorar la vigilancia en la frontera, pero también hay otros con el mismo objetivo.

Hay otro elemento político además de la investigación de fronteras que hacemos, aunque tenga por objetivo controlar o ayudar la gestión de la emigración ilegal, siguen siendo proyectos de seguridad de fronteras. Porque hay una gran presión, parte de las ciencias humanas, de la protección, de los derechos humanos, que no quieren que se mezcle; que todo lo que es innovación para la migración se quede separado.

Para nosotros, migración ilegal va unido a refuerzo de vigilancia en la frontera y así tiene que seguir. Ahora, para el futuro estamos consultando no solamente a los Estados miembros y otros Skateholders, para definir la programación de Horizonte 2020 para el año 2020, sino que vamos a empezar ahora la programación estratégica para Horizonte Europa.

Y, ahora tenemos un reto en las próximas semanas; dentro del *cluster* que es lo que quieren las ciencias sociales humanas, las sociedades resilientes que son actualmente el reto societal nº 6, más el reto societal sociedades seguras; que lo llevamos nosotros y tiene las fronteras, el crimen organizado, el terrorismo, la respuesta y prevención a los desastres naturales y la infraestructura; que lo pongamos todo en una página, lo que deben ser las prioridades para la programación estratégica. Pero, no podemos poner todo esto. Lo que es casi seguro es que la gestión de las fronteras estará dentro de la programación estratégica. Para nosotros, que nos ocupamos de esta área, vemos cómo en el horizonte si tuviéramos que elegir dos, la gestión de las fronteras en el marco de las políticas actuales, para nuestros comisarios, para nuestra jerarquía, es la gestión de las fronteras y es la protección de los espacios públicos. Las ciudades resilientes eso es lo que veo que apunta en el horizonte.

Interviene: Juan Carlos Cortés Pulido

No he contestado a la pregunta de Ingenio. Ingenio está diseñado para tener ocho coberturas completas de la península ibérica. Es cierto que se diseñó teniendo en cuenta requisitos científicos. ¿Cómo se hizo? Convocamos un grupo de investigadores científicos que dieron requisitos científicos y que fueron los que luego dieron lugar al desarrollo del diseño del sistema. En el año 2019 empezaremos a definir la segunda generación, Ingenio 2. ¿Cómo será? No lo sé porque el planteamiento va a ser diferente, estamos hablando con el Estado Mayor de la Defensa para ver qué requisitos quiere. Ingenio 2 que también será óptico, probablemente no será científico, casi con toda certeza, sino que será un sistema operativo nacional y para ello necesitamos requisitos de los operativos y en ese momento también contaremos con Interior. Quizás sea una constelación de satélites para minimizar el tiempo de revisita y muy probablemente sea una constelación subbética, es decir, el instrumento podrá tener una resolución menor del medio metro.

Y, ya tiene implicación en Defensa y en Seguridad. Otra cosa que también he recordado es que, el sistema español de observación del territorio consta de dos satélites que son Ingenio y otro radar que se lanzó en febrero; es un sistema radar que ya está dando imágenes y que también tiene implicaciones de Seguridad y Defensa y que lo gestiona directamente el Ministerio de Defensa. Y un último comentario en relación con los temas futuros para seguimiento de fronteras, vigilancia de fronteras; la acción preparatoria son unos fondos que la Comisión está canalizando para investigar la conveniencia o no de que la Comisión, en el siguiente periodo, se meta en programas de Defensa. En esta acción preparatoria, uno de los programas aprobado es una iniciativa de Leonardo, la empresa italiana, para vigilancia de fronteras. Y, en la siguiente generación de programas, en el Europe anti defens, que es un plan donde hay un montón de millones para desarrollos, probablemente se tratarán también temas relacionados con la

Defensa de las fronteras y, aunque ahí el titular es el punto de contacto de Defensa, creo que las tecnologías base en su estado tecnológico del EDAP y de la temática de seguridad es el mismo, entonces básicamente la tecnología es la misma, lo que varía es la aplicación.

Interviene: Luisa María Benvenuty Cabral

Yo quería hacer una pregunta antes de comenzar la ronda de preguntas: Jorge ha hablado de la ventaja de la compra de innovación y de tecnología que, sobre todo, es una cuestión económica. Los grandes grupos criminales tienen todo el dinero y toda la libertad para adquirir todos los productos y cuando ellos detectan que tenemos un sistema, por ejemplo, para detectar drogas líquidas en los aeropuertos, ellos se van a la empresa para que les fabrique obviamente el sistema más avanzado para poder eludir. Cuando hemos hablado del tema de los teléfonos, de las encriptaciones, hay una aplicación que se puede comprar si se pueden pagar los mil y pico euros diarios, que ellos lo tienen como el Encrochat que te bloquea todo el móvil y además a distancia, se puede mandar un mensaje al móvil para que lo borre absolutamente todo y es irrecuperable. Puedes comprar algo por Internet, es legal la publicidad y la compra, el uso que tú hagas de Encrochat y de otros sistemas radica en el empleo que haga el usuario. Al hilo de esto, hemos hablado de las criptomonedas, del proyecto de Titanium que lidera la Policía Nacional, el Horizonte 2020; blockchain surgió para la protección de la transacción de monedas tipo criptomonedas, pero la inteligencia financiera lo está utilizando cada vez más porque garantiza y simplifica las transacciones y el registro ¿Cómo podíamos aplicar blockchain en nuestras bases de datos policiales o las bases de datos legales, por ejemplo, en el Ministerio, Juan Carlos? ¿Ha surgido alguna idea sobre aplicación de blockchain para nuestras propias transacciones?

Interviene: Jorge Álvaro Navas Elorza

Nosotros no, pero sí que he oído cosas en el Ministerio de Justicia, estoy tratando de recordar una aplicación concreta y ahora mismo no lo sé, yo voy al Comité de dirección TIC que es donde están todos los Ministerios y un día surgió el tema de blockchain; y sé que la Agencia Tributaria tenía aplicaciones de blockchain.

Blockchain, es un registro que no está centralizado y que la seguridad se basa en que para hackear un contenido tienes que hackear dos mil o tres mil ordenadores a la vez, con lo cual se supone que es seguro; por eso, aplicando esto puedes hacer muchas cosas, evidentemente, pero no tengo ningún ejemplo, lo podía buscar; lo que sí he visto con *blockchain* es que no puedes borrar un histórico, es un problema de cara a la informática administrativa, si tienes datos personales en *blockchain* no puedes implantar el derecho al borrado y no lo controlas, es decir, tiene cosas buenas y malas también.

TURNO DE PREGUNTAS

Pregunta en sala: Juan María Cervera, Comisario jefe de la provincial en Badajoz.

Han hablado ustedes de la defensa, de que tenemos que poner cotas al tema de la inmigración, me refiero a las fronteras. Y habla usted de prepararse para el blanqueo de las criptomonedas y de los nuevos intentos que nos pueden venir con la manipulación de las redes sociales ¿Me puede decir algo de las amenazas, de los sabotajes que ha habido, de esas amenazas hibridas auténticos sabotajes que unos Estados pueden hacer sobre otros, incluso atentando contra procesos democráticos y cambiando incluso Estados? En concreto me refiero a una posible injerencia de Rusia en el proceso catalán ¿Estamos preparados para podernos defender de esos ataques?

Responde: Jorge Álvaro Navas Elorza

El tema de la manipulación de redes sociales, es la detección en tiempo real porque todos los estudios que han demostrado que el 1 de octubre 2017 desde cuentas rusas, se retuitearon del orden de cuarenta mil, cincuenta mil mensajes por minuto, por hora; es decir, desde Rusia se retuiteando mensajes del proceso, eso se ha sabido después de unos análisis que han tardado semanas en hacerse. El reto que tenemos es en tiempo real de ese diagnóstico, porque los números en internet son inmensos, el número de cuentas de twitter que se crea por minuto es desmesurado, por lo que es complicado hacer una detección en tiempo real, saber que esa cuenta que se ha creado es falsa o cuál es el originario, es complicado. Métodos tiene que haber, al final es tratamiento de bigdata y creo que habría una manera de que cada cuenta que se retuitea habría que darle unos puntos de calidad, especificando que la cuenta es la primera vez que retuitea, de tal forma que si una información que la han retuiteado cuarenta mil cuentas y de ellas el 95% es el primer tuit que ponen en su vida, que retuitean; pues obviamente no tiene fiabilidad. Eso podía ser una pequeña barrera. Y, de temas físicos tenemos el Centro nacional de Protección de Infraestructuras Críticas (CNPIC), donde se investiga todo tipo de posibles hackeos que pueden afectar a la vida de las personas de una manera que a veces ni nos imaginamos. Si, por ejemplo, se decía que al manipular los temas de control de nivel de agua del pantano de El Atazar consigues desbordar El Atazar, se causarían millones de muertes. Simplemente, si al manipular el nivel de cloro que hay en el agua que nos bebemos del Canal de Isabel II, a una ciudad de tres millones de personas, se les provoca diarrea brutal, pues también se está haciendo un daño tremendo. Otro país con temas más sonoros es Israel, sus servicios secretos, que acabaron con todo el proyecto nuclear de Irán. Lo que hacían era poner un virus que físicamente centrifugaba, y que dañó físicamente y paró el programa y provocó un retraso de uno o dos años. Lo que tienen estas amenazas persistentes (Apt) es que muchas veces se detectan seis meses, dos años después de

que están. El malware y los virus son muy inteligentes, si se coge un software se pone en una *sanbou* preparada para detectar si hay un virus o no, lo tienes seis o siete horas analizando a ver si hace algo y no hace nada porque antes los virus se activaban inmediatamente, pero ahora los virus tienen mucha paciencia y son capaces de dormirse dos semanas.

Cuando se analiza en tiempo real software sospechoso se puede tener en espera de que actúe quince minutos o treinta minutos, pero no una semana, dos; y hay malware que está dos semanas sin hacer nada y luego actúa, de manera que se exfiltra información, esto se suele hacer a través de paquetes mal formados y a lo mejor están filtrando cuatro bits en cada paquete, de manera que son unos datos residuales de un error de red y no lo tienes en cuenta. Para un fichero Word de dos megas, pueden tardar siete días en transmitirlo, pero los ciberespías no tienen prisa. El problema es detectarlos, lo que está claro en la seguridad de formación es que las fronteras y los grandes cortafuegos, ya no existen, hay que vivir pensando que el enemigo ya está dentro y lo que hay que hacer es intentar que no se lleve las cosas; pero es muy difícil poner barreras, sobre todo en las circunstancias en que todo el mundo está conectado y todos necesitan Internet para cualquier cosa y al final, visitando páginas de Internet, por muchos software y antiphishing que tenga, es muy difícil evitar algunos ataques cuando, a veces, vienen de los mismos fabricantes.

Hay casos en que se compran ordenadores vírgenes y tienen virus. EEUU no deja comprar ningún router, ni equipo de huawei porque vienen todos con "regalo". Es un tema enormemente complejo pero no hay que pecar de ingenuidad, hay que pensar que estamos siendo atacados constantemente y hacer todo lo posible para poner obstáculos e ir variando, de hecho el Esquema Nacional de Seguridad, recomiendan sobre el tema cortafuegos, que se tengan de distintos fabricantes, porque si uno tiene la mala suerte de que te hace cosas que no quieres, el otro lo pare. Al final se basa en productos certificados, pero incluso cuando el Centro de Criptografía Nacional hace una certificación de un router, de un modem, de un sistema operativo; lo certifica con una configuración determinada y para una función determinada y son capaces de certificar y de hacer un estudio para algo muy determinado, en cuanto se varían un poco, no lo garantizan; han estado estudiando durante meses la configuración de ese tipo y han visto que no ha pasado nada pero tampoco garantizan. Es un tema difícil.

Interviene: Anabela Gago

Quería añadir un punto porque en relación con todo esto, la única posibilidad es, de hecho, la cooperación, la colaboración y en todo lo que son ataques ciber, independientemente del origen; tenemos el Centro Europeo de lucha contra el cibercrimen en Europol (European Cybercrime Centre),

y esto se desarrolló de una forma muy rápida e importante; y cuantas más operaciones conjuntas se hacen con las autoridades policiales y otras de los Estados miembros y también con las compañías como American Express, Visa, Mastercard o las compañías aéreas por ejemplo, se crea un contexto de confianza. El hecho de que haya tantas operaciones con éxito está creando un ambiente de paz y eso es fundamental. Como han dicho antes se ve una amenaza y cuando hay una operación que tiene éxito, por ejemplo, en relación con criptomonedas, con el *criptowall* que es el ransomware utilizando encriptación, lleva meses y meses o más de un año de observación porque los "bichitos" están tranquilos durante mucho tiempo; pero eso solo es posible porque hay muchas autoridades de distintos países implicadas en todo el procedimiento. Por ejemplo, con el centro SC3 toda la prioridad era, el pago por la explotación sexual de los niños. Tenemos claro muchos proyectos muy interesantes pero ellos no estaban al corriente de nuestros proyectos: proyectos F7, proyectos del 2014…, pero ahora tenemos una relación que empieza siempre por una base personal y a uno de nuestros coordinadores de proyectos que estuvo hace un mes, enseñando los resultados del SC3.

Están utilizando tecnología americana y eso no es nada en comparación con lo que estamos desarrollando nosotros, que al ser una autoridad pública, conectado con el centro universitario en el Reino Unido, lo podéis tener, es *free*, no cuesta nada; y ya han empezado a mostrar interés.

Luego está la parte del análisis de medios sociales, hay muchos proyectos en conexión con la lucha contra el terrorismo. Tenemos el proyecto boxpol y en Europol también se desarrolló otro centro que es la unidad internacional, pero cada vez más la investigación que se hace sobre lo que pasa en lo social tiene que hacerse conjuntamente con la investigación en otras áreas; por ejemplo, hace un año se discutía por los Estados miembros, el programa de trabajo e investigación para dar respuesta a los desastres naturales o ataque terrorista, y se estaba poniendo un tópico sobre investigación en el papel de los sociomilla y luego se estaba haciendo otro para dar lugar a un COL sobre la prevención.

Hay que trabajar juntos porque si se está desarrollando un sistema de estudio y de respuesta delante de una situación de ataque o desastre y no se incorporó la respuesta de solución de los primeros intervinientes, lo que hace la gente con facebook parece uno de los efectos inmediatos que perturba todo. De igual forma, la utilización de los mecanismos de facebook, de localización, de comunicación…, todo esto se tiene que hacer delante de la respuesta y no ser un análisis aparte. Con lo cual, todo tiene que estar y ser uno.

Pregunta en sala: José M. Raba. Trabajo en el departamento de investigación en Policía Municipal.

Las empresas que hemos estado viendo: Amazon, Aipal ..., son todas americanas, no hay ninguna europea ¿por qué, cuál es el problema? Y, por otra parte, se va a hacer algo parecido a Airpaner, agencia norteamericana, se va a hacer un equivalente en Europa?

Responde: Jorge Álvaro Navas Elorza

Voy a contestar a la primera pregunta, con el tema de la innovación se habla mucho de los ecosistemas de innovación. Un ecosistema de innovación, en una ciudad como en EEUU Silicon Valley, o como Tel avi en Israel; es un ecosistema de innovación porque se cumple todo para poder hacer la innovación; se cumple que haya una serie de universidades, científicos, personas potentes en tecnología que estén en esa zona; y a la vez, haya una financiación y una serie de empresas aventureras que quieran arriesgar su dinero. En general todos los innovadores y los grandes empresarios se han arruinado de media una o dos veces. Yo creo que hace falta ese ecosistema de innovación, los americanos lo tienen, tienen miedo al ridículo o no tienen miedo al fracaso, que puede ser que en Europa lo tengamos y, a lo mejor, los financieros americanos se arriesgan más que los españoles.

Interviene: Juan Carlos Cortés Pulido

Siguiendo con esto yo creo que tiene que haber condiciones de contorno, tema cultural, pero lo que marca los diferentes programas marco de I+D+i es que así como Europa tiene una participación muy destacada en conocimientos, un tercio de los papers de todo el mundo son europeos, a la hora de transformar ese conocimiento en negocio, somos realmente malos y hay que ver realmente qué está ocurriendo.

Interviene: Anabela Gago

Algo muy interesante con las crisis económicas es que uno de los utensilios que la Comisión Europea desarrolló, y está teniendo mucho éxito, es el Fondo Europeo para Inversiones Estratégicas, que no es un fondo, es una garantía del Banco Europeo de Inversiones; y lo interesante es que están garantizando a las empresas que se lanzan en áreas de riesgo y que no tienen nada que perder porque ya están mal, o porque no hay perspectivas. Lo más interesante de todo es que hace un año empecé a comunicar con la gente que se ocupa de esto, que está en la Dirección General de Finanzas, que conecta con el Banco Europeo de Inversiones, para ver qué se podía hacer para que nos ayudaran a tener más market at capers para que haya empresas que corran el riesgo de lanzar al mercado cosas que hacemos. Los países que más lo están utilizando, inventando lo que sea, son Grecia, Portugal y España; o sea los que lo pasaron peor porque la banca no daba dinero. En el área de la seguridad hubo algo más difícil porque el Banco Europeo de Inversión tiene unos criterios muy limitados que no dejan apoyo a cierto tipo de actividades conectadas con la función policial.

Interviene: Jorge Álvaro Navas Elorza

Añadir una reflexión personal, los mejores de las universidades, los mejores de la clase, en general, en España ¿qué quieren ser? Funcionarios. La gente más brillante hace oposiciones a notarías, etc. En España, en general, la gente brillante en la universidad es poco emprendedora, todos quieren tener una situación más o menos cómoda y casi todos opositan o hacen algo para tener una estabilidad. Gente muy joven, por ejemplo, en informática, la gente que aprueba el cuerpo superior de informática, tienen alrededor de veintiséis años y lo que quieren es un trabajo estable. En España tienen más aversión al riesgo que en otros países.

Segundo panel: los nuevos avances tecnológicos, beneficios para la sociedad

PERSPECTIVA EUROPEA DESDE EL PUNTO DE VISTA DE LA POLICÍA EN TEMAS RELACIONADOS CON LA INNOVACIÓN

CARLOS ANTONIO VÁZQUEZ ARA
Comisario principal del Cuerpo Nacional de Policía,
Jefe de la División de Cooperación Internacional

INTRODUCCIÓN

Como sabemos, el intercambio de información entre distintas autoridades y actores relevantes para la seguridad se ha identificado, de una forma recurrente, como una herramienta esencial para abordar las amenazas más graves a las que ahora estamos enfrentados en la sociedad. Ha sido y es, probablemente, el más importante caballo de batalla en el proceso de configuración y consolidación del espacio de libertad, seguridad y justicia de que nos hemos dotado en la Unión Europea a través del Tratado de Lisboa que es el que tenemos ahora en vigor. Por otra parte, Europa es una sociedad altamente dinámica, como sociedad desarrollada que es, millones de ciudadanos nacionales de terceros países están cruzando cada día las fronteras exteriores y también las interiores. Las cifras son también significativas en cuanto a cruces irregulares de frontera, por ejemplo, tenemos el conflicto de Siria y la crisis migratoria permanente que estamos viviendo de fondo, que está provocando millones de cruces irregulares en nuestras fronteras. La última oleada de ataques terroristas que ha puesto a Europa en la encrucijada es la amenaza de terrorismo internacional que supone para seguridad interior la que nos hace reflexionar permanentemente sobre estas cuestiones.

Nos consta que ciudadanos de la Unión han cruzado las fronteras para ir a zonas de conflicto, para participar en la guerra de Siria, por ejemplo; y al contrario, ciudadanos que han vuelto utilizando rutas de inmigración irregular o las vías normales de comunicación con la Unión.

La Estrategia de Seguridad Interior de la Unión Europea renovada del año 2015, aborda los retos de: migración, terrorismo y delincuencia organizada. Es parte del Núcleo central de la referida estrategia determinar la forma en que los sistemas de información existentes y futuros podrían reforzar tanto la gestión de las fronteras exteriores como la seguridad interior de la Unión Europea.

A día de hoy, tenemos definidos e implementados una serie de diversos sistemas de información que proporcionan datos relevantes y útiles desde la perspectiva policial, pero la arquitectura de gestión de estos datos, tanto en la Unión Europea como a nivel nacional, dista mucho de ser perfecta. Puede decirse que el conjunto de sistemas se define por una elevada fragmentación, por una complejidad de las bases jurídicas, por las dificultades de acceso de la Policía para el cumplimiento de sus misiones. Se impone, por tanto, la necesidad de mejorar la interoperabilidad de los Sistemas de Información como un objetivo a medio y largo plazo por la complejidad. La interoperabilidad de los Sistemas de Información en el área de justicia e interior, dentro de la Unión Europea, se ha constituido en una prioridad de la agenda política. Están pronunciadas todas las instituciones relevantes de la Unión Europea, desde el Consejo Europeo, al Consejo de Ministros, la Comisión Europea, etc. Todo a raíz de los atentados en Paris, Bataclan, Sendenís, en diciembre del año 2015 cuando los propios jefes de la Unión Europea establecieron el intercambio de información de interoperabilidad de los Sistemas de Información como un requisito esencial para ser efectivos contra esta amenaza.

La ausencia de fronteras, el espacio Schengen, exige una gestión sólida y fiable de la circulación de las personas por las fronteras exteriores. Sabemos que es un mecanismo compensatorio, una condición previa para garantizar el alto nivel de seguridad y libre circulación de personas que nos exige nuestra democracia europea. Los agentes de policía se enfrentan a un panorama complejo de sistemas de información gestionados de forma diferente a escala de la Unión Europea pero también a escala nacional. Esta complejidad ocasiona dificultades prácticas en particular en cuanto a qué bases de datos pueden ser relevantes en cada caso o en cada actuación policial.

No todos los Estados de la Unión Europea están conectados a todos los sistemas, también tenemos diversidad en cuanto a la responsabilidad; ya hemos visto lo que ha ocurrido con las decisiones Prüm que hasta hace muy poco tiempo era solo cuestión de unos pocos Estados miembros de la Unión Europea y el resto no quería saber nada del asunto. Esto se debe a diferentes contextos institucionales, jurídicos y políticos en los que se han desarrollado los distintos sistemas, la información se almacena en sistemas separados de manera que rara vez están interconectados. No hay coherencia entre la

fase de datos y existen divergencias de acceso por parte de las policías y de las autoridades encargadas. Este es el gran problema precisamente, y este es el diagnóstico resumen de la situación. Se ha identificado como urgente el avanzar hacia la interoperabilidad de los Sistemas de Información relevantes para uso policial con el fin de mejorar el intercambio de información, imprescindible para la cooperación en la lucha contra las amenazas mas graves contra la seguridad. Es el núcleo gordiano de la necesaria e imprescindible cooperación multisectorial y multidisciplinar de que debemos dotarnos para la lucha contra las amenazas a las que nos enfrentamos.

Todo esto se articuló en la Unión Europea a nivel interinstitucional, tanto en el Consejo Europeo, como en el Consejo de Ministros, o la Comisión Europea, con su comunicación del año 2016, denominada "Sistemas de información más sólidos e inteligentes para la gestión de fronteras en la seguridad". El grupo de expertos de alto nivel que se generó, a partir de esta comunicación, las conclusiones de este grupo de expertos de alto nivel, la hoja de ruta del Consejo de Ministros para mejorar ¿Con esto qué quiero decir? Que es una verdadera apuesta, una decisión política del más alto nivel en la Unión Europea de la que no podemos sustraernos absolutamente nadie. Es lo que quiero dejar claro desde un principio, estamos obligados a avanzar en el camino de la interoperabilidad de los sistemas de información.

Los sistemas de información que tenemos ahora, en la Unión Europea para gestión de fronteras y seguridad interior, tienen cada uno sus propios objetivos, finalidades, bases jurídicas y usuarios en un contexto institucional. Juntos constituyen un modelo complejo de bases de datos que como digo son tecnológicamente, pero también jurídicamente, diferentes. Esto ocasiona los problemas que vamos a ver a continuación.

DESCRIPCIÓN DE LOS SISTEMAS DE INFORMACIÓN PARA LAS FRONTERAS Y LA SEGURIDAD

Los tres principales sistemas de información centralizados desarrollados por la Unión Europea son:

- El Sistema de Información Schengen (SIS) con un amplio espectro de descripciones de personas y objetos.

- El Sistema de Información de Visados (VIS) con datos sobre visados para estancias de corta duración.

- El sistema Eurodac, con datos relativos a impresiones dactilares de solicitantes de asilo y nacionales de terceros países que han cruzado las

fronteras exteriores de forma irregular. Este es el sistema que está ocasionando gran parte de los problemas en materia de asumir consecuencias en la migración de la Unión Europea.

Los tres sistemas son complementarios y con la excepción del SIS están destinados a ciudadanos de terceros países. También, proporcionan apoyo a las autoridades nacionales en la lucha contra el terrorismo y las amenazas relativas a la delincuencia organizada, en particular el SIS, el Sistema de Información Schengen es actualmente el instrumento de intercambio de información más utilizado.

El acceso de las autoridades policiales, por ejemplo, al VIS y a Eurodac, se puede ejercer pero en unas condiciones muy limitadas, que hoy por hoy son prácticamente inoperantes, muy difícil de integrar en los sistemas de investigación y de control.

Otros sistemas que están en fase de implementación aprobadas recientemente sus bases jurídicas son:

- El Sistema de Entrada y Salida (EES) cuyo reglamento se aprobó a finales del año 2017, y el Programa para viajeros frecuentes (Etias), cuya norma reguladora va a adoptarse antes de finalizar el año 2018, que contiene también información relevante de obtención indirecta para la lucha contra la criminalidad.

- Otros instrumentos son la base de datos de Interpol sobre documentos de viaje robados y perdidos (DVRP) y el sistema de información anticipada sobre los pasajeros (API).

Esto afecta también a ciudadanos de la Unión Europea, no solamente a ciudadanos de terceros países, es un matiz muy importante a la hora de distinguir entre bases jurídicas, por eso lo especifico.

Específicamente con fines policiales de investigación penal y cooperación judicial, la Unión Europea ha desarrollado instrumentos descentralizados para el intercambio de información, a saber:

- El marco Prüm para intercambiar ADN, impresiones dactilares y datos de matriculación de vehículos; y el Sistema Europeo de Información de Antecedentes Penales (Ecris), cuyo Reglamento se adoptará previsiblemente a finales del año 2018. Permite un intercambio de información a través de una red segura sobre condenas de ciudadanos de terceros países en la Unión Europea, cuya base jurídica será próximamente aprobada.

- Europol, por otra parte, apoya el intercambio de información entre autoridades competentes para la lucha contra la criminalidad grave y el terrorismo. Dispone de una serie de instrumentos de gestión de la información y de generación de inteligencia criminal, como el sistema de información de Europol, que dispone igualmente de un canal seguro conocido como canal Siena que se utiliza para intercambio de información relevante entre Estados miembros y los puntos de contacto. De igual modo se va a llegar a utilizar en la lucha contra el terrorismo y dispone también de los focal point, los ficheros de análisis para determinadas especialidades policiales. Europol es hoy en día la referencia en la Unión Europea en materia de intercambio de información contra las graves amenazas que nos enfrentamos.

Conjunto suplementario de sistemas de tratamiento de datos que será desarrollado por el PNR Passenger Name Record (Registro de nombre de pasajero) su Directiva se ha adoptado no hace mucho y ahora estamos en fase de implementación, de hecho ya ha pasado el plazo de trasposición de directiva.

LA NUEVA REGLAMENTACIÓN PARA LA INTEROPERABILIDAD DE LOS SISTEMAS DE INFORMACIÓN

La Comisión Europea por indicación del Consejo Europeo en el Consejo de Ministros de Interior establece dos iniciativas legislativas que se resumen en reglamentos. Una única reglamentación en general para afrontar la interoperabilidad de los Sistemas de Información. Esto es una apuesta determinante desde la Unión Europea. Un Reglamento de la Unión Europea es una norma jurídicamente vinculante desde el inicio en que entra en vigor, no requiere transposición, ni adaptación al Derecho Nacional, aunque pueda adaptarse mediante cualquier tipo de legislación. Esto significa que es obligatorio para todos.

¿Qué objetivos se plantea la Comisión Europea con estos Reglamentos? Se van a adoptar probablemente antes de final de año y ahora están en fase de iniciación con el Parlamento Europeo, se ha dado mandato hace unos días para acentuar esa fase de negociación, lo que se llama los trílogos en el Parlamento Europeo, Comisión y Consejo; con lo cual, se prevé que estén aprobados antes de final de año y, a partir de ese momento, se empezará a dotar de base jurídica global europea todas las iniciativas que ahora están en marcha.

Los Reglamentos, sobre interoperabilidad de los Sistemas de Información, tienen como objetivos específicos:

- Que los usuarios finales, la Policía y otras autoridades competentes,

tengan un acceso rápido, ininterrumpido, sistemático y controlado a la información que necesitan para ejercer sus responsabilidades.

- Ofrecer una solución para detectar identidades múltiples, un gran problema dentro de la Unión Europea, planteado desde muchos puntos de vista: comercio seguro, etc.

- Facilitar los controles de identidad de los nacionales de terceros países. Relacionado con el mismo los biométricos con la doble finalidad de garantizar la correcta identificación a personas de buena fe y luchar contra la usurpación de identidad.

- Facilitar y racionalizar el acceso de los cuerpos policiales a los sistemas de información no policiales a escala de la Unión Europea cuando sea necesario para luchar contra el terrorismo y la criminalidad grave.

- Facilitar la aplicación técnica y operativa por parte de los Estados de los sistemas existentes y futuros de la Unión Europea: financiación, sistemas..., con la ayuda de Bruselas.

- Reforzar y racionalizar las condiciones de seguridad y protección de datos.

- Mejorar y armonizar los requisitos de calidad de los datos de los respectivos sistemas.

Por otra parte, se incluyen dos Disposiciones que son de interés, una es la creación y gobernanza del formato universal de mensajes, el UMF (*universal message format*). Esto tiene una importancia estratégica que vamos a ir viendo. Como una norma de la Unión Europea para el desarrollo de sistemas de la información en el ámbito de Justicia e Interior y, la creación de un repositorio central para la presentación de informes y estadísticas que se hacen de una manera centralizada y evitar la dispersión y descoordinación.

Ámbito de aplicación: junto con su propuesta, presentada el mismo día, el Reglamento se centra en los sistemas de información de la Unión Europea para la gestión de la seguridad, las fronteras y la migración administrados a nivel central. Todo esto son decisiones que se tomaron después de las conclusiones a las que llegó el grupo de expertos de alto nivel, donde se estudió bases de todo: bases de datos nacionales, bases de datos de la Unión Europea, bases de datos de Interpol, cómo se podían interconectar todas y cada una de ellas. Se llegó a la conclusión de que había que ir paso a paso; obviamente, primero había que pensar en las de control de la Unión Europea para

ir avanzando posteriormente con las demás. Por eso, estamos hablando de datos administrados a nivel central en la Unión Europea.

Los tres sistemas existentes. El Sistema de información Schengen, que tiene un centro de descripción de personas (entrada, estancia en la Unión Europea, órdenes de detención, desaparecidos, controles discretos específicos); se está utilizando para el control de los combatientes terroristas internacionales -los desplazados a Siria, a través del Artículo 32.6 en cuanto a alertas específicas-. Como he dicho antes, el sistema de información Schengen es el modo más importante de cooperación y de intercambio de información en el ámbito de la Unión Europea extendido. El sistema Eurodat que se refiere a emigrantes y peticiones de asilo, información de visados. Y, se unen en la reglamentación al Sistema de Entrada y Salida (EES) y el Programa para viajeros frecuentes (Etias)

A finales de año también se incorporará, si la base jurídica se adopta, el Sistema Europeo de Información de Antecedentes Penales (Ecris). Los seis sistemas son complementarios, con la excepción del SVDI que se refiere a nacionales de terceros países. A esto se añadirá la base de datos de Interpol para control en fronteras; hablamos de la base datos de documentos sustraídos o robados y la base de documentos de viajes asociados a la autentificación. Así se pretende conectar con los datos de Europol que sean pertinentes para el funcionamiento de todo lo que estamos hablando.

Quedan fueran del ámbito de aplicación los sistemas de información descentralizados, bases de datos cuyos repositores están en el ámbito nacional aunque en el futuro se prevé su interconexión.

COMPONENTES TÉCNICOS-OPERATIVOS QUE SE CONSIDERAN NECESARIOS PARA LOGRAR LA INTEROPERABILIDAD

Componentes que se consideran necesarios e imprescindibles para lograr la unidad de todos estos sistemas:

- En primer lugar lo que se denomina Portal Europeo de Búsqueda (PEB) es el componente que permitiría la búsqueda simultánea en múltiples sistemas, así como en los datos correspondientes a sistemas de Europol e Interpol, utilizando datos de identidad, biográficos y biométricos. Este sistema -Portal Europeo de Búsqueda- no realiza ningún tratamiento de datos, no genera preocupaciones en materia de protección de datos y actuaría como ventanilla única intermediaria de mensaje para consultar varios sistemas centrales y tener la información necesaria sin pro-

ducción de continuidad. Es decir, este es el gran avance y ahora vamos a ver cómo se está empezando a desarrollar el proyecto CUES.

- El servicio de correspondencia biométrica compartido (SCB compartido) permitiría la consulta y la comparación de datos biométricos (impresiones dactilares e imágenes faciales) de varios sistemas centrales. Como cada uno de los sistemas centrales dispone de un motor específico de búsqueda de datos biométricos; un servicio de correspondencia biométrica proporcionaría una plataforma común en la que los datos se consultarían y compararían simultáneamente.

- El registro común de datos de identidad (RCDI) sería el componente compartido para almacenar los datos de identidad, biográficos y biométricos; de nacionales de terceros países registrados en Eurodat. Se va a añadir una función de aviso y respuesta positiva de forma que sería posible comprobar la presencia o ausencia de datos en cualquiera de los sistemas cubiertos por el RCDI.

- El detector de identidades múltiples (DIM). Verifica los datos de identidad consultados en más de uno de los sistemas consultados que almacenan datos de identidad en el registro central, así como también el SIS.

Estos son los cuatro instrumentos fundamentales con los que se pretende garantizar o iniciar la interoperabilidad de los sistemas fundamentales de la Unión Europea.

PLANTEAMIENTO EN DOS FASES DEL ACCESO DE LOS CUERPOS POLICIALES PREVISTO POR EL REGISTRO COMÚN DE DATOS DE IDENTIDAD

¿Qué es esto del planteamiento en dos fases? Es lo que he dicho que no va a generar problema en materia de protección de datos. Si, hasta ahora, hemos tenido algún problema en la Unión Europea a la hora de determinar nuevos sistemas de información, que son útiles para la lucha contra el terrorismo y el crimen organizado, han sido, precisamente los indicios los que nos venían desde el área de protección de datos. Es lógico, porque la Carta de Derechos Fundamentales de la Unión Europea y nuestra Constitución, son en este sentido medianamente claras, los pronunciamientos del Tribunal de Justicia también son claros, y el Parlamento Europeo, además, ha estado posicionado claramente durante muchos años en una garantía que le hace acreedor de su propio posicionamiento político. Podría contarles de una manera detallada lo que ha sido la gestión de la Directiva PNR (Passenger Name Record) desde su presentación en el año 2011, hasta su adopción en

el 2016, que tuve la oportunidad de gestionar en Bruselas como representante permanente; una auténtica pesadilla, porque siempre nos encontramos con los mismos problemas y aunque suene un poco duro, los avances se producían a golpe de atentado terrorista.

Cada atentado terrorista provocaba un movimiento en un sentido que durante mucho tiempo el péndulo volvía a bajar. Quiero decir con esto que las cuestiones de derechos fundamentales siempre son enormemente importantes y las tenemos en cuenta a la hora de llevar todo esto, pero claro, lo que no podemos es permitirnos disponer de herramientas útiles en la lucha contra el terrorismo y el crimen organizado, que no están disponibles, con todas las garantías obviamente, pero no lo están. Ese es el gran problema que se ha suscitado en la Unión Europea y que ahora con estos reglamentos, con toda esta nueva iniciativa de interoperabilidad, creo que se van a superar casi definitivamente.

Este planteamiento en dos fases es lo que es el *Privacy by design* la privacidad y la protección de datos garantizada mediante leyes y normas, y los controles que se pueden hacer a través de los tribunales.

La consulta policial es un objetivo, normalmente accesorio, en buen número de los sistemas que estamos hablando, por ejemplo, en Eurodat, en el VIS, o en el sistema de entrada y salida, la consulta de datos desde el Policía, no es el objetivo fundamental. Sabemos, por ejemplo, que el principio de necesidad o de determinar claramente el objeto para una base de datos que se genera, es esencial a la hora de definir su base jurídica. Por tanto, el hecho de ser utilizados los datos desde un punto de vista policial, al ser secundario, supone que se deben imponer una serie de restricciones. En consecuencia, las posibilidades de acceso a estos datos almacenados es muy limitada, los cuerpos policiales solo pueden consultar directamente estos sistemas con fines de prevención e investigaciones de detección de terrorismo y delitos graves y con unas muy importantes restricciones: a través de autoridades específicas, con accesos controlados. Policía y fronteras no puede consultar, el policía investigador, que está en brigada, tampoco con carácter general.

El registro general del que veníamos hablando, que es el registro central de identidades, tiene lo que se llama una funcionalidad de aviso de respuesta positiva. Es decir, se introduce la posibilidad de acceder a los distintos sistemas: SIS, VIS, Eurodat, utilizando un planteamiento de dos fases:

- En una primera fase, un agente de policía iniciaría una consulta sobre una persona concreta, utilizando los datos de identidad, el documento de viaje o los datos biométricos de esa persona, para comprobar si

el RCDI almacena información sobre la persona buscada. El registro central es el que proporciona solamente la noticia de que hay datos en un sistema.

- En una segunda fase, el agente podría solicitar el acceso a cada uno de los sistemas que, según las indicaciones, contengan datos, con el fin de obtener el expediente completo.

Esto es lo que garantiza que no se van a tener los datos de Eurodat a disposición de todo el mundo de manera general que es lo que se pretende evitar. Siendo este el planteamiento en dos fases que garantiza que no vamos a tener problemas con las autoridades de protección de datos.

OTRAS FUNCIONALIDADES DE LA INTEROPERABILIDAD

- El Reglamento también incluye la propuesta de crear un repositorio central para la presentación de informes y estadísticas (RCIE). Necesario para el intercambio de informes de una manera coordinada y coherente.

- El Reglamento propone, asimismo, establecer el formato universal de mensajes (UMF) como la norma que se utilizaría a escala de la Unión Europea para la interacción entre múltiples sistemas de forma interoperable. Vienen desarrollándose en distintos formatos en los últimos años y en el ámbito de actuación de Europol. La Unión Europea va a fomentar el uso del formato universal de cambio de mensajes también con las agencias Europol e Interpol.

FORMATO UNIVERSAL DE MENSAJES (Universal Messaging Format-UMF)

La norma UMF -formato universal de mensajes- introduce un lenguaje técnico común, unificado, para describir y vincular elementos de datos, en particular los elementos relativos a las personas o documentos de viaje. Utilizar la norma UMF al desarrollar nuevos sistemas de información garantiza una integración más fácil y la interoperabilidad con otros sistemas, e introduce mecanismos automáticos de control de la calidad de los datos que es otra de las grandes preocupaciones.

El UMF es la clave del asunto para garantizar el poder internacional en las distintas bases de datos, es el formato universal de mensajes, e introduce ese lenguaje común que va a permitir que todas las policías, de cualquier sitio de la Unión Europea, incluso de espacios Schengen que se puedan

incorporar, puedan consultar en tiempo real y de una manera directa, todos los sistemas de los que hemos venido hablando.

QUEST. PROYECTO UMF3 FINANCIADO POR ISF

El Proyecto UMF3 es un proyecto muy importante dentro de la Unión Europea, con financiación europea, en el que participan varios Estados miembros, Europol, Interpol y otras instituciones de la Unión Europea, que permitirá la interconexión de las bases de datos de las que estamos hablando, de forma que en una única consulta se podrá acceder, además de a nuestras bases de datos nacionales, al Sistema de Información de Europol (SIE) en una primera fase, más adelante se extenderá y será el instrumento fundamental de la interoperabilidad.

El proyecto piloto se ha planteado en esta fase inicial como acceso limitado a consulta de ciertas entidades en el SIE; por un lado a personas: nombre, apellido, fecha de nacimiento y por otro lado armas: número de serie.

España se ha posicionado como primer Estado miembro en lograr poner en marcha un servicio Quest, un servicio muy sencillo que interactúa con la base de datos de Europol. Esto se está llevando a cabo con el liderazgo de la Policía Nacional, con la Jefatura Central de Logística e Innovación y con la actuación de la división de cooperación internacional.

En estos momentos, el desarrollo técnico se encuentra en fase de producción lo que significa que se ha diseñado como lo llaman los técnicos, un cliente ligero; es decir un software y un hardware muy sencillos, a través del que se puede acceder y que se basa en el concepto de UMF.

En un futuro próximo también será posible que una consulta realizada a través de la aplicación Arcos de la Policía Nacional pueda tener el resultado de la consulta en el sistema de información de Europol; es decir, en primer lugar se está desarrollando en fase piloto, pero más adelante el objetivo es que se haga a través de las aplicaciones de la Policía Nacional en este caso y, en el futuro, de todas las autoridades competentes en la materia.

PARTICIPANTES UMF3 Y PROYECTO PILOTO

- UMF3: Alemania, Austria, Bulgaria, Estonia, Finlandia, Grecia, Hungria, Italia, Letonia, Lituania, Malta, Holanda, Polonia, España, Suecia y Noruega.

- Quest: Estonia, Finlandia, Polonia, España, Grecia y Alemania.

España es líder en esto, es lo que quiero reflejar y dejar claro.

La primera fase, la fase inicial, es un acceso limitado. Estamos en fase de pruebas y se trata de restablecer un sistema que nos permita ejercer. Esta serie de consultas al sistema Europol solamente datos de personas: nombre, apellidos, fecha de nacimiento, y por otro lado, armas, en cuanto a su número de serie, devuelve otros datos adicionales que son el sistema de información de Europol, sobre esa persona o ese arma. Ese sería el objetivo, muy sencillo, pero para iniciar el proceso.

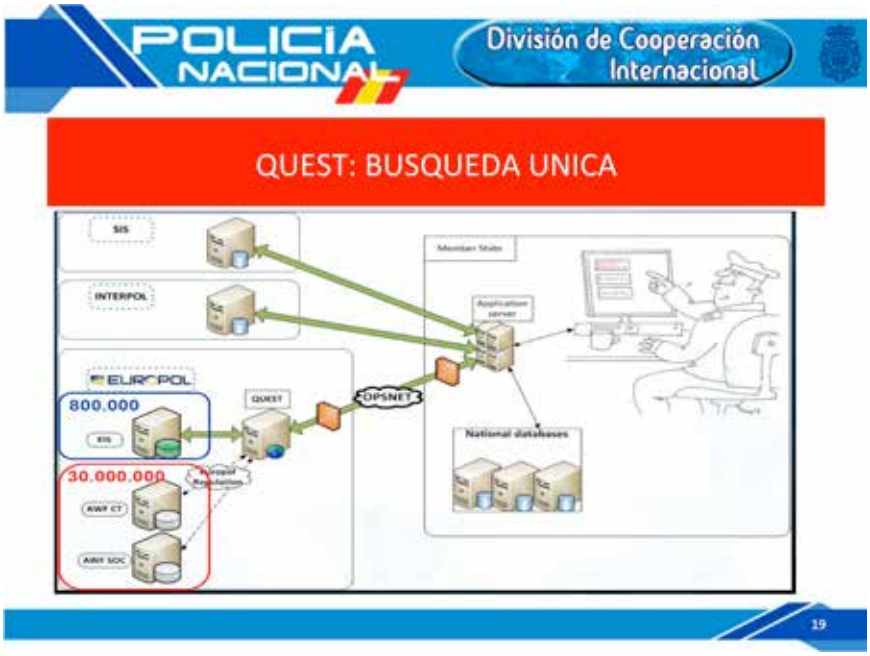
QUEST. PROYECTO UMF3 FINANCIADO POR ISF

Desde la unidad de Europol han diseñado distintos niveles de acceso, propuestos en el proyecto español, a través de la consulta Quest:

- Nivel 1: acceso total a los datos de personas y armas obtenidos en una consulta Quest con indicación además de los datos básicos previstos, de los relativos a códigos de manejo, (los que permiten el acceso a la información que tiene Europol hasta unos determinados límites, según el propietario de la información lo determine, es muy importante porque genera confianza en el trasiego de información con la agencia) nacionalidad, país proveedor, titular de los datos, observaciones (*warning*) y referencia. Este nivel está reservado a la Unidad Nacional de Europol, porque está dentro de la División de Cooperación Internacional de la Policía Nacional, incorpora funcionarios de otras autoridades competentes, con responsabilidad en la lucha contra el crimen organizado; es decir, no es solo de la Policía Nacional.

- Nivel 2: acceso a datos de personas y armas así como observaciones (*warning*) y código de manejo. Este nivel de usuario se correspondería con un número limitado a convenir de usuarios en Unidades Centrales de Inteligencia en Policía Nacional (UCIC; CIAR, CGI) y, cuando técnicamente sea posible, al resto de autoridades nacionales competentes. (Guardia Civil, Policías Autonómicas y DAVA).

- Nivel 3: acceso básico a hit/no hit con indicación de nombre, apellidos, fecha de nacimiento y referencia, con un mensaje en el que se informa al usuario de que para obtener datos a este respecto se dirija a la Unidad Nacional de Europol. Este nivel de usuario correspondería a unidades de investigación de Policía Nacional y Autoridades Nacionales competentes.



Esto es un esquema de cómo funciona la búsqueda, es un esquema sencillo, "un cliente ligero" donde se introduce la consulta y devuelven la información que tienen uno y otro. Las decisiones operativas le corresponden al operativo. Es muy sencillo de utilizar no tiene ningún condicionante, pero sí tiene el interés de poner la información de Europol a disposición de todos los actores en la materia. Es una de las grandes quejas, incluso políticas, ya que se quejan de que no tienen acceso a la información de Europol. No es cierto, la información de Europol está accesible a través de la unidad de información para todos los que tengan necesidad de ella y con su propia responsabilidad, sus competencias o sus funciones. La unidad nacional ejerce de ello, no se imaginan la cantidad de información que, a diario, sale de la unidad de información y la cantidad de investigaciones que se coordinan.

QUEST ESPAÑA: IMPACTO ESTRATÉGICO

Es importante que sepamos que no todos los Estados miembros de la Unión Europea contribuyen de la misma manera al Sistema de Información de Europol, sobre todo saber que la mayoría de las aportaciones no tienen que ver con investigaciones activas. Las investigaciones activas se coordinan normalmente a través de los "*focal points*", o a través de los ficheros, incluso estableciendo equipos conjuntos de investigación. Por ejemplo, la fecha de enero del año 2018, el sistema de información del Word tiene más de un millón de objetos o entidades: personas, armas, cuestiones específicas iden-

tificables dentro de las distintas entidades que se pueden meter dentro del sistema de información de Europol.

¿Se pueden imaginar lo que ha supuesto, desde el inicio, la estrategia de control de los desplazamientos de los *foreign fighters* hasta ahora, la explosión de entrada de información que ha supuesto esto en Europol? Eso lo hemos vivido en directo, les aseguro que jamás se ha visto una cosa igual. Actualmente, Europol no se ve capaz de gestionar tanta información, tienen necesidades tecnológicas y de recursos para gestionarlo y, también, de presupuesto; tienen setenta y tantos millones de presupuesto, desde hace ocho o nueve años, y ahora tienen ciento y pico. La Unión Europea tiene claro esto.

Me gustaría resaltar otra vez el papel de la unidad nacional de Europol, la gestión de todas estas consultas, de toda esta información, desde el punto de vista de España.

¿Cómo funciona esto? la Unidad Nacional recibe una comunicación indicando que se ha producido un hitter en el sistema de consulta *Quest* del que estamos hablando, y los datos necesarios para identificar la consulta. Se inician gestiones para ampliar la información: tipo de delito, objeto relacionado, persona, zona, vehículo…, toda la información que figure en el sistema. Asimismo, saber si esa persona ha sido ya consultada por otra unidad de investigación e inteligencia: ADEP, Siena -que es el canal seguro de Europol-, y esto es importante a la hora de coordinarlos. Y, sobre todo, para evitar el acceso inadecuado a datos que puedan comprometer investigaciones. Si nos cargamos esto, nos cargamos la confianza en el sistema. Es importante

que sepamos coordinarnos y respetarnos mutuamente. También permitiría poner en evidencia posibles cruces con otras consultas relacionadas con la Unión Europea. Fíjense el trabajo que esto genera, es una unidad de inteligencia y coordinación al mismo tiempo que conlleva todos los datos que figuran en el sistema que incorpora toda la información que le dan los Estados miembros.

QUEST ESPAÑA: IMPACTO OPERATIVO

- La descentralización del acceso a consultas básicas del Sistema de Información de Europol. Para nosotros es un objetivo esencial. La queja recurrente es que no está a disposición de las autoridades competentes. Sin embargo, Europol lo pone a disposición de todo el mundo. La idea es que esto sea real sin necesidad de tirar de la unidad de información de Europol, que la consulta se realice de forma descentralizada. El objetivo último de este sistema, que el investigador autorizado tenga acceso al sistema de información de Europol inmediatamente. Ese es el objetivo último y en eso estamos trabajando, creo que estamos en la línea adecuada y se va a conseguir.

- Mayor número de usuarios en Policía Nacional y resto de autoridades nacionales competentes.

- Consulta básica rápida sobre la existencia de vínculos internacionales en sus casos abiertos.

- Apoyo a Unidades de inteligencia en coordinación nacional e internacional de investigaciones con conexiones transfronterizas, evitando duplicidades y solapamientos.

Me gustaría mencionar otras iniciativas que estamos llevando desde la Policía Nacional en aras de la intemporalidad de los sistemas. Estamos convencidos de que los sistemas deben ser interoperables en la Policía Nacional, nosotros somos los principales promotores a nivel nacional y europeo, porque creemos en ello y además, tenemos la experiencia y el conocimiento suficiente en materia de cooperación internacional para saber que esa, es la herramienta fundamental, el intercambio de información.

OTROS PROYECTOS PARA LA INTEROPERABILIDAD Y DE APOYO TECNOLÓGICO DE LA POLICÍA NACIONAL CON LAS POLICÍAS DE OTROS PAÍSES

- ADEP.- Proyecto por el que se desarrolla una tecnología de acceso a los antecedentes policiales en todos los Estados miembros de la UE. Va a permitir el intercambio de antecedentes policiales con carácter inmediato. Es importantísimo, va a ser posible y muy pronto.

- SIENA CT.- Desarrollo informático que posibilite la acreditación de seguridad al nivel Confidential EU. Lucha contra el terrorismo. Se trata de alcanzar el estándar confidencial de la Unión Europea, requisito esencial para el intercambio de información en la lucha contra el terrorismo.

- Proyecto Kenitra: detección de documentos falsos de viaje de la DGSN marroquí. Con esto le estamos proporcionando a Marruecos hardware, software, en materia de control de fronteras muy importante. Marruecos es un socio estratégico como sabemos, el control de fronteras en Marruecos es prácticamente el control de fronteras en la Unión Europea. La cooperación con ese país es estratégica y el proyecto, financiado por la Unión Europea, es determinante.

- Proyecto de desarrollo de capacidades en frontera en Nigeria.

- Proyecto de Lucha contra el Crimen Organizado Euroasiático.

- Proyecto de Apoyo a Ameripol. SIPA. A principios de agosto se va a firmar "la declaración de Buenos Aires", España es el país promotor de esta iniciativa que va a intentar en el futuro conectar con Europol, la vocación española de ser puente entre América y Europa se manifiesta

claramente en esta iniciativa. El SIPA es el sistema para intercambiar datos.

- Con Argentina, Memorándum de Entendimiento recientemente firmados con las fuerzas policiales federales dependientes del Ministerio de Seguridad Nacional: Argos, Icaro, DIFO, GATI, ASIA, Alertcops.

CONCLUSION

La verdadera apuesta de "presente", no ya de futuro, en la cooperación global en la lucha contra las amenazas más graves, es la generación de sistemas de información con un alto grado de interoperabilidad, sino totalmente interoperables que sería lo deseable, que permita la disponibilidad de toda la información que sea relevante para los policías en el momento en que la necesiten para ser efectivos y eficientes, con pleno respeto a los Derechos y Libertades Fundamentales de las personas, en particular la privacidad y la protección de datos personales.

Esta es ya la principal área de Investigación, desarrollo e innovación en la que nos estamos moviendo junto a nuestros socios y amigos y proyectándonos, allá donde sea necesario, para abordar, como decía, las amenazas globales contra nuestro modo de vida.

EL CENTRO TECNOLÓGICO DE SEGURIDAD DEL ESTADO DEL MINISTERIO DEL INTERIOR

ENRIQUE BELDA ESPLUGUES
Subdirector General de Sistemas de Información y Comunicaciones para la Seguridad de la SES

Creo que uno de los problemas más importantes que tenemos es el control en fronteras, e intentando llegar hacia esa real desmaterialización de las fronteras, gracias a la tecnología no necesitemos pedir cien veces lo mismo, puesto que, por ejemplo, si ya hemos dado nuestros datos biométricos, somos capaces de que con esos datos nos identifiquen sin necesidad de hacer eternas colas como pasa en los aeropuertos.

España se está convirtiendo en un referente tecnológico, aunque creo que nos falta algo que es vender las cosas; es decir, que hacemos las cosas bien y no nos damos ni cuenta. Tenéis unos sistemas de comunicación obsoletos pero robustos y que van modernizándose poco a poco como el SIRE que es capaz de enlazaros a Policía, Guardia Civil, UME, Servicios de rescate y el DABA. En nuestro entorno hay países donde todavía los dos grandes cuerpos no se hablan entre ellos y tienen un sistema igual que el nuestro tecnológicamente, ¿por qué le hemos dado ese valor añadido al sistema?, ¿cómo hemos sido capaces? Es que no nos vendemos, nos falta contar las cosas que hacemos y con un factor de escala importante y aquí es donde yo quería iniciar la conferencia de hoy, el por qué hemos creado este centro tecnológico que, además, entre sus encargos tiene lo que es motivo de las conferencias de hoy, la I+D+i.

Ese factor de escala tan importante que es tener un país con cuarenta y cinco millones de habitantes, tener unas Fuerzas y Cuerpos con una dimensión notable; que aunque siempre nos falta personal, nos falta dinero…, pero que, sin embargo, el problema es que nos falta agilidad en la gestión

de determinadas soluciones que, además, no es por la parte de la tecnología, es porque se aclaren determinados términos jurídicos, que nos permitan acabar de lanzar las tecnologías. En España, fuimos los primeros en acabar el PNR, pero no se ha traspuesto la Directiva con lo cual vamos a ser el último país de Europa en ponerlo en marcha. Muchas veces no vamos a la misma velocidad en un sentido y en el otro. En muchas ocasiones, necesitamos dictámenes jurídicos que nos permitan consolidar soluciones tecnológicas. La tecnología es facilísima, el problema es ajustar la tecnología a los requerimientos legales. Ese es el gran problema. Porque la tecnología, hoy, lo puede alcanzar casi todo; pero en ese casi todo muchas veces vulneramos derechos debidamente establecidos. Y para no vulnerarlos, necesitamos que los expertos en la materia nos indiquen cuáles son los límites que no debemos vulnerar, porque la tecnología nunca hace aquello que no sabes hacer, siempre hace aquello que sabes hacer de una manera mucho más rápida y eficiente. Pero, jamás, hace nada que no sepas hacer.

Volviendo al factor de escala, yo he encontrado en las Fuerzas y Cuerpos de Seguridad del Estado, una capacidad, un estilo, unos valores y, sobre todo, esa gran variedad de oficios, profesiones; son auténticos genios. Muchas veces las propias evoluciones profesionales, dentro de los Cuerpos, no pone a todo el mundo donde debería ponerlo, porque si te encasillas en uno de los sitios te obliga a acortar una promoción profesional y eso debería estudiarse.

Soy de los que piensan que todo el mundo es un genio, lo que pasa es que cada uno necesita saber dónde es un genio y en qué es un genio. Una de las cosas que me gustó en mi experiencia de estudiar en la Administración francesa, fue la organización de estado que tienen en Francia, cómo está estudiada esa movilidad horizontal y transversal, por lo menos teóricamente, luego en la práctica será la que sea, pero cómo te permite en tu carrera profesional tener una evolución horizontal o transversal que te posibilita crecer de alguna manera. Luego vienen los especialistas, ellos lo tienen más crudo, porque el que hacen experto en hormigones de alta resistencia -recordando mi pasado laboral- como comprenderéis poco juego tiene en otras unidades que no sean hormigones de alta resistencia. Ahí es donde uno tiene que tener la evolución vertical muy asegurada para poder hacer coincidir la genialidad de cada uno con el desarrollo profesional. Esto es un reto que los de recursos humanos tienen que tener en cuenta porque hay auténticos genios informáticos patrullando en las calles y que yo daría cientos de miles de euros para poder tenerlos en el Centro Tecnológico de Seguridad; pero, si a esta persona se la retira de la calle, y se lleva al Centro, alguien la tiene que sustituir.

Este es un reto importante, y a partir de ahí arranco en este gran mundo que son las Fuerzas y Cuerpos de Seguridad, empezando con la tecnología

y acabando con la innovación, y lo que creo sigue a la innovación; porque la investigación y el desarrollo, al final es el embrión, el nacimiento, de todo país evolucionado, pero no puede quedar solo en investigación y desarrollo, porque necesita una innovación, y la innovación necesita llegar al mercado; porque si no llega al mercado, el país no evoluciona y, además de no evolucionar, son recursos económicos ingentes desperdiciados en papel o en "cacharreo". A partir de ahora lo que se necesita es que esto sea útil para aquellos que lo necesitan y lo primero que hay que hacer es escuchar.

INTRODUCCIÓN AL CENTRO TECNOLÓGICO DE SEGURIDAD (CETSE)

Arranco con la tecnología, lo primero que nos encargan en el año 2011 es ordenar esa gran necesidad que empezaba a haber en las Fuerzas y Cuerpos de Seguridad y que el factor de escala podía hacer que, si no se desarrollaba de una manera lógica y coherente, no hubiese presupuestos generales del Estado capaces de sostener la evolución de esa tecnología. Yo siempre pongo el ejemplo de que si un iluminado decidiese que todos los miembros de las Fuerzas y Cuerpos de Seguridad del Estado de este país, necesitase una chocolatina para sostener sus niveles de azúcar en la actividad diaria, a la Secretaría de Estado de Seguridad le costaría veinticinco millones de las antiguas pesetas, cada día, o ciento cincuenta mil euros cada día. Al final, estamos hablando de proyectos, que en Policía está la movilidad, el tema de la dotación de equipos móviles …, lo que no pueden ser son ingentes compras, por ejemplo de ordenadores; y pasarse cinco mil de ellos guardados en un almacén durante cuatro años. Que cuando los hemos sacado de sus cajas, ya no rodaba la nueva versión de Windows.

Estas cosas son fundamentales, ese equilibrio, esa racionalización, es lo que me pedían y yo creo que lo conseguimos en la Dirección General de Tráfico, donde en el plazo de seis años pusimos en marcha el Plan Nacional de Control de Velocidad, el de radares, el centro de tratamiento de denuncias automatizadas, los centros de control, la monitorización de las carreteras y, por supuesto, la recepción de todos esos datos con capacidad para gestionar. Y aquello se convirtió en que, desde el año 2004 hasta el 2012, en España se redujo el número de víctimas mortales en carreteras en un 69,5%. Algo tendría que ver todo ese orden en las medidas; porque al final, toda esa tecnología lo que hacía era poner en marcha aquella famosa filosofía del carnet por puntos que solamente alguien es capaz de trasladar a la sociedad cuando, quien infringe es localizado de manera inmediata y, por supuesto, "detenido" en el mundo del tráfico con su correspondiente "receta" encima de la mesa.

Todas estas cosas son las que a nosotros, de alguna manera, nos pedían.

Las amenazas, en este momento, van asociadas a la tecnología, y muchas veces sabemos que, asociados al ataque físico de la matanza que es lo que nos impacta, ha habido ataques tecnológicos a diferentes sistemas que han impedido que la reacción ante esa amenaza haya sido la debida, por ejemplo, el problema que teníamos el 11M del año 2004, asociado a aquel reparto tan dramático de explosivos en los trenes, amenaza de bomba a centros de control de tráfico, a centros sanitarios; para todo, de alguna manera, generar el caos absoluto, de tal forma que no se controlasen los flujos, que se colapsasen las carreteras, que se impidiese el acceso a determinados centros médicos, que son los que al final atienden. Todo esto había que ordenarlo, lo que no podía ser era empezar a adquirir, sin ton ni son, soluciones en el mercado que, por supuesto, funcionan todas las Demos que presentan, pero cuando se arranca en el día y a ver qué pasa, es cuando empiezan a aparecer los problemas. Sabemos, que hay países que venden soluciones con ocho cifras y no han bajado. Europa tiene que empezar a, si otros países son capaces de hacerlo, nosotros tenemos que subirnos a ese carro. Pero para eso tenemos que tener claras cuáles son las necesidades y a partir de ese momento empezar a funcionar.

Para eso se creó el Centro Tecnológico de Seguridad. Este centro es un paraguas, es una filosofía realmente y tal como marca el Real Decreto de Estructura Orgánica Básica, quien lo dirige es el Subdirector General de Sistemas de Información y Comunicación para la Seguridad y lo que le da esa cobertura de centro tecnológico que le permite poner en marcha, de una manera centralizada, todo aquello, no solamente lo que es de sistemas de comunicaciones y sistemas de información para la seguridad, sino lo que va más allá, que es la innovación y el desarrollo.

Ahora es I+D+i, y hubo una temporada en el séptimo programa marco, que era I+D+i+d, en que se utilizaban los cuatro términos, y la "d" significaba despliegue que es a lo que tenemos que volver, porque si no hay despliegue de lo que precisamente primero se ha investigado, desarrollado, innovado; no sirve para nada.

SUBDIRECCIÓN GENERAL DE SISTEMAS DE INFORMACIÓN Y COMUNICACIÓN. ESTRUCTURA MINISTERIAL

Como habéis visto, en el Cetse tenemos la Subdirección General de Sistemas de Información y Comunicaciones para la Seguridad (Sgsics) y el Centro Nacional para la Protección de las Infraestructuras Críticas y Ciberseguridad (Cnpic). El Cnpic es un usuario de esa tecnología. Ellos, por un tema de sinergia, están en el Centro Tecnológico porque realmente necesitan mucha infraestructura tecnológica para acometer sus responsabilidades.

En este momento, se ha pretendido centralizar bajo ese Ffccse lo que en el lenguaje empresarial se llama *Chief information officer* que es el responsable de toda la parte de información del Ministerio del Interior. Había otra Subdirección General TIC, en la Subsecretaría y todas las competencias en ejecución de sistemas se han centralizado en una única unidad y en este momento somos noventa funcionarios y miembros de las Fuerzas y Cuerpos de Seguridad del Estado, y ciento treinta personas externas. Y me gustaría aclarar que, el hecho de que sean externas no significa que estemos externalizando, externalizamos horas hombre, de técnicos especialistas en según qué materia; el conocimiento, el knowledge, queda en la Secretaría de Estado de Seguridad, porque la alta competencia de los miembros, en este caso la parte de seguridad de las Ffccse que están en este momento trabajando, es muy superior a todas las competencias de las horas hombre que estamos contratando en la calle. Lo único que pasa es que uno es especialista absolutamente de todo y lo que buscamos en la calle son expertos en: desarrollo de big data y en comunicaciones D, y esto, una vez realizado su trabajo, se deposita. Por eso es tan importante la creación del Centro Tecnológico.

Nosotros, al principio teníamos seis grandes bloques, porque estamos gestionando ciento treinta y tres proyectos. Decía antes Mario Hernández Lores que somos los conseguidores, pues es cierto, decimos que sí a todo, porque si alguien nos lo pide, lo hace por algo, porque lo necesita; y hay que decir que sí. Luego, las circunstancias legales, la típica broma de "se cierra el año en el mes de julio" eso impide muchas veces responder; es decir, me impide desarrollar los proyectos porque hay un corte, pero eso es lo único que nos ha cerrado en muchas ocasiones, nunca la falta de presupuesto. Esa palabra en las personas que trabajamos en la Dirección no existe, no existe la falta de presupuesto, lo que existe es: no hemos abierto el año, alguien nos ha dicho que nos hemos quedado al 50%, no podemos tramitar más allá del 50%, en vez de cerrar en diciembre, nos cierran en julio…, pero el dinero está, la idea está y el inicio del expediente está. Por tanto, tenemos personas muy válidas y dinero suficiente para intentar llevar adelante todo. Entonces, lo que hemos hecho ha sido encerrar los proyectos, de alguna manera, en ocho grandes bloques:

El sistema de comunicaciones, donde hemos incluidos los dos grandes proyectos que está haciendo la Administración del Estado. Los proyectos más grandes son el Sirdee y el Sistema Unificado de Comunicaciones. El Sirdee es un proyecto de trescientos sesenta millones de euros (360 M) a cuatro años, y el Sistema Unificado de Comunicaciones es un proyecto de doscientos sesenta y cuatro millones de euros (264 M). Esto nos hace sentirnos orgullosos, que los mayores proyectos en cuanto a volumen económico que el país está generando, estén en manos de las Ffccs, es un motivo de

orgullo porque es la confianza y sobre todo saber que aquellos que decidan hacerlos piensan que es necesaria una relación de confianza en los que lo van a necesitar.

Luego tenemos el tema de Interceptación Legal y Conservación de Datos, que aparte de clásico lo que conseguimos con el cambio conceptual de modelo de compra, adquisición, pasar al modelo servicio; nos ha permitido de una manera muy eficaz adaptarnos a las evoluciones de la tecnología. Hay que definir un modelo de gestión que nos permita ir al mismo ritmo que evoluciona la tecnología. Aquí no sirve aquello de "se me ha quedado la Comisaría vieja" y durante años hago el proyecto, lo adjudico, porque cuando lo construya, lo más probable es que tenga ocho o nueve años hasta que se vuelva a quedar obsoleta; pero en el tema tecnológico cuando lo adquiero, ya se ha quedado desfasado. Con lo cual, es algo que necesitamos cambiar.

El tema de Schengen y Fronteras Inteligentes: sistemas de inteligencia y coordinación de operaciones que trabajamos con la Comisaría General de Información, con el Centro de Inteligencia contra el Terrorismo (Citco) y con los servicios organizados de Policía y Guardia Civil, porque nosotros somos fabricantes tecnólogos a disposición de las necesidades de los Cuerpos e intentamos hacer las cosas con orden, tenemos soluciones que transmiten la coordinación que las Fuerzas y Cuerpos de Seguridad tienen sobre todo en su horizonte medio y de ejecución, por ejemplo, el tema de las balizas. El contrato de mantenimiento de las balizas es el mismo contrato para Policía y Guardia Civil, se gestiona exactamente igual. Y creo que todo aquello que desarrollemos tiene que estar pensado para que lo desarrolle quien lo pida y lo necesite pero siempre con la capacidad de que si otro pide y necesita algo igual, por dos motivos A) porque lo necesita o B) porque lo tiene otro y yo también lo quiero; es decir, que estas cosas sean escalables, no tenga que volver a inventar la rueda porque, repito, con ciento cincuenta mil (150 m) efectivos, no hay Presupuestos Generales del Estado que sean capaces de adaptarse a la evolución de la tecnología.

También tenemos las bases de datos de intercambio de datos, es muy importante, por una parte hay bases de datos centralizadas, distribuidas, centros de compensación para pasar datos, pero lo más importante es la calidad del dato. La Comisaría General de Científica o Criminalística en Guardia Civil tienen que generar datos de calidad, porque si los datos no son de calidad, no estamos haciendo nada. Podemos tener unas extraordinarias bases de datos, podemos tener unos dispositivos móviles que nos permitan recibir los datos; pero, los datos han de ser de calidad.

Proyectos de seguridad que hablamos en general, pero que son los más

dispersos: Desde el PNR, el Alertcops, y los dos últimos que es toda la gestión del día a día de aplicaciones y portales web en el Ministerio: puestos de trabajo, desarrollos y toda la gestión de infraestructura de comunicaciones del Ministerio. Hemos hecho una estructura totalmente matricial, por una parte tenemos los sistemas de información y a quien le damos cobertura; por otra parte están las comunicaciones y a quien le damos cobertura y en medio de todo ello es en lo que nosotros nos estamos centrando en este momento que es en la I+D+i, en seguridad; y en la transformación digital del Ministerio. La transformación digital del Ministerio, de momento, queda fuera de este ámbito; para nosotros la Policía y Guardia Civil, pero estamos a disposición para que todos los avances que hagamos en el Ministerio sean útiles para Policía y Guardia Civil y se puedan extender, pero hay otros responsables dentro de cada Cuerpo para poderlo hacer.

Identificar qué proyecto estamos haciendo y a quién le damos servicio es nuestra misión; hay casos en que es al propio Ministerio del Interior y también a las cinco Fuerzas y Cuerpos de Seguridad del Estado de este país, pero también hay otros usuarios: La Armada, la UME, el Citco, La Comisión Europea, Europol, el TIC, Casa Real, Presidencia de Gobierno; y a todos les damos servicio ¿Cómo lo hacemos? Dependemos directamente de la Secretaría de Estado de Seguridad, junto con el Gabinete de Coordinación, la Inspección, la Gerencia de Infraestructuras, la Subdirección de Planificación y el Citco, somos una Subdirección más.

SUBDIRECCIÓN GENERAL DE SISTEMAS DE INFORMACIÓN Y COMUNICACIÓN. FUNCIONES DE LA SGSICS

Lo que es importante son las competencias que el BOE marca:

- Planificar, coordinar y, en su caso, gestionar las inversiones en sistemas de información y comunicaciones, teniendo en cuenta las propuestas de las Direcciones Generales de la Policía y de la Guardia Civil.

- Estandarizar y homogeneizar sistemas de información y comunicaciones, codificación y estructuras de datos en el ámbito de la seguridad.

- Proponer al Secretario de Estado los planes y programas que afecten a los sistemas de información y comunicaciones en el ámbito de la seguridad, así como coordinarlos, supervisar su ejecución, evaluarlos y analizar sus costes.

- Promover proyectos para la implantación, adquisición y mantenimiento

de sistemas de información y comunicaciones para la seguridad, incluyendo expresamente aquellos de utilización conjunta o compartida por las Fuerzas y Cuerpos de Seguridad del Estado, así como los dirigidos a garantizar la seguridad ciudadana a través del uso de las tecnologías de la información y las comunicaciones; coordinar y supervisar la determinación de sus requisitos técnicos, pliegos de condiciones, programación económica y ejecución, así como cualesquiera otras acciones necesarias para llevar a término los proyectos promovidos en esta materia por unidades u órganos dependientes de la Secretaría de Estado de Seguridad, cuando se financien total o parcialmente con créditos del servicio presupuestario de la Secretaría de Estado.

Y hay cosas tan fundamentales como las que son de utilización conjunta o compartida, aquellas dedicadas a la seguridad ciudadana a través del uso de las tecnologías:

- Controlar y coordinar la ejecución de los programas y proyectos derivados de compromisos contraídos por España con otros países u organismos internacionales, en las materias propias de su competencia.

- Gestionar y ejecutar los programas y proyectos de sistemas de información y comunicaciones derivados de la financiación procedente de Fondos Europeos o de otros organismos internacionales que expresamente se le encomienden, incluyendo los provenientes de las Fuerzas y Cuerpos de Seguridad del Estado.

- Coordinar, desarrollar e implantar bases de datos, sistemas de información y sistemas de comunicaciones de utilización conjunta o compartida por las Fuerzas y Cuerpos de Seguridad del Estado, incluyendo aquellos relacionados con la Agencia Europea para la Gestión Operativa de Sistemas Informáticos de gran magnitud en el Espacio de Libertad, Seguridad y Justicia (eu-LISA), los correspondientes al Sistema Schengen y al Sistema de Radiocomunicaciones Digitales de Emergencia del Estado (Sirdee).

Esto también destaca por su importancia como epígrafe dentro del Real Decreto:

- Acordamos, coordinamos, ejecutamos y llevamos a cabo cualquier otra acción necesaria relativa a la participación en proyectos europeos de investigación, desarrollo e innovación (I+D+i) en materia de seguridad de acuerdo con las instrucciones del Secretario de Estado.
- Dirigir el Centro Tecnológico de Seguridad (Cetse) como órgano de

implementación de las funciones específicas de esta Subdirección y de las políticas de I+D+i del órgano Directivo.

- Bajo la dependencia funcional del Subsecretario, ejercerá las funciones a las que se refieren los párrafos r) y s) del apartado 3 del artículo 7.

Formamos este equipo (Imagen 1) que es el que se dedica a estos trabajos y ¿por qué hemos decidido montar un Centro Tecnológico de Seguridad? Desde hace tiempo, me reúno con los informáticos en estas comisiones TIC y hace ocho años oía unas cosas y vuelvo ahora y oigo las mismas cosas; entonces, cuando se monta un grupo de trabajo está bien, pero lo que sale del grupo de trabajo, sobre todo si son varios grupos de trabajo, cada uno dedicado a una cosa, no se sabe cómo va a acabar esto, ¿qué va a nacer de esto?, ¿algo seguro?, porque todo el mundo tiene que justificarse pero ¿qué queremos nosotros?

CETSE.Visión 360º

Imagen 1

Arrancamos por planes. Nosotros queremos planificar, es nuestro trabajo, queremos redactar los proyectos, programarlos. Nunca hemos impuesto condiciones porque han sido ellos los que nos han dado sus necesidades y nosotros hemos hecho lo que ellos han necesitado, nada más; y cuando se

habla de soluciones, son las necesidades de esa unidad y las que nos ha tras-
126 ladado. En algún caso, lo hemos hecho con horas hombre nuestras, en algún caso con horas de la calle; ahí están fundamentalmente las grandes soluciones que tenemos que dar. Entonces, nosotros planificamos proyectamos, programamos, hacemos la consultoría, el control del desarrollo, la coordinación entre las unidades que participan, porque como he comentado antes, nosotros no somos nadie, simplemente somos gestores de necesidades, pura intendencia tecnológica y estamos orgullos.

Y la estandarización y armonización y he quitado la homologación que solamente existe cuando hay una norma y un laboratorio acreditado que es capaz de dictaminar que el producto se ciñe a la norma. Y nosotros no somos eso. Es decir, aquí no homologamos lo que hacemos es armonizar. Lo que hagamos que sea por todos, de la misma manera, que la solución sea la misma, que tengamos desarrollos armonizados y homogeneizados.

También es importante promocionar, vender lo que hacemos, hacer la I+D+i, evaluar si sirve para algo y, por supuesto, intentar a nivel internacional decir: esto es lo que hacemos.

Las sinergias que se crean y como el STSE pretende ser en temas tecnológicos el buque y cómo en el mundo industrial lo que pretendemos es que se vaya acoplando dentro de estos grandes bloques.

Si se fijan en la imagen superior, la orquesta, todos podemos tocar igual

de mal o igual de bien, pero toquemos todos la misma partitura. Vemos como hay unidades dentro de los mismos Cuerpos y se toman soluciones diferentes para casos similares. Eso es lo que hay que impulsar.

El Cetse y el futuro de las tecnologías para la seguridad, son más de cien proyectos.

PROYECTOS DE LA SGSICS + 100 PROYECTOS

En estas ocho áreas se desarrollan los proyectos:

- Sistemas de Comunicaciones.
- Schengen y Fronteras Inteligentes.
- Bases de Datos de Seguridad.
- Interceptación legal y conservación de datos.
- Sistemas de inteligencia y coordinación de operaciones.
- Proyectos de seguridad.
- Gestión de aplicaciones y portales Web ministeriales.
- Gestión de la infraestructura TIC del Ministerio.

Por ejemplo, en el tema de los Sistemas ABC, hemos cumplido nuestro trabajo, ponerlo en marcha. Pusimos en marcha los ABC, primero fue una prueba piloto que se hizo en el año 2008, aquello se paró, pero vimos que era bueno y actualizamos los sistemas de captación de huella dactilar, de biometría, y pusimos en marcha ciento veintisiete puestos (127): en aeropuertos, en pasos fronterizos, en la Línea y en puertos en Algeciras. Creamos tres centros de gestión que reciben información para la toma de decisiones y a partir de ese momento ya desarrollamos, para los centros de gestión, para los gestores del centro, aquello que los gestores del centro quieran desarrollar.

En el tema de la ampliación que AENA quiere hacer de esos ciento veintisiete puestos, porque se vio que el año pasado era bueno en aquellos sitios donde estaba, pero como se cedió la tecnología y la forma de hacerlo, es Policía y AENA quienes se están encargando de llevarlo adelante. Nosotros estamos para lo que necesiten de la tecnología pero nuestra misión es poner en marcha las cosas; porque ya no es Policía quien la invierte, es AENA; pero si el usuario es la Comisaría General de Extranjería y Fronteras, pues de acuerdo con ellos, con el soporte tecnológico nuestro y de la propia logística de Policía, arranca con esto.

CETSE - COORDINACIÓN DE PARTICIPANTES EN SEGURIDAD PÚBLICA

Sistemas de información para la Seguridad:

- Base de Datos de ADN.
- Sistema Automático de Identificación Dactilar (SAID).
- Sistema Automático de Identificación Balística (SAIB).
- Registro de nombres de pasajeros (PNR).
- Sistema Europeo de Información de Licencias de Conducción (Eucaris).
- Sistema de Información Avanzada de Pasajeros (APIS).

- Sistema de Información Schengen (SIS-II).
- Otros sistemas y bases de datos.

FUTURO DE LAS TECNOLOGÍAS PARA LA SEGURIDAD

En la parte de I+D+i, lo que pretendemos con el Cetse es centralizar la representación del Ministerio, para que no pase lo que ocurrió con el PNR. Se hace un proyecto y aparece por un lado un proyecto que se manda a Bruselas de Policía, un proyecto que se manda a Bruselas de Guardia Civil… España es un país, y tiene que haber alguien para centralizar; luego está el tema de las competencias. Al final, las leyes o se cumplen o se cambian, lo que no se puede hacer es saltárselas. Lo que hay que hacer es centralizar e identificar oportunidades de financiación porque, muchas veces, el problema al arrancar proyectos es a la hora de gestionar el retorno de Europa. Hay que pensar en cómo hacer una única unidad para gestionar el retorno, porque hemos llegado a tal nivel de proyectos europeos que con los actuales recursos humanos, no tenemos problema, pero hay que decir que falta gente, preparar un equipo para hacerlo; porque no podemos perder recursos de Europa por no hacer la siguiente parte. Tenemos que hacer los papeles porque si no: a) no vendemos = no damos a conocer lo que hacemos y b) recuperamos el dinero. Esto es lo que pretendemos y luego apoyar la tramitación de propuestas de Policía, de Guardia Civil y de cualquier otra unidad del Ministerio. Hay proyectos en los que interviene la Dirección General de Tráfico, Protección civil y que podíamos hacer de manera conjunta. Y, por supuesto, impulsar la colaboración entre Administración, Empresa y Universidad.

ACTIVIDADES

¿Qué actividades hacemos?:

- Seguimiento de los principales Programas de I+D+i de cara a la identificación de oportunidades de financiación de iniciativas procedentes de las unidades ministeriales.
- Apoyo a la presentación de propuestas y tramitación de solicitudes de financiación.
- Recopilación de buenas prácticas y gestión del conocimiento.
- Prospectiva y vigilancia tecnológica.
- Propuesta de proyectos de I+D+i.
- Seguimiento del estado y apoyo técnico a la ejecución de proyectos de I+D+i.
- Coordinación con las entidades y organismos relacionados con la

I+D+i.

• Difusión de contenidos y resultados.

Hay unos datos que quiero que conozcan:

Del año 2007 al 2016, gestionamos, en un programa de ocho, con cuatro millones de euros (8,4 M), España estaba en el cuarto y ocupábamos dentro de la Unión Europea el puesto diecisiete. No son países, no son diecisiete de veintiocho, son diecisiete de las más de cien entidades que se presentan para ser receptoras de este tipo de ayuda que no va por países; pero cuando se hizo el ranking entre Ministerios del Interior europeos, éramos los pri-

meros. En particular, del año 2007 al 2013 estábamos en el cuarto lugar, el veinticuatro y éramos el segundo; y en los dos últimos años del 2014 al 2016, hemos vuelto a ser los primeros, está España en el tercero y nosotros en el puesto veintidós.

Si no recuerdo mal, mientras España estaba en general en un 8% al nivel general de proyectos presentados que han sido aceptados por Europa, creo que en el Ministerio del Interior estamos en el doble.

El porcentaje del éxito de los proyectos europeos del Ministerio del Interior viene dado fundamentalmente por dos factores: el primero que se empezó antes que nadie. Empezar en la primera época de número uno, era fácil, porque de hecho todavía a nivel europeo somos los que más partici-

pamos y gracias a la Guardia Civil que tiene unas dinámicas muy logradas de participación. Además, en esos rankings, hace dos años, fuimos la primera entidad europea en recibir la mayor cantidad de dinero; más que cualquier empresa. Efectivamente, todos esos porcentajes y estadísticas son correctos.

Y creo que ahí seguimos. Y lo que yo digo: desarrollo, innovación y producto. Y, sobre todo, lo que hagamos, darle visibilidad y capitalizar, sobre todo, darle rentabilidad.

CoU ORIGEN

Si seguimos con esto, no es suficiente que estemos las Fuerzas y Cuerpos de Seguridad y hay algo que es la Comunidad de Usuarios Nacional de Seguridad, el CoU, la presentamos en el año 2014, se lanza en la Comunidad de usuarios frente a capacidades de resistencia ante desastres, se amplía en el año 2016 a cualquier ámbito de seguridad y en el año 2017, Europa propone a los países que cree Comunidad de Usuarios. Nosotros tenemos la primera reunión en octubre del año 2017, luego en marzo de 2018 lo presentamos a la Comisión Europea y en mayo del año 2018 hemos celebrado la segunda reunión del CoU Nacional en el Cetse.

CoU ORGANIZACIÓN

- La Comunidad Nacional de Usuarios pretende ser un punto de encuentro entre los diferentes Organismos participantes habituales del programa Europeo de Sociedades Seguras, porque seguridad no es solo Policía, Guardia Civil, ni Mossos, ni Ertzaintza, ni Forales. Seguridad es lo que hacen las policías locales con la seguridad vial; no solamente es seguridad ciudadana, es todo aquello que forma parte de la seguridad global. Y hay soluciones que son las mismas para todos, en este caso para identificar a través de análisis de imagen, la biometría facial es la misma que se va a utilizar para saber cuáles son las congestiones de vehículos en los cruces, simplemente hay que parametrizarlo, pero al final es un análisis, pura geometría, matematizas aquello que estás viendo y a partir de ahí, pones una serie de reglas para que se identifiquen una serie de cosas: una cara, unos vehículos, un ancho de calzada. Esto ha evolucionado en los últimos años y esto es innovar, ya no es aquello de

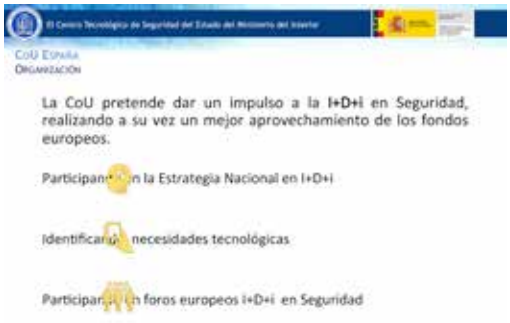
dedicar una cámara para el control de cara, una cámara para el control de coches. Ahora con soluciones globales se puede hacer:

- Una Comunidad abierta, por lo que serán bienvenidas otras entidades que aun no habiendo participado en dicho programa, puedan identificar necesidades tecnológicas en el ámbito de la seguridad. Porque todo el mundo aporta. Y esto es lo que pretendemos.

La CoU pretende dar un impulso a la I+D+i en Seguridad, realizando a su vez un mejor aprovechamiento de los fondos europeos.

- Participación en la Estrategia Nacional en I+D+i.
- Identificación necesidades tecnológicas.
- Participación en foros europeos I+D+i en Seguridad.
- Creación de una red de comunicación entre usuarios de seguridad y desarrolladores.
- Mejoras del aprovechamiento de la financiación externa y, sobre todo, compartir información y recursos.

GRUPOS DE TRABAJO



PROXIMOS PASOS

- Constitución de la CoU como entidad de referencia en los próximos programas marco de la Comisión Europea (FP9).
- CoU como entidad de representación en Europa.
- Continuar con la Integración de nuevos miembros de AA.PP.
- Toma de contacto con Universidades.
- Inclusión de empresas nacionales relacionadas con la innovación tecnológica en Seguridad.

Esto son los próximos pasos en la constitución como entidad de referencia en el noveno programa marco y algo muy importante hay un Instituto de Innovación Tecnológica en Budapest.Y hay un triángulo importante: los usuarios, la industria y la universidad; y como resultado el beneficio que puede proporcionar todo esto, por una mejor comunicación, una mejor colaboración y un mayor beneficio.

Ahí estamos trabajando en el tema de sociedades seguras y un ejemplo, de lo que hemos trabajado en drones ha sido la prueba piloto que nos ha permitido diseñar qué debe ser la I+D+i y volver a añadir la "d" de despliegue que alguien se la ha quitado y no sé por qué.

Para finalizar, una dirección para saber lo que es el CoU.
https://www.securityresearch-cou.eu/

TURNO DE PREGUNTAS

Pregunta en sala: Soy Mª Jesús Llorente, estoy en el área de publicaciones, pero hasta hace poco estaba en Policía Científica en la sección de informática forense y he tenido relación con gente que está contigo y nos decían la importancia del desarrollo de aplicaciones y nos insistían en que había que pedirlas, nosotros las pedíamos. Nosotros los cauces de petición los hacíamos, pero nunca llegaban y al preguntar nos decían que no llegaban, entonces ¿dónde se quedan? También has contado lo del whatsApp, la gente con la que estoy ha desarrollado cómo sacar cosas del whatsApp, rompiéndose la cabeza y ahora me dices que vosotros también los teníais?

Responde: Enrique Belda Esplugues

No, no he dicho que lo hayamos hecho, he puesto el ejemplo y he contado lo del whatsApp por ilustrar el problema de comprar las cosas cuando se necesitan o tener un servicio que, el primer día de la innovación, sea capaz de una manera ágil de ponernos en el mercado a buscar soluciones.

Interviene: Mª Jesús Llorente

Yo veo lo que hacéis y que es importante para las Fuerzas y Cuerpos de Seguridad, nosotros estabamos en la Comisaría General de Policía Científica, un sitio donde tenía que llegar esa información y no nos llegaba. Hemos tenido relaciones con UIT (Unidad de Investigación Tecnológica) y ciberterrorismo de la Comisaría General de Seguridad de Información, estábamos los tres unidos y nos manteníamos para ver si así podíamos ir tirando y no…

Responde: Enrique Belda Esplugues

Ha habido unidades que al no llegar la información han puenteado, los puentes están para salvar distancias y corrientes, han ido directamente y hemos desarrollado cosas. Si es verdad que ahora estamos en una fase de coordinación con logística, estamos trabajando mucho para ser verdaderamente un recurso útil a todos, no aquellos que nos conocen. La primera labor importante fue en el Curso de Comisarios Principales, dedicar dos horas a los futuros Comisarios Principales, que son los que van a tomar decisiones sobre qué en sus unidades, que conozcan el alcance de esta unidad. En el último Curso de Comisarios lo conocían tres, había aproximadamente veintitrés, solo tres conocían lo que hace la unidad. Es una labor que no se hace de hoy para mañana y sobre todo hay que mejorar los cauces. Pero, no se tiene que tomar esta unidad como un financiero porque no lo somos, de hecho lo que hacemos es que financiamos ochenta millones de euros (80M) al año, títulos dos y seis, sin tener presupuesto. No hacemos milagros es que trabajamos contra ocho aplicaciones presupuestarias, de hecho mi secretaría

y la de mi compañero Felipe, que es la que se encarga de gestionar; nosotros cargamos sobre la de Felipe, sobre la 0,1 de la Secretaría, sobre la Dirección General de Tráfico, sobre procesos electorales, sobre Policía, sobre Guardia Civil; es decir, entre nosotros generamos el proyecto y luego, en función de los repartos, se aplica; porque, muchas veces recurren a nosotros porque dicen: Policía no puede comprar un servidor, un sistema que cuesta un millón de euros (1M), comprádmelo vosotros. Pierde un poco la esencia de lo que es el Cetse. El GAT en el que he invertido un millón y medios de euros (1,5M) porque estaba para actualizarlo, porque nosotros teníamos el millón y medio y la Policía no lo tenía, porque si no os quedabais sin él.

Pero esa no debería ser la tarea principal, la tarea principal es planificar de manera conjunta y a partir de ese momento, pedir.

GESTIÓN DE INNOVACIÓN Y DESARROLLO EN LA POLICÍA NACIONAL

JOSÉ FRANCISCO LÓPEZ SÁNCHEZ
Inspector Jefe del CNP. Jefe del Servicio de Innovación y Desarrollo de la Jefatura Central de Logística e Innovación

Mi intención con esta presentación no es explicar lo que yo hago como Jefe de Servicio, ni el servicio en sí, evidentemente voy a hablar de ello, el objetivo de mi presentación va a ser concienciar sobre el significado de la palabra innovación; cómo se tiene que gestionar la innovación, cómo se está gestionando ahora y como se debería gestionar.

La actividad que desarrollamos dentro del Servicio de Innovación y Desarrollo tiene un componente nacional bastante grande y el hecho de comparar la forma de actuación de otras policías respecto de la innovación, o cómo se estructura en otros países la gestión de la innovación, la verdad, da que pensar y tomar nota de cuáles pueden ser los objetivos que debe tener un Servicio de Innovación. Esto es de lo que pretendo hablar:

¿QUÉ ES LA INNOVACIÓN?

En Internet se pueden encontrar diferentes definiciones de innovación todas ellas válidas. Para mí, la forma diferente de presentar la innovación es concienciar sobre ella, pero haciendo pensar. Innovación, cada uno la podemos considerar de una forma diferente: pragmática, tecnológica, relacionado con la gestión de calidad (los ciclos de innovación y gestión de calidad son medianamente paralelos), etc.

UNA VISIÓN DE LA REALIDAD

Para empezar, voy a dar una visión de la realidad. El crecimiento exponencial de la tecnología es grande y sobre todo si tenemos en cuenta lo que

decía la ley de Moore "cada dos años la capacidad de procesado y capacidad de almacenamiento va a multiplicarse por dos". Si hacemos esto, (gráfico 1), la capacidad de almacenamiento en un Micro SD del 2005 al 2014 pasa de ciento veintiocho (128) megas a ciento veintiocho gigas (128). El cambio es

Gráfico 1

importante; hemos cambiado nuestras estructuras, nuestras formas de actuar, ya no hacemos como antes, incluso en la telefonía. Cuando éramos pequeños quedábamos a una hora todos en un sitio y allí esperábamos hasta que llegábamos todos; ahora eso ya no se hace, hay otros sistemas de comunicación más eficaces y eso es porque la tecnología ha evolucionado y no solo en nuestro día a día, sino también en la función policial.

Estamos en unos cambios tecnológicos continuos, el proceso evolutivo nos ha hecho mejorar muchas capacidades, por eso el gran cambio que tenemos que hacer y la innovación, va por ese camino, la mejora de capacidades. La tecnología es un apoyo pero tenemos que utilizarla de una forma correcta en la que se mejore nuestro trabajo diario, y por ende se mejore nuestra forma de actuación policial; que saquemos más rendimiento y hagamos de la tecnología un aliado más para nuestro trabajo diario.

Continuando con la visión de realidad, aquí se presentan algunas frases que he cogido de diferentes sitios y que intento que hagan pensar un poco a los asistentes:

"El cambio está cambiando". No es solo que cambie la tecnología, ni que estemos evolucionando; es que hasta las formas de producir el cambio están cambiando. Ya no se hace un proceso de cambio como antes, ni aun-

que tengamos una mecánica de proceso de cambios, porque incluso eso ha cambiado también; y cuando estamos evolucionando a una nueva tecnología, inmediatamente el proceso de implementación, los procesos de toma de decisiones, están cambiando, porque está apoyado por otra tecnología y otra metodología de cambio. Es decir, la evolución es continua en todos los ámbitos.

"La realidad de hoy no estará de moda mañana". Hoy se implanta una tecnología y mañana es anticuada, tengo que empezar a pensar en el cambio ya durante la implantación.

"Innovas o mueres". Esto es una realidad que también se ha plasmado de alguna forma. La frase es: No es obligatorio sobrevivir. No se pueden utilizar los métodos de hace años, o se cambian, o mueres. Es así de sencillo, no se puede seguir trabajando igual.

"Se debe pensar en cómo hacer las cosas de forma diferente" (los métodos tradicionales de hacer las cosas deben morir) ¿Cuál es la misión de la innovación?, ¿cuál es la misión que tenemos todos? La misión de la innovación es evolucionar pero haciendo las cosas de forma diferente, evidentemente, es innovación el cambio, porque se entiende que el cambio es mejora, pero la mejora tiene que ir soportada por una serie de formas diferentes de mejora. Es decir, se trata de pensar diferente en como mejorar.

"Reinvéntate a ti mismo: el futuro se crea hablando de futuro" (para reinventarse a sí misma la Policía debe crear un ecosistema de innovación apoyado por planificación y estrategia). Uno mismo debe pensar cómo hacer y cómo mejorar las cosas desde el plano personal, pero nosotros como organización también tenemos que pensar en cómo reinventarnos a nosotros mismos para evolucionar. La Comisaría General de Información se ha reinventado a sí misma y ha dado un paso muy importante para mejorar sus capacidades de trabajo en inteligencia. Este tipo de rueda para reinventarse uno mismo tiene que ser continuo y en todas las organizaciones tiene que haber una parte de la organización, por pequeña que sea, que tiene que pensar en el futuro.Y esto es lo que tiene que hacer un Servicio de Innovación. Digamos que a mí me pagan por pensar en el futuro dentro de los márgenes que me dan. La frase "el futuro se crea hablando de futuro" es una evidencia. Cuando se quiere saber cómo será el futuro, lo que hay que hacer es hablar de futuro: ¿qué voy a hacer?, ¿cómo voy a hacer?, ¿estoy donde quiero ir?, ¿qué instrumentos tengo de apoyo, en el plano humano, tecnológico, formativo, organizacional, estructural? Todas estas cosas hay que ir pensándolas y eso es hablar de futuro, porque hay un objetivo ¡llegar! Hay que pensar en las cosas que hay alrededor para llegar al objetivo, esto es pensar en el futuro.

"Para reinventarse a sí misma la Policía debe crear un ecosistema de innovación apoyado por planificación y estrategia" esta es la frase que voy a repetir continuamente porque concienciación, planificación y estrategia son las claves de la presentación. Son las tres palabras clave. Ecosistema de innovación, entendido como colaboración público-privada, como participación internacional.Y la gestión del cambio, la gestión cultural, el cambio cultural, el cambio de mentalidades; con diferencia, es la mayor tarea que tenemos delante cualquier Servicio de Innovación para cualquier tarea que suponga un cambio y también para cualquier persona que quiera hacer un cambio tecnológico dentro de una organización. O sea, la resistencia al cambio es brutal, seguimos todavía en muchas estructuras anclados en la "filosofía del cajón", que en la gestión de calidad es lo primero que se intenta romper. Es decir, "esto es mío" "yo aquí soy el que mando" "este es mi cajón" ¿Cómo nos ven al Servicio de Innovación desde esta perspectiva de la "cultura del cajón"? Como perturbadores. Pero sin embargo nosotros, como Servicio de Innovación somos los más colaborativos, los que pretendemos aportar valor, porque si no aportamos valor no tenemos esencia.

Gráfico 2

GESTIONAR EL CAMBIO Y LA INNOVACIÓN EL CICLO DE LA INNOVACIÓN

El ciclo de la innovación es algo muy sencillo y la forma de funcionamiento es muy parecida a la de la calidad, entonces ¿cuál es la función que tenemos encomendada como gestores de innovación?

1º Identificación del problema o necesidad. Muchas veces los problemas nos vienen identificados como retos internos por la Unión Europea y, muchas veces, estamos más retrasados en la evolución respecto a un sistema técnico concreto y que, también, nos viene identificado como incapacidad para gestionar ciertas cosas; en consecuencia, lo que tenemos que hacer es identificar esos problemas e incapacidades dentro de nuestra organización. Una vez identificados estamos creando una necesidad. Esta es nuestra principal función como Servicio de Innovación.

2º Crear la necesidad. Identificamos un problema pero para que realmente podamos suplir o luchar contra ese problema, hay que crear la necesidad dentro de la organización para que realmente se tome una decisión respecto a cómo suplir ese problema. Esta es una parte difícil porque ya estamos luchando contra el cambio, contra la organización.

3º Buscar soluciones. Es algo relativamente sencillo. Si tengo un problema, una necesidad y miro el mercado, a lo mejor encuentro una solución, ¿que no la encuentro en el mercado? Busco en I+D+i ¿Cuál es el mecanismo por el que voy a hacer el I+D+i? Hay muchos, el otro día se estuvo hablando de Horizonte 2020, el nuevo Horizonte Europa para los próximos años. Se nombró la compra pública innovadora o la compra pública pre-comercial, o compra pública de innovación, las colaboraciones con universidades, empresas, relaciones con *cluster*, licitaciones de cualquier tipo como posibles mecanismos. Pero por desgracia, no tenemos un presupuesto para I+D+i. Los capítulos seis y dos están muy limitados y nosotros, en innovación, tenemos que hacer cábalas para una vez identificados los problemas y necesidades poder suplirlos. Por eso, lo del "conseguidor" que es como denominan algunos a la Subdirección General de Sistemas de Información y Comunicaciones para la Seguridad de la Secretaría de Estado de Seguridad. El "conseguidor" de Secretaría de Estado" es realmente una solución para nosotros como organización para poder incorporar innovaciones, ellos ponen sus condiciones y nosotros nada más tenemos que preocuparnos por cumplir sus condiciones para conseguir la financiación. Nuestra función hasta cierto punto, es buscar esas soluciones y asesorar sobre cómo buscar soluciones, o buscar el mecanismo de hacer I+D+i, para encontrar las soluciones.

4º Definir ideas. Es complejo, porque a la hora de plasmar las ideas en un papel, necesitamos decir exactamente qué es lo que se necesita, cuáles son los requisitos, las especificaciones de lo que hay que hacer y cómo implementarlo. Es complicado porque se trata de buscar la

parte paralela de la tecnología y preguntarse, ¿hasta dónde puedo llegar, cuál es mi marco legislativo, cuáles son los procedimientos a los que afecta, cuáles son los procedimientos que tengo que cambiar cuando lo implemente, qué impacto va a tener no solo en el propio proceso, en el propio cambio, sino en la organización; cómo afecta a otros sistemas, qué impacto va a tener en la sociedad, cuáles son los aspectos éticos que pueden afectar a la tecnología? Todas estas cosas hay que tenerlas en cuenta a la hora de generar la idea. Es fundamental definirlas y podría poner un ejemplo, en Policía, el Área de Telecomunicaciones, ha hecho un análisis técnico de las cámaras corporales que se están utilizando en otras policías, y es un elemento técnico fundamental para una organización policial; en el Reino Unido ha conseguido reducir el 70% de la agresividad contra las policías en las actuaciones policiales, solamente con ese dato vale la pena pensar en invertir en esa tecnología. Y el Área ha hecho un análisis técnico estupendo, pero de qué sirve si no estamos pensando en los aspectos legales que tenemos detrás. Evidentemente, tenemos nuestra ley de utilización de video, y hay que pensar en los aspectos procedimentales; es decir, ¿cuándo se va a utilizar esa cámara, en qué condiciones, cómo tengo que advertir al ciudadano de que voy a utilizar esa cámara, si tiene piloto visual, qué voy a hacer con esa información, cuáles son los plazos de almacenamiento que puedo usar, cómo se van a volcarse esos datos? Todas estas cosas son en parte las que van paralelas a la generación de la idea. Es decir, de nada me sirve tener un análisis técnico estupendo de cámaras de este tipo si no estoy pensando en un aspecto general de uso y aprovechamiento de la información. Pues esa es la función de un Servicio de I+D, tener una visión general del funcionamiento de las cosas, tener una visión general de la tecnología y nosotros, en la gestión de la innovación, lo que tenemos que hacer es proporcionar esa visión general. Nuestra función no es meternos en la parte técnica, sino coordinar gente. Nuestro objetivo principal es ser puentes, unir a gente. Una vez conseguido el presupuesto, hay que realizar el análisis de la innovación ya implementada. Hay que hacer un post análisis de cómo funciona esto, porque después tenemos que estar pensando en el siguiente paso, una vez que lo tenemos implantado y funcionando, tenemos que pensar en cómo evolucionar.

En el fondo, esto es el ciclo de la innovación, tener una necesidad, cubrirla, ver el impacto que tiene y pensar en cómo lo vamos a evolucionar. Es buscar el efecto "guau" que es como se suele denominar en inglés (Gráfico 2): identificar problemas + crear la necesidad + buscar soluciones (si existen soluciones las compramos, si no i+d) + definir ideas + presupuesto+ análisis

de la innovación realizada (¿efecto "guau"?, el efecto de admiración ante esa innovación y la mejora que ha supuesto)

Las innovaciones no tienen por qué ser una cosa disruptiva, ni tienen que generar un efecto sorpresivo, ni ser totalmente rompedor con lo anterior; las innovaciones aunque sean pequeñas también valen porque mejoran y esa actividad es importante tenerla coordinada. Y, sobre todo, dentro de la organización tenemos que evolucionar tecnológicamente procedimientos, pero todos a una.

Gráfico 3

GESTIONAR EL CAMBIO Y LA INNOVACIÓN CONCIENCIACIÓN

Concienciación. Aquí tenemos la gran palabra, ¿por dónde empezar todo un sistema de innovación? Primero conocer tu organización, es súper importante, ¿qué tiene y qué necesita cada uno, cómo tener una visión de las tecnologías transversales? No tiene sentido, por ejemplo, que en Policía tengamos cuatro sistemas diferentes de inteligencia, el suyo (el de la Comisaría General de Información) es el más evolucionado con diferencia. En una visión como organización deberíamos habernos planteado previamente el cómo aprovechar las capacidades que se pueden haber implementado con este sistema de inteligencia para toda la organización; y esa visión de la evolución es la que se puede dar dentro de un Servicio de Innovación. O cómo, por ejemplo, en cuatro unidades diferentes se está haciendo análisis de inteligencia de fuentes abiertas con sistemas diferentes, unos más evolucionados que otros, otros usando un software específico… Ese tipo de cosas no tienen sentido dentro de una misma organización. Otro ejemplo, en Policía se están utilizando tres sistemas de reconocimiento facial diferentes, eviden-

temente con objetivos diferentes, pero ¿por qué? Si centralizásemos todo se podría dar un servicio perfecto a todos los que lo necesitasen, tanto en inteligencia, como estudio de fuentes abiertas, como en reconocimiento facial y, es más, podría estar unido lo que aportaría un valor añadido increíble, podríamos aprovecharnos toda la organización de las mismas cosas incluso gastando menos dinero. Eso implica una labor de liderazgo y el liderazgo de la organización es la innovación hecha de abajo-arriba (del técnico al Jefe de Unidad) y de arriba-abajo (de los grandes planes de la cúpula policial hacia los operativos que van a usar esa tecnología); por eso la de ideas y concienciación de las necesidades es fundamental a todos los niveles.

La concienciación va unida a un cambio cultural, la concienciación y el cambio cultural, para que una organización evolucione y tenga capacidad de mirar adelante, es importante. En el último cuadro del gráfico 3, donde se indica que la resistencia al cambio es brutal dentro de las organizaciones, se ve que casi la mitad de una organización tiene una resistencia absoluta al cambio. Podemos decir, por lo tanto, que al 40% le afecta el cambio y que en ese porcentaje de afectados hay un porcentaje muy pequeño que son los denominados innovadores, los cuales aceptan bien los cambios y otra pequeña parte que son los grandes innovadores que son los que piensan en el futuro. En esa parte, de grandes innovadores, es en la que nos incluimos nosotros como Servicio de Innovación.

En cuanto a gestionar el cambio y la innovación, volvemos a la misma idea: Crear un ecosistema de innovación. Es el único sistema que funciona interna y externamente (ecosistema interno y externo) a la organización, son ecosistemas relacionados unos con otros. El ejemplo lo tenemos en el proyecto Surveiron, es un proyecto que se inició en el año 2013 presentado por una empresa española de Málaga, Aeorum, un proyecto realmente interesante. En su momento nos dimos cuenta de que esta empresa tenía un potencial tecnológico importante (ecosistema interno), pero que no sabían cómo salir de este entramado generado dentro del proyecto. Les ayudamos a hacer toda la parte internacional del proyecto, y ahora mismo es un referente a nivel europeo, tanto por el tipo de proyecto como por la implicación de los usuarios finales que somos nosotros y otras policías europeas. Es un proyecto que ha conseguido el desarrollo de una plataforma de control de drones desde un punto único, que es como una nave espacial, y desde donde se controlan las flotas de drones. Con este sistema se ha llegado a hacer el primer vuelo controlado a distancia, en Finlandia y dirigido desde Málaga, dentro de una prueba piloto con la misión de búsqueda de una persona perdida en los bosques de Laponia, es decir, en el Polo Norte, los drones fueron pilotados desde Málaga, se hizo el seguimiento desde la Secretaría de Estado de Seguridad (consiguió concienciar a la Secretaría de Estado sobre

la necesidad de este producto en un futuro próximo) de nuestro Ministerio y también se hizo el seguimiento de la operación desde Bruselas (ecosistema externo).

En cuanto al ecosistema de innovación y relacionar a la gente, esta actividad está muy bien; pero esa relación entre gente y ecosistemas tiene que hacerse de forma estructurada, no podemos pensar que cada uno podamos ir por nuestra cuenta. Nosotros, como Servicio de Innovación nos aprovechamos de esto, entonces ¿cuál es un objetivo de nuestro Servicio de Innovación? Empezar a abordar estos temas (problemas y necesidades) de forma estructurada, es decir, yo no voy a pensar en implantar cámaras corporales sin la colaboración del área de informática, sin la colaboración de seguridad ciudadana, sin la colaboración del Gabinete, sin la colaboración, por supuesto del Área de Telecomunicaciones, etc. La idea que tenemos en el Servicio de Innovación es identificar estas innovaciones transversales, que afectan a todos y empezar a trabajar en planificar cómo evolucionar en el futuro con esas innovaciones. Por eso, crear equipos de innovación, pensar en el futuro, pensar fuera de la caja, muchas veces no es crear esos equipos para esos objetivos concretos y ya está, es algo más, hay que hacer que trabajen con una metodología estructurada. Conversaciones con expertos en determinadas materias, te hacen pensar "fuera de la caja", te hace pensar en cosas de las que no te habías percatado y hablando con nadie, darte cuenta, de la potencialidad de las ideas generadas dentro de esos equipos de innovación, pero para llegar a tener todos una idea común sobre una tecnología debemos hacerlo de forma estructurada. Eso es lo que falta, un poco de empuje para ese tipo de actividades y la realización de la misma de forma estructurada para conseguir el éxito y el consenso en la innovación.

Respecto a la prospectiva tecnológica, estamos trabajando en el radar tecnológico, este (el de la diapositiva) es el que tiene implantado Interpol, y que, por lo tanto, nos da una idea directa sobre lo que hace este Organismo. Estamos liderando parte de un proyecto (I-LEAD) en el que también participan Guardia Civil y Secretaría de Estado, dentro del paquete 3 del proyecto se pretende crear un radar tecnológico junto con todas las policías europeas, lo estamos liderando nosotros (Servicio de Innovación y Desarrollo); tenemos implantada una metodología, que la hicimos junto con TNO y vamos a usar esa misma metodología que están utilizando en una gran empresa, como es TNO, para identificar cuáles son las tecnologías de futuro y cómo pueden afectarnos.Volviendo al radar de Interpol, vemos por ejemplo que el Internet de las cosas, es una auténtica amenaza ahora mismo. La robótica del futuro va a ir por Internet de las cosas, la identificación de las amenazas de cualquier tipo en el hogar también está identificada, pero nosotros también nos tenemos que aprovechar de esa tecnología.Y también

tenemos que empezar a pensar cómo haremos temas forenses en Internet de las cosas porque, dentro de unos años, va a estar todo absolutamente conectado. Eso es lo que un radar tecnológico nos puede proporcionar como institución, la identificación de la tecnología, las amenazas que supone y cómo podemos usarla.

En definitiva, nuestra misión es conectar gente, se puede decir que el único sistema de innovación consiste en conectar gente y nuestra gran ilusión es ser puente con otras policías europeas (dimensión internacional), con las empresas y con la Comisión en muchos aspectos; no aspiramos a más, de momento, en el Servicio de Innovación.

LA MISIÓN DEL SERVICIO DE INNOVACIÓN

La misión del Servicio de Innovación y Desarrollo es:

- Lanzar retos a corto, medio y largo plazo (buscar prioridades y retos asociados, innovación centrada en prioridades estratégicas). Obligar a la gente a pensar en cómo evolucionar en su trabajo, crear grupos de trabajo donde se piense, hablar de futuro.

- Colaborar. Generar puntos de colaboración para aprovechamiento de capacidades (no es función la participación directa, solo la estructuración de la actividad).

- Identificar necesidades.

- Ayudar en la planificación (planificar la inversión en la mejora de las capacidades y evitar duplicidad de inversiones).

Es decir, y continuando con los ejemplos anteriores ¿cuál sería la hoja de ruta para implantar las cámaras corporales? Aparte de las restricciones económicas, ¿qué tendríamos que tener en cuenta, cuáles serían los pasos que tendríamos que dar, cuándo sería el momento de implantar un sistema de análisis de video inteligencia para analizar la información que se está guardando y el sistema de reconocimiento facial, también, para esas cámaras? Hacer una hoja de ruta y planificar lo que en cinco o seis años queremos conseguir. Ese es el gran objetivo de un Servicio de Innovación.

Gestionar proyectos, puede ser una parte pero sería algo muy farragoso, ya tenemos un servicio que gestiona proyectos, entonces sería simplemente colaborar con ellos. Y, evidentemente, ser el punto único de contacto para la innovación, es decir, todo lo nuevo que se intenta hacer en el Cuerpo

Nacional de Policía, que de alguna forma pase por nosotros, que lo que queremos es colaborar, ayudar, aconsejar, intentar buscar las formas porque tenemos experiencia; por lo tanto, ese es el gran interés que tenemos nosotros relativo a la gestión de la innovación.

Nuestra actuación se centra en el campo interno dentro de la Policía, en el campo nacional y en el campo internacional. Es decir, interactuamos con empresas, universidades, centros tecnológicos, Administraciones Públicas y unidades policiales. De todas recibimos información, a todos intentamos dar información, y de lo que se trata es de ver cómo se maneja, en todas las direcciones, la información. La forma de colaboración y los instrumentos que podemos utilizar ya están inventados, los conozco y lo que intento es aprovecharme de ellos, unos vienen del aspecto internacional, otros son ideas internas. Tenemos la gran suerte en la Policía de tener un capital humano impresionante, personal con grandes ideas; y nuestro trabajo es identificarlos y aprovechar sus conocimientos en beneficio de la corporación.

Igualmente, intentamos tener una red de puntos en diferentes unidades con los que tenemos más contacto, que son más colaborativos. Participamos continuamente con Administraciones Públicas, tenemos contacto con el Ministerio de Defensa, con Guardia Civil y con Secretaría de Estado. También colaboramos con el Centro para el Desarrollo Tecnológico e Industrial (CDTI), que es nuestro punto de contacto, el cual nos une a todos a nivel nacional para temas de innovación.

Es decir, buscamos ser el punto de contacto real de innovación dentro de la Policía, pero sin olvidarnos de que hay otros puntos de contacto dentro del Ministerio. La situación ideal sería seguir una estrategia, nuestra estrategia es muy buena pero nos falta la estrategia tecnológica en apoyo al Plan Estratégico.

En el plano internacional, colaboramos con proyectos europeos, en redes europeas (fundamentalmente Enlets) donde se aglutinan compañeros de otras policías que trabajan en la innovación; y además de Horizonte 2020, somos el punto de contacto para algunos proyectos de Fondos de Interior de la UE, estos Fondos tienen una parte que se dedica a I+D+i, de estos gestionamos la parte de proyectos en convocatorias específicas de los Fondos de Interior que se dedican a I+D. Estamos muy unidos los servicios dentro de la Jefatura Central. Enlets, es una red en la que participamos muy activamente, el punto nacional de contacto está en Secretaría de Estado, pero desde Policía y Guardia Civil se les apoya totalmente. Es una red de la que sacamos mucha información, una red con empresas y policías de otros países y que constituye un punto de unión para ir más adelante en innovación y

tecnologías innovadoras. Es con quien estamos haciendo el radar tecnológico (I-LEAD); que surge del mandato del Consejo de la Unión Europea, al crear Enlets, un radar a nivel europeo del que nos vamos a nutrir todas las fuerzas policiales incluso Europol, Interpol, Frontex, Eu-Lisa y Cepol.

Yo, como Jefe del Servicio de Innovación y Desarrollo, he sido designado como miembro del Comité del Programa que dirige Anabela Gago, asisto como asesor y además asistimos a reuniones internacionales donde se juntan empresas de toda Europa para ponerse de acuerdo en la formación de consorcios para determinadas temáticas planteadas por la Comisión a través de Horizonte 2020, con lo cual, somos muy activos en las relaciones con la Comisión, con los encargados de la revisión de proyectos en la Comisión y, por supuesto, con los responsables del proyecto I-LEAD.

Para terminar, volvería otra vez a las mismas palabras claves de la actividad de innovación en una fuerza policial: planificación, estrategia, identificación de tecnologías transversales, preparación y coordinación de hojas de ruta. Esta actividad sería la ideal, tener una estrategia es la clave, ser capaces de planificar, identificar las tecnologías que capacitan más a toda la Policía y ponerlas en marcha sería nuestra actividad. Sería la situación ideal, evidentemente, convenía un aumento de personal del Servicio de Innovación y Desarrollo, somos tres, y me gustaría que nos pudiéramos multiplicar por tres; y tener capacidad para crear un sistema colaborativo de innovación.

Volviendo otra vez al principio de la presentación, ¿qué es innovación? Crear, crecer, actualizar, desarrollar, generar, imaginar, compartir, resiliencia, convertir, mejorar, adaptar, futuro, idear, pensar. Todo esto y más es la innovación.

I+D+i EN LA FORMACIÓN DE POLICÍA NACIONAL: LA EXCELENCIA FORMATIVA Y LA GESTIÓN DE CALIDAD

JOSÉ GARCÍA MOLINA
Comisario Principal del CNP.
Jefe de la División de Formación y Perfeccionamiento

1. CONSIDERACIONES PREVIAS SOBRE LA FORMACIÓN POR COMPETENCIAS

La Formación Policial, entendida como el conjunto de acciones formativas que capacitan para el desempeño cualificado de la profesión policial, se encuentra incardinada, por tanto, en el marco de la formación académica, en los principios del Sistema Educativo Español (SEE) y el Espacio Europeo de Educación Superior (EEES), que implican la aceptación conceptual de las premisas de la Declaración de Bolonia, que aboga porque la Europa de los conocimientos debe conferir a los ciudadanos las competencias necesarias para afrontar los retos presentes y futuros, en un contexto mundial globalizado.(1)

En este orden de cosas, el marco jurídico español contempla en el RD 1393/2007, de 29 de octubre, por el que se establece la ordenación de las enseñanzas universitarias oficiales, que "los planes de estudios conducentes a la obtención de un título deberán, por tanto, tener en el centro de sus objetivos la adquisición de competencias por parte de los estudiantes".

Por otra parte, como afirma Riesco (2008), la formación profesional en España, siguiendo las tendencias del contexto de la globalización mundial, liga la educación y la organización de los recursos humanos al Sistema Nacional de Cualificaciones y Formación Profesional mediante la LO 5/2002,

de 19 de junio, de las Cualificaciones y de la Formación Profesional, que también incide en la mejora de la calidad educativa basada en la formación por competencias.

Es evidente que tanto desde el punto de vista académico, como profesional o laboral, el enfoque educativo se centra, actualmente, en la formación por competencias concebida como una concepción holística (2), que podemos esquematizar en:

- Los conocimientos, habilidades, valores y actitudes de la persona.
- La capacidad para aplicar esos conocimientos, habilidades y actitudes a una casuística concreta: ejecutar procedimientos técnico-operativos y de gestión policial.
- El aprendizaje para toda la vida. Formación continua o lifelonglearning.

Para cumplir con estas orientaciones, la Dirección General de la Policía ha definido las siguientes líneas estratégicas para el periodo 2017-2021:

1.1.- Normalizar y armonizar los procesos selectivos y la formación, en un marco de calidad y excelencia, que viene desarrollándose a través de las Cartas de servicios de la División de Formación y Perfeccionamiento, de sus Centros formativos y de los Premios y Reconocimientos en Gestión de Calidad.

1.2.- Perfeccionar la metodología docente, promoviendo una mayor formación científica y el uso de las tecnologías puestas al servicio de la formación, que viene cumpliéndose con la realización de Cursos de Formación de Formadores y de Dirección de TFT, para Profesores e Instructores; Cursos de Selección de Personal y Jornadas para Psicólogos entrevistadores y del Curso sobre nuevas metodologías formativas impartido por la Universidad Isabel de Castilla de Burgos.

1.3.- Adaptar los Planes Formativos al Sistema General de Educación y al Espacio Europeo de Educación Superior, que se ha materializado con la puesta en funcionamiento de los Planes Formativos que fundamentaron el reconocimiento de la formación de Grado y Máster, por las Órdenes Ministeriales: Orden EDU/3125/2011, de 11 de noviembre, por la que se establece la equivalencia de la formación conducente al nombramiento de Inspector del Cuerpo Nacional de Policía al nivel académico de Máster Universitario

Oficial, y la Orden ECD/775/2015, de 29 de abril, por la que se establece la equivalencia de la formación conducente al nombramiento de Subinspector del Cuerpo Nacional de Policía al nivel académico universitario oficial de Grado, y se modifica la Orden EDU/3125/2011, de 11 de noviembre, por la que se establece la equivalencia de la formación conducente al nombramiento de Inspector del Cuerpo Nacional de Policía al nivel académico de Máster Universitario Oficial.

1.4.- Desarrollar la normativa de Formación dentro de la LO 9/2015,de 28 de julio, de Régimen de Personal de la Policía Nacional, desde donde se pretende actualizar el actual Reglamento de Procesos Selectivos y Formación de 1995, así como el Reglamento de Régimen Interior de Centros Docentes de 1981.

1.5.- Estudiar las necesidades de infraestructuras y material de la División de Formación y Perfeccionamiento (DFP) para adecuarlo a las necesidades planteadas actualmente, que se ha desarrollado presentando los planes de adaptación tecnológica en los Centros buscando la conectividad total y las necesidades de nuevas infraestructuras en la Escuela Nacional de Policía de Ávila y en el Complejo Policial de Carabanchel.

Estas líneas estratégicas han sido complementadas con las propias de la DFP:

1.6.- La internacionalización de la formación policial en todos los Centros, avanzando en lo ya conseguido:

- En la Escuela Nacional de la Policía, con la recepción de alumnos extranjeros en programas de larga y corta duración, a través de los Programas de la Secretaría de Estado de Seguridad, Acuerdos formativos con Academias Policiales de países europeos y de Asia, realización de cursos de especialización patrocinados por Europol, Frontex e Iberpol.

- En el Centro de Actualización y Especialización con sus programas de especialización para policías extranjeras con los cuerpos policiales con los que mantenemos convenios o acuerdos de colaboración, bien directamente a través de Cepol o con Frontex.

- Y pretendiendo extender esta colaboración al Centro de Altos Estudios Policiales, pudiendo invitar a estudiar a alumnos extran-

jeros en algunos de nuestros cursos de promoción a Comisario o Inspector Jefe, o en los cursos de alta especialización y posgrado.

1.7.- La constitución de Grupos de Trabajo que puedan investigar sobre los nuevos procedimientos técnico-operativos y de gestión policial necesarios, como por ejemplo: Cómo, cuándo, por quién y dónde emplear la defensa retráctil o el arma eléctrica Taser, antes de que se autorice su empleo, o nuevos procedimientos de investigación en el ciberespacio, para unificar los criterios de los investigadores con las dificultades técnico-jurídicas con que nos encontramos.

1.8.- La colaboración y coordinación de acciones entre los Centros Formativos. El apoyo en la consecución de los objetivos marcados y la participación de TODOS en el desempeño de nuestras funciones y actividades que nos permitan evitar el efecto parcelación y el individualismo/ aislamiento en la gestión por los centros formativos.

Pretendemos trabajar en RED, no linealmente, no en estrella. Creando Grupos de Trabajo para todos y cada uno de los proyectos que pongamos en marcha, lo que ya se ha materializado en la presentación del proyecto de nuevo Reglamento de ingreso, promoción y formación, pero viéndonos las caras, debatiendo y compartiendo opiniones y atendiendo a todas las áreas del problema, estudiando y analizando esféricamente el proyecto y en plazos definidos.

Nosotros queremos profundizar en la Ciencia Policial, entendida como "el conjunto de teorías, estudios y opiniones de diferentes autores que tratan sobre la Policía y proponen métodos o procedimientos de actuación verificables y útiles para el desempeño de la función policial" (3) y convertir nuestras investigaciones, diseños y definiciones en doctrina policial para poder enseñarla por igual en todos los Centros y niveles formativos.

Doctrina Policial entendida como"conjunto de principios, valores, creencias e ideas fundamentales que permiten caracterizar la conducta de la institución policial y que se compone de las normas legales de regulación de la misión y funciones policiales (Constitución, Leyes Orgánicas, Leyes, Reales Decretos, Órdenes Ministeriales, Resoluciones, Instrucciones, Circulares y otras normas), que establecen la misión, funciones, organización, estructura, procesos y procedimientos técnico-operativos y de gestión policiales que han de ser cumplidos por el Cuerpo de Policía Nacional y, por tanto, enseñado y entrenado en sus Centros Docentes, considerando que

forman parte de esta doctrina los usos y costumbres de la idiosincrasia policial, lo que nos permite ir constituyendo la "cultura policial" (4).

La colaboración inter-centros supone una distribución de actividades de acuerdo con las dotaciones personales, materiales y de infraestructuras de los mismos. Supone compartir esfuerzos en conseguir que todos nuestros estudiantes puedan conseguir sus objetivos con el apoyo tutorial de los profesores, con independencia de a qué Centro formativo pertenezcan, en la confección de TFG para el Curso de Subinspectores y para el Curso de Complementos Formativos para Subinspectores e Inspectores, así como en los TFM para el curso de Inspectores.

1.9.- La normalización de procesos y procedimientos formativos y de gestión, reflejados en documentos normalizados, para que el conocimiento no permanezca solo en la memoria personal de cada uno de nosotros. El conocimiento se ha de compartir, comunicar, expresar para poder crear modelos, estilos avalados y contrastados que constituyan las mejores prácticas que podamos ofrecer. El compartir entre todos ese saber acumulado mejoraría el conocimiento de todos los miembros de la Corporación Policial. Investigar, escribir, compartir, publicar, ese es el valor añadido de un Cuerpo Policial. La información individual es poder efímero, puede hacer sentir importante a una persona pero no a la Policía Nacional sino se comparte.

Estamos normalizando nuestros procesos y procedimientos para poder certificarnos bajo los estándares de calidad requeridos a la formación del presente siglo y buscamos la excelencia en los procesos de renovación de nuestras credenciales por la valoración periódica de La Agencia Nacional de Evaluación y Certificación Académica-Aneca.

El modelo de gestión de los Centros Formativos se basa en un sistema de gestión de calidad total en busca de la excelencia que ya, desde el año 2000, se inició con el establecimiento de este sistema de gestión en la Dirección de la Escuela Nacional de Policía, donde se ha realizado un gran esfuerzo de implantación del sistema, reconocido ampliamente en premios a las mejores prácticas en el 2000, 2002, 2006 y sellos de excelencia en 2008 y 2010, así como en el Centro de Altos Estudios Policiales donde se han obtenido Certificados del Nivel de Excelencia del modelo EVAM en 2011 y de Autoevaluación del Modelo EFQM de Excelencia en 2018.

1.10.- La revisión escalonada de la selección y formación en todos los procesos. Escalonar los temarios de oposición a las categorías superiores es una necesidad, actualizar los contenidos de los cursos de formación una obligación, que nos permite dotar a los mandos de la Policía de todos los conocimientos, habilidades y herramientas que les facilite el buen gobierno y dirección de los recursos que la administración pone a su disposición.

1.11.- La colaboración en la formación integral de las policías locales, supone colaborar en la formación de base, en la promoción interna y en la actualización y especialización de los miembros de las PPLL que nos lo demanden, por una parte; pero por otra, ofreciéndoles participar en los diferentes cursos, seminarios y jornadas formativas que realizamos tanto centralizada como descentralizadamente.

2.- EL MODELO EDUCATIVO DE LA POLICÍA NACIONAL

Estas líneas estratégicas afianzan que desde el año 1995, con el RD 614, por el que se establece el Reglamento de Procesos Selectivos y de Formación, y hasta la actualidad, la División de Formación y Perfeccionamiento ha ido adaptando gradualmente los planes formativos y mallas curriculares de ingreso y ascenso a las categorías de Policía, Oficial de Policía, Subinspector e Inspector al Sistema Educativo Español (SEE) y el Espacio Europeo de Educación Superior (EEES), en una clara apuesta por la homologación de la formación policial.

La asunción de los principios del Sistema Educativo Español y el Espacio Europeo de Educación Superior, implica la aceptación conceptual de que tanto la selección como la formación para el ingreso, la promoción, la actualización y la especialización se enfoquen al desarrollo de las competencias. Ya el preámbulo de la LO 2/86, de 13 de marzo, de Fuerzas y Cuerpos de Seguridad, mencionaba, con especial énfasis, la exigencia de una actividad de formación y perfeccionamiento permanentes, sobre la bases de una adecuada selección que garantice el equilibrio psicológico de la persona.

Más recientemente, la LO 9/2015, de 28 de julio, de Régimen de Personal de la Policía Nacional, en su artículo 25 hace referencia a los principios rectores del ingreso mediante la "adecuación entre el contenido de los procesos selectivos y las funciones o tareas a desarrollar", en el mismo sentido que el artículo 61, apartado segundo, del estatuto Básico del Empleado Público, lo que determina que la selección debe realizarse en base a las competencias necesarias para el desempeño profesional.

En otro orden, la LO 9/2015, también señala claras referencias a que tanto los procesos selectivos como la formación, ambos por competencias, deben ser entendidos como un proceso unitario, tal y como se desprende de los artículos:

- Artículo 26 referente a las titulaciones académicas necesarias para el ingreso, las cuales, como es preceptivo, se enmarcan en el Sistema Educativo Español y el Espacio Europeo de Educación Superior y donde las convocatorias de ingreso podrán exigir requisitos que guarden relación objetiva con funciones y tareas a desempeñar.

- Artículo 32, donde se establece que la formación de ingreso y la capacitación profesional para la promoción interna tendrán como finalidad la consecución de la capacitación necesaria para desempeñar con profesionalidad y eficacia las funciones policiales.

- Artículo 42, donde se regulan las tres fases de los procesos de promoción por concurso-oposición, siendo una de ellas la "formación profesional específica de carácter selectivo"·

- Artículo 30, referente a que "el régimen de formación se configura como un proceso unitario y progresivo, con vocación de ser reconocido en el ámbito del Sistema Educativo Español, y servido en su parte fundamental por la estructura docente del órgano encargado de la formación de la Policía Nacional".

Asimismo, en el mismo orden de ideas, se articulan los procesos selectivos y formación del Cuerpo Nacional de Policía en el RD 614/1995 de 21 de abril y modificaciones posteriores, referentes a considerar la promoción interna como un proceso unitario de selección y formación por competencias (art. 3) y el carácter selectivo de los cursos de formación y prácticas para los funcionarios de nuevo ingreso (art. 10).

Este esfuerzo de adaptación se ha reflejado en la obtención de:

A) Equivalencia a Licenciado Universitario del Inspector: Orden de 18 de abril de 2000, por la que se establece la equivalencia del nombramiento de Inspector del Cuerpo Nacional de Policía al título de Licenciado universitario de los Diplomados, Arquitectos Técnicos, Ingeniero Técnico o equivalente.

B) Equivalencia a Técnico y a Técnico Superior del Policía y del Oficial de Policía: Orden ECI/1995/2007, de 29 de junio, por la que se esta-

blece la equivalencia de las categorías de Policía y Oficial de Policía, de la Escala Básica del Cuerpo Nacional de Policía, a los títulos de Técnico y de Técnico Superior, respectivamente, correspondientes a la formación profesional del sistema educativo.

C) Equivalencia a Master Universitario Oficial del Inspector: Orden EDU/3125/2011, de 11 de noviembre, por la que se establece la equivalencia de la formación conducente al nombramiento de Inspector del Cuerpo Nacional de Policía al nivel académico de Master Universitario Oficial.

D) Equivalencia a Grado Universitario Oficial del Subinspector: Orden ECD/775/2015, de 29 de abril, por la que se establece la equivalencia de la formación conducente al nombramiento de Subinspector del Cuerpo Nacional de Policía al nivel académico universitario oficial de Grado, y se modifica la Orden EDU/3125/2011, de 11 de noviembre, por la que se establece la equivalencia de la formación conducente al nombramiento de Inspector del Cuerpo Nacional de Policía al nivel académico de Master Universitario Oficial.

3.- I+D+I EN LA FORMACIÓN POLICIAL

En el cumplimiento de los objetivos estratégicos definidos se están desarrollando diferentes grupos de Investigación sobre los mejores procesos y procedimientos formativos, desarrollados por el Gabinete Psicopedagógico y por el Instituto de Estudios de la Policía de la División de Formación y Perfeccionamiento, que nos permiten ir adecuando la formación a las necesidades que se nos planteen superando las técnicas y metodologías de la formación actual e introduciéndonos en el "estudio de casos concretos" similares a la realidad policial, que realizamos en los Centros de Formación; en los periodos de prácticas que realizamos en las diferentes plantillas policiales y en el seguimiento y evaluación de la eficacia formativa en los Puestos de Trabajo asignados a los funcionarios policiales durante sus 5 primeros años de actividad policial.

Proyecto de investigación sobre la eficiencia formativa impartida a las diferentes categorías profesionales y su desarrollo en los Puestos de Trabajo que van desarrollando, profundizando en los datos obtenidos de las encuestas que anualmente nos rellenan los Jefes de Plantillas que reciben alumnos en prácticas y en las encuestas de los ya, profesionales, que nos permitirá evaluar la eficiencia formativa y ajustar los programas académicos a la realidad y necesidad policial.

Hemos iniciado el estudio con los Inspectores y Policías que han ejercido su actividad durante los primeros cinco años de actividad, y pretendemos realizar, también, esta investigación con otras categorías profesionales para poder analizar la progresión en la formación por competencias en los diferentes niveles de la organización policial.

Estas investigaciones nos permiten el Desarrollo de las metodologías formativas en los centros de formación de nuevo ingreso, con puesta en práctica de la adaptación de adultos, ya educados y formados de manera generalista en los valores de la sociedad en la que se vive, a los valores corporativos que supone el ingresar en la "cultura policial" que no solo se rige por las normas constitucionales y usos y costumbres consuetudinarios policiales (5), sino también bajo los principios éticos y morales de actuación, basados en los principios básicos de actuación policial y el propio Código Ético de la Policía Nacional, internacionalmente reconocidos y que tras investigar sobre los diferentes modelos y códigos deontológicos del mundo y especialmente de las policías iberoamericanas, se definió un Código Ético de las Policías Iberoamericanas dentro de la Red Iberpol, que se están implementando en los Centros Formativos de los veinticuatro Cuerpos Policiales que constituyen la mencionada RED.

Este Código establece los principios éticos orientados a marcar la conducta policial en un Estado Democrático: legalidad, responsabilidad, transparencia, objetividad, integridad…, contemplando los objetivos de:

1.- Que los policías tengamos un Código Ético al que ajustar nuestras intervenciones/actuaciones y decisiones.

2.- Que los ciudadanos conozcan este Código y sepan qué pueden esperar y exigir de su Policía.

3.- Fomentar la relación ciudadano-policía.

4.- Consolidar las condiciones en la Organización Policial que fomenten el reconocimiento, la autoestima y la asunción de la responsabilidad por todos y cada uno de nosotros, independientemente del nivel o escala policial.

5.- Afianzar el concepto de "profesionalidad policial", apoyado en la legitimidad y credibilidad de las actuaciones de la Policía.

Este Código Ético, como código deontológico, es el conjunto de principios, valores e ideales que regirán las actuaciones policiales y que servirá de

guía práctica para obtener los mejores instrumentos, acordes con el ordenamiento jurídico, para la toma de decisiones en las intervenciones, bajo el principio de responsabilidad individual, que les llevará a realizar conductas presididas por la ética policial y que se convertirá en un modo de vida, ajustado a la convicción interior de servicio a los demás.

Los Principios inspiradores del Código son: Compromiso con el ordenamiento vigente y las instituciones nacionales: probidad, integridad, objetividad, respeto y transparencia.

El Código Ético de las Policías Iberoamericanas se desarrolla en 12 artículos:

Artículo 1. Ámbito de aplicación.

El presente Código Ético será aplicable a todos los miembros de las fuerzas y de los cuerpos policiales que integran los Estados de la Comunidad Iberoamericana de Naciones – Iberpol (en adelante, las Policías de la red Iberpol), quienes respetarán los principios y las disposiciones establecidos en su articulado.

Artículo 2. Legalidad.

Las Policías de la red Iberpol actuarán de conformidad con lo dispuesto en su Constitución o Norma Fundamental y demás disposiciones legales.

Artículo 3. Protección de los derechos humanos.

1. Las Policías de la red Iberpol promoverán, respetarán, protegerán y asegurarán la dignidad humana, los derechos fundamentales y las libertades públicas de todas las personas.

2. En su proceder tendrán como referencia la Declaración Universal de los Derechos Humanos y el Código de conducta para funcionarios encargados de hacer cumplir la ley, ambos de las Naciones Unidas; la Convención Interamericana sobre Derechos Humanos; el Convenio Europeo de Derechos Humanos; así como los tratados y acuerdos internacionales sobre esta materia ratificados por sus Estados.

Artículo 4. Prohibición de la tortura.

Las Policías de la red Iberpol se abstendrán de infligir, instigar o tolerar cualquier acto de tortura u otros tratos o penas crueles, inhumanos o degra-

dantes, oponiéndose resueltamente a todo comportamiento que implique conductas de esta naturaleza.

Artículo 5. No discriminación e igualdad de trato.

Las Policías de la red Iberpol garantizarán el respeto del principio de igualdad de trato, evitando resueltamente toda discriminación como consecuencia de nacionalidad, sexo, raza, color, origen étnico o social, características genéticas, lengua, religión o creencias, opiniones políticas o de cualquier otro tipo, pertenencia a una minoría nacional, propiedad, nacimiento, discapacidad, edad u orientación sexual.

Artículo 6. Proporcionalidad. Uso legítimo de la fuerza.

1. Las Policías de la red Iberpol garantizarán en su actuación que las medidas adoptadas sean proporcionales al objetivo que se persigue.

2. Solamente harán uso de la fuerza cuando sea estrictamente necesario, guiándose por el principio de proporcionalidad y uso racional y progresivo de los medios.

Artículo 7. Uso de las armas.

Las Policías de la red Iberpol utilizarán las armas únicamente en aquellas situaciones en las que no puedan aplicarse medidas menos gravosas y cuando esté en grave peligro su vida, integridad física o la de otras personas; así como en aquellas circunstancias previstas en sus legislaciones. En todo caso, tendrán en cuenta el principio de proporcionalidad.

Artículo 8. Prohibición del abuso de poder y de la corrupción.

1. Las Policías de la red Iberpol actuarán en todo momento con rectitud, probidad, integridad y honestidad, absteniéndose de llevar a cabo cualquier abuso de poder.

2. Asimismo, impedirán y no cometerán actos de corrupción.

Artículo 9. Objetividad, imparcialidad e independencia.

Las Policías de la red Iberpol, en el ejercicio de sus funciones, deberán ser imparciales e independientes, actuando de manera objetiva.

Artículo 10. Buen ejemplo y cortesía.

Las Policías de la red Iberpol darán buen ejemplo con su conducta y actuación profesional, y observarán siempre un trato correcto, actuando de modo amable, diligente y accesible.

Artículo 11. Confidencialidad y protección de datos.

1. Las Policías de la red Iberpol respetarán el principio de confidencialidad sobre los asuntos de los que tengan conocimiento en el ejercicio de sus funciones, salvo que el cumplimiento de la Ley les exija actuar de otro modo.

2. Protegerán la privacidad e integridad de los datos de carácter personal e impedirán su uso injustificado.

Artículo 12. Responsabilidad profesional.

Las Policías de la red Iberpol serán responsables personal y directamente de sus actos y omisiones, debiendo asumir las consecuencias derivadas de éstos.

Vemos, por tanto, como las diferentes investigaciones sobre procedimientos técnico-operativos y de gestión se van materializando en normas de obligado cumplimiento que van incrementando el acervo de la "cultura policial".

Así, las técnicas formativas adaptadas a las exigencias de Bolonia, suponen que seamos conscientes de que desde hace décadas la Policía ya empleaba la formación por competencias, puesto que nosotros enseñamos a hacer, a actuar con el empleo de procedimientos técnico-operativos y de gestión que se han ido adaptando a la evolución jurídico-social y que desde el primer momento se han practicado para el correcto uso de los procesos, procedimientos y herramientas policiales con la eficiencia requerida a la función policial.

El desarrollo formativo nos permite, desde el primer momento, el experimentar en los centros de formación inicial, promoción profesional y actualización y especialización, las técnicas formativas contrastadas para obtener el éxito adecuado a la formación y entrenamiento de adultos en la organización policial.

Todo ello determina que la Innovación educativa va de la mano de la práctica reiterada de la enseñanza de los procedimientos técnico-operativos que se realizan poniendo el foco, desde el primer momento, en los alumnos.

Con una carga formativa teórica muy ajustada para ofrecer el conocimiento necesario y básico que nos permita desarrollar las funciones y actividades de acuerdo a las normas y procedimientos legalmente establecidos y a los usos y costumbres de la cultura policial, que van más allá de las normas de cortesía.

Nuestro mayor esfuerzo está en la implicación del alumnado en experimentar el cómo se hacen las cosas, en cómo practicar los procedimientos técnico-operativos y de gestión policial perfectamente, teniendo la posibilidad de investigar y proponer nuevas formas de hacer y de actuar, al poder aportar su importante formación y experiencia en otros muchos campos del saber.

Con el estudio y análisis del "caso concreto" comprobamos la eficiencia formativa en los Centros y obtenemos propuestas de mejora que suponen una gran implicación en el proceso de gestión de calidad educativa que nos permite ir en busca de la excelencia en el proceso.

La formación policial se desarrolla bajo un sistema de dirección participativa basada en valores y apoyada en un sistema de gestión de calidad en busca de la excelencia formativa, en la que todo el personal docente y de apoyo, tiene algo que aportar, algo que decir, qué mejorar, estableciéndose un conjunto de caminos mediante los que tenemos que conseguir un servicio de calidad por convencimiento de los partícipes en los procesos(6).

Este estilo de dirección impone un alto grado de convencimiento e interés en que la implantación y su desarrollo están favoreciendo la eficacia, la productividad e imagen de la Formación Policial como servicio de apoyo y valor agregado a la Policía Nacional.

En este nuevo estilo de dirección, la calidad es un elemento fundamental y movilizador al actuar como motivación, integración y satisfacción de los miembros del cuerpo docente, por lo que nos sentimos más parte de la corporación y del sistema, así como más partícipes en la consecución de los objetivos, de tal forma que estamos más motivados en la ejecución de los procesos formativos y técnico-operativos, sintiendo la necesidad de coordinarse e integrarse en los esfuerzos de todos los miembros dedicados a la docencia, y la consecución de mejores niveles de calidad en la prestación del servicio hace que sintamos una mayor satisfacción personal.

Finalmente cerramos el proceso de comprobación de la eficiencia formativa con el análisis de los resultados obtenidos en la preparación policial

con la observación directa de la práctica de los procedimientos técnico-operativos y de gestión enseñados en los puestos de trabajo durante:

A) Su primer año de ejercicio policial, a través de:

- Profesores-Tutores académicos que les visitan anualmente en sus puestos de trabajo, donde realizan las preceptivas prácticas policiales.

- Profesionales-Tutores que en su destino asesoran y observan su quehacer diario.

- Mandos policiales que emiten informes de evaluación del desempeño profesional.

- Encuestas de opinión de los propios alumnos sobre esta fase formativa.

B) Estudios de impacto formativo en los primeros 5 años de desempeño profesional:

- Encuestas de opinión de los policías sobre su experiencia durante este tiempo.

- Encuestas de opinión de los Mandos Policiales sobre la evaluación del desempeño profesional durante este tiempo.

- Observación indirecta con las encuestas de opinión sobre el desarrollo de los servicios policiales en la sociedad y que nos contrasta el CIS. Así nuestros clientes externos, desde hace varios años, nos dan el feedback necesario para ir ajustando la formación, actualización y el entrenamiento de los Policías para ofrecer el mejor y mayor servicio policial percibido por la sociedad.

Del análisis de todos estos datos podemos concluir que los procesos y técnicas formativos de la Policía están plenamente avalados por la sociedad receptora de nuestros servicios y que está acorde con los principios básicos de actuación policial bajo el Código Ético profesional que nos ilumina.

Indudablemente estamos en el camino de la mejora permanente que nos sugieren las opiniones reiteradas, contrastadas y avaladas por profesionales y la sociedad, que nos permite ir adaptando los programas formativos de acuerdo a las exigencias de Aneca sobre nuestra especial forma de

enseñar, reconocida por las Órdenes sobre equivalencias anteriormente mencionadas.

La innovación en las técnicas educativas y formativas de adultos tiene sus complejidades y nosotros empleamos todas las conocidas en nuestro amplio campo formativo de la ciencia policial, ya que nosotros aglutinamos el saber de muchas ramas de la ciencia y de la práctica profesional, aplicándolas en la formación de base, en la especialización (desactivación de explosivos, Investigación tecnológica, desarrollo programas informativos…) y en la promoción vertical.

La formación policial se está realizando simultánea y progresivamente en todas las formas actualmente conocidas. Formación presencial con participación muy activa de los alumnos en el proceso de formación; formación semipresencial combinando las formación "online" con la presencial; formación "online" y pretendemos innovar nuevamente introduciendo la autoformación que nos permitirá llegar a la gran mayoría de los miembros de la Corporación, al poder emplearse medios tecnológicos a disposición de todos los usuarios, tanto en los puestos de trabajo como en sus propios espacios vitales, que les permitirá adquirir conocimientos de refuerzo de sus especialidades policiales o les abrirá la posibilidad de conocer otras especialidades a las que posteriormente puedan acceder con unos amplios conocimientos previos, fundamento suficiente para realizar especialidades formativas que les dará la opción de participar en ese tipo de grupos de trabajo.

BIBLIOGRAFÍA

1.- Riesco González, Manuel. El enfoque por competencias en el EEES y sus implicaciones en la enseñanza y el aprendizaje. Tendencias Pedagógicas nº13- 2008.

2.- Larraín Undurraga, Ana Mª. Formación Universitaria por Competencias. Pontificia Universidad Católica. Chile-2009.

3.- García Molina, José. Ciencia y Doctrina Policial. Ciencia Policial nº 142-DGP-2017.

4.- García Molina, José. Ciencia y Doctrina Policial. Ciencia Policial nº 142-DGP-2017.

5.- García Molina, José. Ciencia y Doctrina Policial. Ciencia Policial nº 142-DGP-2017.

6.- García Molina, José. La función directiva y el estilo de dirección de un directivo de seguridad. Cuadernos de la Guardia Civil nº XXXIII-DGGC-2006.

TURNO DE PREGUNTAS

Pregunta en sala: Atanasio González

Me trae al recuerdo de hace cuatro años donde pude vivir una auditoría que se hizo desde Secretaría de Estado en Ávila a la Comisaría y la Comandancia y a la Escuela Nacional de Policía. Y hay una cosa que me llamó la atención que, efectivamente, seguimos sin un reglamento de centros docentes, cuando esto en el año 2014 era un reglamento provisional del año 80 y tenían nueve borradores; creíamos que iban a ser diez pero ya ha dicho usted que hay un proyecto para decidirlo. Lo que yo quería preguntarle, ya que estamos en innovación, si es posible, sin que sea ciencia ficción, pensar en una Escuela Nacional de Policía sin libros físicos; es decir, ya se hablaba en el año 2014 de la intención de ir suprimiendo los libros pero no sé si la tecnología, si se les pudiera dar una tablet, un pincho, etc. Con todo el mamotreto que se les da a los alumnos cuando llega el mes de septiembre. Finalmente mi felicitación por ese proyecto de autoformación que creo va a ser exitoso.

Responde: José García Molina, Comisario Principal del CNP, Jefe de la División de Formación y Perfeccionamiento. Gracias por su interesante pregunta. Podemos decir con respecto a la realidad del reglamento docente de que seguimos funcionando con el del año 1981; como dice el reglamento, es provisional y les puedo confesar que procedo de una formación previa militar. Los centros académicos militares que llevan muchos años de antigüedad siguen siendo provisionales a día de hoy. Siempre el régimen interior de un centro docente provisional. Si es cierto que estamos trabajando constantemente, pero siempre nos ha ido parando actualizar el reglamento de centros docentes el esperar a la normalización, readaptación del reglamento de procesos selectivos y de formación. En este periodo nos hemos marcado que este año pondremos a disposición del Gobierno, ese reglamento para que con los estudios pertinentes, si lo estima oportuno, lo publiquen. Y ahí estamos trabajando sobre el nuevo reglamento de centros docentes, con la particularidad de que hay matices que ajustaremos cuando salga el reglamento. Si no tenemos un nuevo reglamento de formación, mal podemos ajustar algunas cuestiones. Pero estamos trabajando en paralelo con esos grupos de trabajo e innovación y el objetivo es, este año, reglamento, Real Decreto de selección y formación, año próximo, Orden Ministerial para desarrollar el reglamento de centros docentes.

La segunda pregunta que nos hacía, es muy interesante porque es uno de los objetivos que se tiene en la formación, hemos dicho y he hablado de la conectividad. La conectividad en todos los centros está íntimamente relacionada con la alta tecnología y en la primera fase podemos decir que la Escue-

la Nacional de Policía ya en los dos últimos años se ha dotado de fibra óptica en parte de la escuela. Actualmente está en toda la zona docente, si ustedes no conocen la Escuela no se pueden imaginar que estamos hablando de cincuenta y cinco (55) Ha de terreno, quinientos cincuenta mil (550.000) m^2 y setenta y dos (72) aulas. Pero eso ha sido lo fácil, instalar la fibra óptica, pero la fibra óptica tenemos que llevarla a todas las zonas comunes, deportivas y, además, a toda la residencia donde hay novecientas (900) habitaciones, diez (10) edificios. Estamos en esa segunda fase.

Y, luego, parece que no pero le costó a telefónica llevar fibra óptica, algo muy distinto a lo que ofrece en Madrid; actualmente se está sectorizando la Escuela y se está dotando de trescientas (300) megas por sector y, ahora mismo, tenemos dotado toda la zona de aulario. La fase próxima, ya está pedida, y estamos tirando de los recursos económicos para poder dotar al resto de la Escuela con esas tablets. Sinceramente, la dotación tecnológica, los programas ya están en digital, se pueden descargar los programas, pero el salto digital es darles a todos los alumnos su tablet con el material cargado, o que lo carguen ellos, porque hablamos de tres mil quinientos (3.500) alumnos por curso. Está en esa fase, pero estamos en fase de presupuesto porque, sinceramente, pasar del papel a la tecnología es diez veces más caro, económicamente es diez veces más caro. Sin duda será más eficaz, más cómodo, pero es más caro y tenemos que presupuestarlo dentro de la Dirección General de la Policía para que nos quede la reserva económica adecuada. Una tablet para cada alumno con el material cargado, tiene su coste y, además, necesitamos toda la potencia de Wifi que nos permita ser ágiles, pero estamos en ello.

Pregunta en sala: Soy el Comisario Gámez, Jefe de operaciones de Melilla. Durante un periodo de tiempo yo me dediqué a la formación y quiero hablar de innovación pasada. Mi pregunta creo que es fácil: cuando yo estaba en la Escuela en los años del 92 al 99 ya se hablaba de formación por competencias, el problema que teníamos entonces es que no sabíamos cuál era la competencia; es decir, teníamos conversaciones entre el profesorado para definir cuáles eran las competencias de un Policía, de un oficial, o de un inspector; y ya no digo si encima le poníamos un adjetivo -si el Policía era de investigación, o el inspector estaba en seguridad- con lo cual, empezamos en ese momento a hablar de tareas y poco después, cuando yo no estaba en la escuela, recuerdo que recibíamos una especie de test o encuestas donde teníamos que hablar a los mandos de esta definición de tareas.

Y ahora viene mi pregunta, ese trabajo de investigación que se hizo en su momento, supongo que dio resultado; es decir, entiendo que ahora la aplicación por competencias es derivada de ese trabajo de investigación o de campo que se hizo en su momento y entiendo que debe ser así, porque eso

que acabamos de ver me ha llamado la atención muy positivamente que es el *feedback* de los próximos cinco años, es muy atrevido. Es decir, ese trabajo de campo se plasmó porque la propia norma nuestra no define las competencias muy claramente, son competencias muy generalistas: Policía, oficial y no le pongamos apellido porque entonces nos perdemos.

Responde: José García Molina, Comisario Principal del CNP, Jefe de la División de Formación y Perfeccionamiento. Una reflexión muy interesante, aquí estamos algunos miembros que participamos en formación en los años 80 y voy a recordar un elemento fundamental; en el año 1988 desde la División de Formación y Perfeccionamiento, patrocinábamos desde el Instituto de Estudios de la Policía, un estudio de investigación sobre las funciones, actividades y tareas por todas las categorías profesionales de todas las especialidades, la dirigía el catedrático profesor Vacas de la Universidad Autónoma de Madrid. Ese cúmulo de conocimientos que quedó en la División de Formación y Perfeccionamiento, sirvió para estratificar las funciones, actividades y tareas que cada una de las categorías profesionales debería hacer dentro de nuestra corporación. Con el tiempo, esto se actualiza, posteriormente en este análisis que tú dices de la escuela e indudablemente ha servido para algo, para fundamentar cuál es el curriculum académico y el curriculum del programa formativo que damos, para que el Ministerio de Educación nos reconozca a través de órdenes ministeriales que nuestra formación es equivalente a un grado, es equivalente a un master ¿Por qué? Porque avalamos todos esos perfiles, avalamos todos estos trabajos previos realizados y muchos años de experiencia en la formación.

Os decía que antes de la Ley Orgánica de Fuerzas y Cuerpos de Seguridad del 86, nuestros cuerpos, la Policía, la Guardia Civil, las Policías Locales, hemos formado por competencias porque nos han enseñado a hacer cosas para desarrollar nuestro trabajo, probablemente nos enseñaron todas las competencias que necesitábamos, ahora estamos en enseñar la mayoría de las competencias generalistas que damos en los centros de formación de base; las especialidades son especialidades, hablamos con los especialistas y ellos nos definen cuáles son las competencias concretas sobre las que tenemos que formar. Los especialistas propiamente dichos son los profesores de esos cursos, por lo tanto, estamos en la práctica de las mejores prácticas policiales que tenemos contrastadas y demostradas. Por tanto, no es algo de un día, ni de dos, cuando hemos hecho la ligazón como hemos ido consiguiendo, por ejemplo en los años 80 ya trabajábamos sobre estas cuestiones en el Instituto de Estudio de Policía, Gabinete Psicopedagógico, cada uno en su función, y estábamos en contacto con el Ministerio de Educación para ver cómo podemos hacer que nuestros policías tengan la titulación de técnico

superior. Hablamos de los 80 y lo conseguimos en el año 2007 y lo hacemos continuamente, nos ha costado mucho demostrar y documentar; pero lo hemos conseguido y con idea de perdurar; porque el elemento fundamental en todos los grupos de investigación que conllevan posteriormente innovaciones, es la continuidad. Cuando se pone en marcha un proyecto de trabajo, y se hace con convencimiento de que tiene un objetivo final positivo para la organización, se puede conseguir. Si se marca un plazo y depende de uno, la empresa privada depende de esto y de su beneficio, posiblemente corra; cuando depende de otros y las decisiones están fuera del campo competencial, probablemente sea más lento pero demostramos que lo hemos conseguido.

Pregunta en sala: soy J. Javier Da Silva, Inspector Adjunto. Quería saber cómo está el centro universitario de la Policía Nacional y qué se supone que tiene que hacerse, tal como contemplaba la Ley de personal.

Responde: José García Molina, Comisario Principal del CNP, Jefe de la División de Formación y Perfeccionamiento. Pregunta muy interesante y no comprometida porque lo tenemos resuelto; es cierto que la L.O. de Régimen de Personal contempla la creación de un centro universitario para la Policía. El proyecto está hecho, acabado, con todos los vistos y parabienes, de Policía, Secretaría Técnica del Ministerio, Ministerio de Educación, etc. Nos hemos detenido en el presupuesto. Nosotros tenemos una formación que venimos dando por equivalencia con la del Ministerio que tenemos el mismo grado universitario y master universitario a efectos académicos, el que tenga grado puede hacer un master y el que tenga master puede hacer un doctorado en cualquier universidad del círculo de Bolonia. Sin embargo, al transformarnos en centro universitario y depender de una universidad tenemos que pagar unas cuotas. Nosotros damos una formación apoyada por el Estado que es gratuita, cuando se entra en la Universidad, entes autónomos, piden una matrícula. Eso supone más de tres millones de euros al año para la Policía. Problema, con tres millones hacemos una Comisaría nueva cada año; y tenemos más, entonces estamos en fase de dotación económica para desarrollar el proyecto. Nosotros estamos apostando por algo que es la Universidad de la Policía que, de acuerdo a la Ley Universitaria, requiere una serie de condiciones que son: tener unas instalaciones -que tenemos-, tener unos profesores doctorados, en la Policía contamos con más de cien doctorados especialistas en todas las ramas del saber, contamos con un claustro de profesores suficientes para la formación policial. Contamos con los alumnos, el empleo público que ofertamos cada año, no competimos con nadie, ni le quitamos clientela a nadie, y toda la formación nos sale con el mismo presupuesto que nos sale actualmente. Por lo tanto, hemos presentado un proyecto para crear una Universidad de la Policía.

Está presentada y todos los condicionantes para ser una Universidad Pública de Seguridad o de la Policía están sobre la mesa y presentados a las instancias de la Dirección General de la Policía y Ministerio de Interior.

La diferencia es que cuando acabamos los estudios de Inspector, o de Policía, recibimos un diploma que dice: El Director General de la Policía, Secretario de Estado de Seguridad; es decir, nombra funcionarios, pero académicamente no; así cuando al Inspector se le da un certificado que dice "el Ministerio de Educación de acuerdo a la Orden Ministerial, le concede la homologación, la equivalencia a un título de master universitario oficial", no especifica de qué es el master, si es Policía científica, Policía integral, Seguridad integral, y ese documento tiene la misma validez que el master oficial que se haya realizado de Dirección estratégica, donde al lado dice: El Rector Magnífico de la Universidad X, en nombre de Su Majestad el Rey, le concede el master en… Lo firman tres personas, te cobran ciento cincuenta (150) euros por el título y tiene la misma validez que el que entregamos al Inspector. Si esto se transforma, primero nos autorizan a transformar en Universidad, damos el mismo título que cualquiera. El Rector de la Universidad de la Policía, no, Su Majestad el Rey titula a una determinada persona.Y la última condición que se me había olvidado mencionar, tenemos que tener ocho títulos universitarios que impartir, Grado de Subinspectores, Master de Inspector promoción libre, Master de promoción interna, Master de dirección estratégica, Master en ciberseguridad, y los tres cursos que tenemos como alta especialización con otras universidades de alta gestión, que es dos meses más de clase, treinta créditos más; es decir, nos queda por hacer tres Master nuevos, estamos en ello para tener ocho titulaciones que es lo que se exige para crear universidad y luego que el Consejo de Universidades, el factótum del Consejo de Universidades, dé el visto bueno, autorice y se convenza de que no competimos con nadie, nuestros clientes son nuestros, son internos.

Pregunta en sala: soy J. Manuel Rava y estoy en la División de Policía Municipal de Madrid. Mi pregunta es: ¿Es solo para la Policía Nacional o es transversal y horizontal y podía presentarse Policía Local a este tipo de formación universitaria?

Responde: José García Molina, Comisario Principal del CNP, Jefe de la División de Formación y Perfeccionamiento. En principio es crear la Universidad de la Seguridad, dentro de la Policía. Repito, esto es la idea original, todo es factible de adaptarse. Uno de los objetivos prioritarios de la división es compartir formación con las Policías Locales, si lo conseguimos, una vez que lo tengamos, por convenio o por acuerdo con las Policías Locales autorizados convenientemente no hay ningún problema

en abrirlo, formación de Comisario, de Inspector Jefe, de formación de Inspector, máximo que ahora ustedes tienen prácticamente los mismos nombres que nosotros, y que se pueda llevar a efecto es cuestión de convenios específicos.

MESA REDONDA: FOMENTAR UNA SOCIEDAD MÁS SEGURA

Modera: Enrique Belda Esplugues.
Participan: José García Molina; Carlos Antonio Vázquez Ara; Carlos Gajero Grande; José Francisco López Sánchez

Interviene: José Francisco López Sánchez

De la ponencia de D. José García Molina, me ha alegrado el poder comparar dos o tres puntos clave que, más o menos, se repiten en lo que yo he hablado esta mañana.

El primero de ellos es el tema de la colaboración, la internacionalización, el buscar siempre los puntos comunes; y el otro asunto es el tema de los ciclos tanto de la innovación, como de la calidad y que son muy paralelos, bastante similares en el fondo. Y, el tema de la formación por competencias está ligado, muchas veces, con lo que yo he nombrado capacitaciones. Viene a ser lo mismo, buscar capacidades unidas a competencias y tecnología. El Sr. García Molina, no ha mencionado algo que para mí fue impresionante, que fue la primera administración pública europea que consiguió EFQM+400, es el mejor premio que la Policía ha recibido en gestión de calidad, y hay que decirlo porque fue un orgullo. Y hay otro punto que destacar y es el tema de la creación de grupos de trabajo en investigación. Algo parecido a lo que yo he planteado, creación de grupos de trabajo multidisciplinares para muchas cosas y unido todo esto a la generación de sinergias, por qué no unir esos grupos de trabajo con la creación de grupos de trabajo específicos con temas de formación. También, hay que tener en cuenta que Cepol a nivel europeo organiza también un congreso anual sobre tecnologías y formación. Todas estas cosas, de alguna manera, se pueden unir dentro de la corporación porque crea valor.

Quería destacar algunos temas de los que se ha hablado esta mañana que son fundamentales desde el punto de vista de la innovación, y uno de ellas es el tema de la interoperabilidad y la importancia que puede tener si lo unimos a la internacionalización; y me gustaría comentar un ejemplo del que se habló, el tema de las telecomunicaciones, desde Policía, junto con Guardia Civil y Secretaría de Estado, se está trabajando en un proyecto desde el año 2014 donde se van a generar futuros sistemas que van a sustituir a Sirdee, el problema es que cuando se ponga en funcionamiento la mayoría estaremos jubilados. Así que quiero destacar una cosa muy sencilla, que estamos planteando desde el año 2014 un sistema de comunicaciones seguras, de ancho de banda interoperable a nivel europeo, con lo que se puede estar trabajando en Holanda y comunicado como si estuviera en España y mandar la información a mi centro de control.

Este sistema que va a sustituir Sirdee, nosotros pensamos que le aporta una capacidad superior, vamos a tener capacidad de transmisión de video, todo tipo de información de datos, con lo cual es como la base de futuros campos de evolución tecnológica en el sentido de las tecnologías de movilidad que es el objetivo. Es decir, se va a poder tener la oficina virtual en cualquier lugar, todo el mundo va a poder transmitir. El Alertcops, ahora mismo, va por una red comercial, pero nosotros vamos a poder transmitir el mismo número de datos, incluso más todavía, por una red privada policial. Este tipo de evoluciones, quiero destacar que son lentas; está muy bien hablar de innovación pero tiene que basarse en planificación porque es lenta.

Anabel Gago habló ayer de la preocupación que tiene la Comisión porque no son capaces de realizar acciones innovadoras rápidas; es decir, ante un evento concreto como puede ser un cambio en los atentados terroristas en cualquier sitio, no tienen capacidad para innovar o aplicar innovaciones de una forma rápida y aportar una solución inmediata en un plazo menor de un año. Es un tema que preocupa bastante a la Comisión. Ahora mismo están las *Fast track for innovation* pero se emplean como mínimo dos años para la implementación de cualquier innovación y con un resultado final que suele ser bastante rápido y siempre estamos hablando de tecnologías con un desarrollo o madurez bastante elevados. En ese sentido me gustaría preguntar ¿qué tipo de sinergias o entornos colaborativos tienen en la división para relacionarse con otras Policías europeas? Y ¿cuál es la vinculación con Cepol en relación con las tecnologías que están evolucionando continuamente, pensando no solo en realidad virtual sino también en la aplicación de sistemas de formación con inteligencia artificial, etc? En ese sentido ¿cuál es la interacción que tiene la División con otras policías europeas, con Cepol en aspectos tecnológicos de formación?

Responde: José García Molina, Comisario Principal del CNP, Jefe de la División de Formación y Perfeccionamiento. Gracias por la pregunta, es muy interesante. En el momento actual, la división de formación, mantiene relaciones con policías europeas en general y con Cepol en particular, están más orientadas a la actividad académica que a la tecnológica. Hoy por hoy, no tenemos ningún grupo tecnológico abierto en el que podamos compartir experiencias, o incluso estudiar, o investigar la necesidad de complementar con nuevas tecnologías de comunicación, por ejemplo, o de apertura a través de sistemas informáticos. Yo creo que la agencia Cepol está todavía en la fase de asentarse para hacer cosas. Por otra parte, tenemos convenios bilaterales con academias de policías y todas orientadas al aspecto formativo, especialmente formación de base. La formación de base la tenemos en convenios privados bilaterales con estas policías: Francia, Alemania, Italia, Rumanía..., incluso con la de China, pero no la especialización porque la hacemos a través de Cepol en Europa y estamos limitados a lo que ellos plantean. Quizá podríamos nosotros plantear la iniciativa de crear un grupo de investigación en esta cuestión tecnológica, estamos abiertos a hacerlo, sabéis que el punto de contacto está en el Centro de Actualización y Especialización de la Policía, dependiente de la Secretaría de Estado de Seguridad. Es decir, posiblemente sería un proyecto para hacer conjuntamente con Guardia Civil.

Interviene: Mario Hernández Lores

Ahora mismo, hay compañeros que están en la periferia en diferentes ciudades: Badajoz, Melilla…, y una serie de unidades que tienen contactos con universidades tienen compañeros con inquietudes, ellos mismos tienen inquietudes y algunos compañeros son responsables de unidades del Cuerpo Nacional de Policía de alta tecnología, este es un primer aspecto que quería comentar, y el siguiente es que hace unos años, se me ocurrió presentar en una institución en la que estaba entonces, proyectos al séptimo programa marco, proyectos preciosos pero complicadísimos, muy grandes y, concretamente, lo que más se defendía -con bastante ignorancia- era el de las estructuras críticas, uno de los grandes objetivos del séptimo programa marco. Esta es la segunda premisa y la tercera que quiero situar, investigación dentro del Cuerpo Nacional de Policía, de esas iniciativas que tenemos todos. Una de las inquietudes que tiene la Fundación Policía Española, no sé si influido por mi personalidad, es la de la investigación. Tenemos aspectos como este curso, tenemos aspectos a nivel individual, las becas están convocadas y hace un rato estaba hablando con el Jefe de la División para pagar aquellos proyectos e iniciativas casi a nivel individual. También, tenemos la propia Fundación, los premios de investigación, y que algunos de los que los han ganado presentarán sus ponencias en este curso. Pero ahí, ya estamos a esos niveles, es un salto económico importante pero también un salto importante de implicación y de profundidad de los estudios. Por ejemplo, esta mañana hablaba Anabela de los Programas europeos de innovación, ahí ya implicamos a un

centro universitario por regla general, a un compañero que tiene la iniciativa y a una universidad.

Y, a esto es a lo que voy, dentro de lo que es ahora el Horizonte 2020 y lo que en un futuro será Horizonte Europa tiene que haber la misma salida para estimular a los compañeros, para que se alíen con esas universidades, para que se creen esos grupos y acceder a esas cuestiones. Por lo tanto ¿Qué iniciativas concretas se deberían estimular para conseguir esos objetivos?

Responde: José Francisco López Sánchez, Inspector Jefe del CNP, Jefe del Servicio de Innovación y Desarrollo de la Jefatura Central de Logística e Innovación. La pregunta tiene enjundia porque nuestra participación dentro de Horizonte 2020 o del futuro Horizonte Europa es relativamente limitada, digamos que la mayor parte de las temáticas de I+D+i nos vienen impuestas y además hay que tener en cuenta otras cuestiones, positivas y negativas. En el plano negativo, en cuanto a los niveles de desarrollo de I+D+i de las tecnologías, hay una escala de desarrollo tecnológico desde la ciencia base que es el nivel TRL1, hasta la llegada al mercado que es un TRL9, los niveles intermedios de I+D+i son los que están posicionados en Horizonte 2020, entre el TRL4, TRL5 a TRL7. En esos niveles de desarrollo tecnológico se llega a la realización de pilotos; es decir, nunca es una tecnología final y menos una tecnología muy próxima al mercado. Para nosotros es un freno porque es muy difícil implicar alguna unidad policial o decir a un jefe de una unidad policial que, a pesar de la ayuda de personal que ha conseguido para colaborar en el proyecto, no se ha conseguido nada porque lo que no se puede es conseguir un producto finalizado, se puede conseguir que ese producto en forma de piloto lo dejes instalado en tu unidad pero es un producto que nadie te lo va a poder actualizar porque no está en el mercado. Entonces, en un año se queda medianamente desfasado.

Para animar a las unidades hay una serie de valores en el plano de aprendizaje de conocimientos sobre la tecnología, sobre lo que viene en el futuro que va a ser muy interesante para las personas que participan y por otra parte, una cuestión importante: hay que vender, y nosotros a través de estos proyectos tenemos una gran oportunidad de vender lo que hacemos, la actividad de I+D+i y la actividad tecnológica que realizamos. Si se hace un balance entre lo que es más interesante para una unidad -al final es el jefe el que decide si entra dentro de un proyecto o no entra- y te pones en su lugar, es un problema engorroso ¿Por qué? si va a detraer de su actividad diaria gente, ¿qué beneficio voy a tener a cambio? Además, va a ser un tema a largo plazo y ¿cuándo voy a conseguir el beneficio? Nosotros cuando planteamos el tema de una propuesta de proyecto en el que conocemos a las universidades que van a participar, a las empresas europeas, centros tecnológicos, el resto de usuarios finales que van a participar en el proyecto a nivel

europeo, es decir, ¿qué otras policías participan, quién va a liderar, quién va a hacer cada parte del proyecto? Llega un punto en que, a pesar de toda esa información que está proporcionando, siempre preguntan lo mismo ¿y esto cuando empieza? Esto es competitivo, ya de entrada el hecho de estar trabajando en la preparación de esta propuesta de proyecto no garantiza que lo vayan a conceder; es decir, es tan competitivo como que normalmente vienen a financiar el 10% de los proyectos que se presentan. Hay años que no conseguimos ninguno y otros que cuatro o cinco; la Policía Municipal de Madrid, por ejemplo, ha tenido el año pasado, la mala suerte de que en los ocho o nueve que participaban, entraron solo en seis. Eso supone una carga de trabajo horrible y para un jefe tomar esas decisiones, es complicado, porque de entrada, hay que poner gente a trabajar, sin ninguna garantía de que vaya a salir; si luego sale y hay que perder a dos personas durante dos años, tres meses al año, se sigue perdiendo capacidad de trabajo y si encima hay poco beneficio es más difícil. El vender la imagen de Policía Nacional fuera de España, muchas veces es menos importante cuando esta tarea la tiene que realizar personal operativo. Esto hace difícil vender Horizonte 2020 a las Unidades operativas.

Interviene: Mario Hernández Lores

Entonces, habría que derivarlo a las relaciones con las universidades y otra vez tendríamos que pasarlo al Jefe de la división, esa es una cuestión; pero el otro punto que quería dejar claro es que la gente fuese consciente del gran trabajo que estás haciendo y la dificultad que tienes, porque me consta y quería dejarlo de manifiesto. Por otra parte, quizás serían las relaciones con las universidades, en este aspecto.

Interviene: José García Molina

Desde la división de la Unión Europea nos pasa igual, y participamos en un montón de proyectos. Bueno, presentamos nuestra propuesta de participación en proyectos, tanto en Iberoamérica como en Europa, la realidad es que dedicamos mucho tiempo y personal muy cualificado a presentar todos estos proyectos que tenemos que presentar en perfecto inglés y que además te lo evalúan administraciones que no te conocen, por ejemplo, presentamos proyectos de formación policial para Uruguay, Perú..., a través del Banco Interamericano de Desarrollo de EEUU (BID); participamos con la Universidad de: Salamanca, Uruguay, Argentina o Perú. Conlleva tres meses de trabajo duro, de presentar grandes proyectos escritos y estás a expensas de que incluso no consigas ninguno. En Europa, la formación de la Policía Moldava, la formación de la Policía Serbia,en problemas de la Unión Europea, ha participando con otras policías, porque si vamos solos, es difícil, pero si participas con otras policías de: Alemania, Italia, tampoco te los dan. Es decir, estos proyectos presentan mucha gente y, además, tienen más experiencia tecnológica. Yo vengo de la perspectiva de formación. Hay una serie de

empresas civiles especializadas en preparar proyectos de la Unión Europea, del Banco Mundial y de la BID, que son expertos en presentar proyectos, y lo que hay que hacer es lo que nosotros hacemos, investigar qué pasa dentro de cinco años de haber hecho el proyecto ¿Ha sido eficaz, es útil, sirve para algo? Eso es lo que tenemos que analizar, porque nos estamos gastando millonadas en la Unión Europea, Banco Iberoamericano de desarrollo, OEA en EEUU y el Banco Mundial, en cosas que sinceramente, al poco de haberse terminado, no sabemos qué rentabilidad tienen, y hablo desde la perspectiva de formación. Hemos estado en El Salvador con la Unión Europea, años, y ahora recibo a los grandes jefes de El Salvador y después de treinta años me pregunto cómo hemos avanzado tan poco. Sinceramente, y hablo del campo de la formación. Cada dos, tres meses yo estoy en Iberoamérica, reunido con todos los jefes de la formación policial, con programas de la Unión Europea formando, dando programas, proporcionándoles manuales, escribiendo, haciéndoles las cosas, y no hemos avanzado nada. He estado cinco años en un programa de trabajo de la OEA con las agencias federales americanas y cuando nos reuníamos cada seis meses, les decíamos a los americanos que quitaran la subvención; llevamos diez años con esto y no hemos pasado del art. 2. La rentabilidad posterior de analizar un proyecto es poca y en nuestro caso el prestigio policial que tiene la Policía Española, sinceramente y con respecto al resto de instituciones, es muy elevado en muchos campos y en el de formación también, pero eso no quita que no entremos. Ejemplo, ¿alguien concibe que se presente un proyecto de formación para la Policía de Uruguay, con la Universidad Uruguaya, con la Universidad de Salamanca, con el potencial tecnológico de la Policía Española y gane el concurso la Policía londinense? Dará el curso en inglés o en perfecto español, fijaos en este condicionante. Quizá nos faltan los lobbies y España no los tiene en el mundo internacional. Tenemos conocimiento, saber, nos llaman como expertos, como conferenciantes, pero nos falta el lobbie.

Interviene y pregunta: José Francisco López Sánchez

A mí me alegra saber que en ese mundo existen empresas que viven de redactar propuestas. Es I+D+i donde existen auténticos especialistas, a nivel europeo, en gestión y redacción de propuestas, empresas que por veinticuatro mil (24m) euros redactan una propuesta con ciertas garantías de funcionamiento.

También, quería comentar sobre la pregunta anterior, que nosotros sí podemos plantear temáticas para desarrollar I+D+i; previo a la salida de la convocatoria de la Unión Europea. En el comité de programa, podemos hacer presentaciones, es decir, si tenemos alguna inquietud tecnológica, con una perspectiva de futuro. Es lo que comentaba esta mañana, que nos falta estrategia, si lo tuviéramos, tendríamos idea de futuro que es lo que queremos dentro de cinco años. Si tuviéramos una idea de ese tipo, podríamos plantear algo y Horizonte 2020, entonces, sí es el marco adecuado; por eso,

esta mañana, yo apenas hablé de Horizonte 2020, dije que nuestro servicio lo que debe ofertar es la capacidad de poner en marcha ciertos instrumentos que favorezcan la I+D+i. No solamente existe Horizonte 2020, ayer se estuvo hablando de compra pública pre comercial, de compra pública de innovación, de compra pública innovadora de diferentes fases. Esos instrumentos están por explorar hasta cierto punto, el planteamiento de ideas nuevas se puede hacer de muy diferentes maneras dentro del Ministerio del Interior de forma conjunta; y la innovación nos va a salir gratis, son mecanismos que nos permiten innovar y aplicar con instrumentos nuevos y tecnología nueva totalmente adaptada a nosotros.

De igual manera hay que tener en cuenta que el Horizonte 2020, con el paso de los años, se va ajustando a la estrategia europea de interior en los tres grandes pilares: ciberdelincuencia, crimen organizado y terrorismo. La temática que hace I+D+i cada año, va cambiando, va modificándose y, por eso, es importante; además, yo quería enlazarlo con una pregunta que he lanzado esta mañana, uno de los ejemplos que existe en tecnologías transversales dentro de la Policía que son adaptables a todo el mundo, uno de ellos es el tema de inteligencia y la pregunta que quería hacerle a Carlos es ¿qué le parecería que "i3" fuera implementado para toda la Policía?Hemos hablado de un Gati que está anticuado, hemos hablado de que la Comisaría General de Extranjería y Fronteras tiene un sistema de inteligencia independiente y tenemos por delante un "i3" que es un sistema súper avanzado y que al fin y al cabo, como decía Belda, la tecnología no tiene límites y muchas veces es una cuestión de licencias, de trabajar con capas de forma modulada para que cada una, aprovechando la misma tecnología, se hagan cosas totalmente diferentes. La pregunta es ¿Qué le parecería a Carlos Gajero el extender "i3" al resto de la Policía?

*Responde: Carlos Gajero Grande***.** Voy a contestar como Carlos Gajero y como Comisaría de información, pero antes quería hacer una puntualización para hilvanar el tema de formación y de fondos, y luego te contesto.

En primero lugar, respecto a la formación, esta mañana, el subdirector E. Belda decía que sin despliegue no hay nada, hablábamos de tecnología; yo que estoy metido en un proyecto que es innovador, aplica mucha tecnología y conlleva un despliegue por todo el territorio, tengo aquí compañeros que están sufriendo las consecuencias del despliegue, hay otros que están anhelantes de que llegue, efectivamente, sin despliegue no hay nada, pero me atrevería a decir que sin formación tampoco. Todo el apoyo que tenemos de la unidad de formación me gustaría ponerlo en valor, porque es un apoyo muy importante sin el cual no conseguiríamos nuestro objetivo, porque el objetivo es que I3 lo utilice el usuario y cualquier tipo de tecnologías de estas; por la complejidad que lleva, requieren un esfuerzo importante por

parte de la corporación de formación y la Policía lo está haciendo.

En cuanto a los fondos, I3 se ha beneficiado de financiación europea pero el esfuerzo que se hace a cambio de lo que se consigue muchas veces es desproporcionado. Y tienes el día a día, hay tantas bocas de agua que tapar, que detraer dos o tres personas para dedicarlo a algo que no sabes si va a tener resultado, tiene un coste muy importante para la corporación. En mi opinión, en los fondos, tal como los enfoca la Comisión, creo que se ha perdido el contacto con la realidad. Ellos llegan, marcan unas estrategias, que en teoría vienen marcadas por las reuniones de la Comisión, pero creo que tendría que ser algo mucho más ágil, mucho más dinámico y mucho más abierto a las verdaderas necesidades que tiene la Policía de seguridad, y que está marcado dentro de la estrategia de seguridad nacional que, a su vez, está marcado dentro de la estrategia de seguridad europea. O sea, no puedo diferir mucho de lo que pide un compañero de lucha antiterrorista francés, o italiano, de lo que le pueda pedir yo, estoy convencido. Y, sin embargo, la financiación de la Unión Europea, por ejemplo, este año, financia guantes de látex, y sin embargo, tenemos un problema de migración y nos están entrando *foreign fighters* por las fronteras. Tenía que ser algo más dinámico.

Y, para contestar tu pregunta, puedo decirte que coincido plenamente, la Comisaría General de Información y yo. Decía que es un sistema de inteligencia que ha nacido dentro del ámbito de la Comisaría General de Información para la lucha antiterrorista como está en la agencia de protección de datos y solo, en el ámbito de la especialidad, los compañeros que pertenecen a este ámbito, son los que lo pueden utilizarla.

También os decía que Itress es una plataforma Big Data, lo que significa "montón de datos". Big Data en una corporación como la nuestra solo debe haber una. Es escalar el problema que me encontré en la Comisaría de Información, más de ciento sesenta bases de datos dispersas cada una por su lado; bases de datos que cada uno tenía para resolver su problema, cuando estamos poniendo en valor los datos que tenemos. Nos está costando mucho conectar bases de datos de la Policía, tenemos más facilidad para conectar bases de datos de Secretaría de Estado que de la Policía. Entonces, en mi opinión y en la de la Comisaría General de Información, esto es lo que debería ser sin ningún género de duda.

Recordaréis que os decía que hay un cerebro y alrededor un universo de herramientas que son "empujadores de datos"; cualquiera de las especialidades de la Policía sería un "empujador" más de datos y consumiría sus datos conforme a los procesos, las necesidades, su forma de trabajar, sin ningún problema. Es más, la tecnología permite darle el nivel de seguridad, o de tratamiento o de secreto, a cada dato, a cada entidad. Esto es, no se cruzaría una información clasificada de crimen organizado o de terrorismo, no sal-

dría a la vista para un investigador de extranjería y fronteras, por ejemplo, o de seguridad ciudadana, o de Policía Científica; ahora bien, todos tendríamos el valor de que estaríamos volcando todos nuestros datos en el mismo repositorio de datos. Eso significa que todos los datos se enriquecerían con el contraste de todos los demás. O sea, desde mi punto de vista, debería ser así. Sin embargo, esto no es tan sencillo y requeriría un trabajo, el primero de ellos es que el sistema se tiene que estabilizar en la especialidad, deberíamos crecer, escalar, el sistema; porque ahora está diseñado para que lo utilicen cerca de tres mil personas (3.000) y pasaríamos a utilizarlo sesenta mil (60.000). Eso supone inversión y lo primero de todo es la especialidad, debería hacer lo que hicimos nosotros en información y es ordenar los procesos y los procedimientos. Hay que saber de dónde vienen los datos, quién me pide algo, cómo lo hago y quién es mi cliente; organizar todos y cada uno de los procedimientos que se llevan a cabo dentro de la especialidad. De todos los grupos, de todas las brigadas, de todas las unidades, antes de nada porque dependiendo de lo que se hace, así se necesita consumir, así se necesita que I3 aporte los datos.¿Sería recomendable? Desde luego que sí, es lo que debería ser.

Interviene: José Francisco López Sánchez

Yo de todas formas, discrepo de ti en una cosa, Horizonte 2020 ha cambiado mucho con respecto a hace algunos años, por algo muy sencillo, ahora uno de los grandes requisitos que ponen para participar en los proyectos es la participación de usuarios finales dentro del proyecto, como condición de legibilidad, es decir, si no tienes cinco usuarios finales dentro del proyecto, sencillamente el proyecto ya está eliminado de antemano. De entrada es un primer paso muy importante porque ahora, de repente, desde hace dos años nos hemos convertido en "caramelito" de las empresas y ahora recibimos propuestas; el año pasado recibimos cincuenta y cuatro, de proyectos. Es algo inmanejable, porque cada uno genera mucho trabajo. Ahora mismo, las fuerzas policiales estamos muy valoradas dentro de la participación de proyectos porque la Unión Europea se ha dado cuenta de que sin nuestra opinión los proyectos no llegan a ningún sitio positivo y menos al mercado. En ese sentido, se va avanzando en la Unión Europea, aunque sea lento.

Tercer panel: horizonte 2020

H2020, SOCIEDADES SEGURAS

MAITE BOYERO EGIDO
Representante de los intereses de España en el Comité de Gestión del programa Sociedades Seguras en la Unión Europea

El CDTI tiene una doble labor, por un lado, como entidad pública empresarial, realiza una labor de banco, que financia la I+D+i a empresas españolas, y otra que es la de defender los intereses españoles en determinadas instituciones europeas o internacionales. Ahí, es donde se ubica mi departamento; estoy en el ámbito de Horizonte2020 que es el programa marco de I+D+i de la Unión Europea, un programa que tiene más de cuarenta años de historia, un programa que financia actividades de desarrollo e innovación, en consorcio común entre varias entidades de países europeos, en distintos sectores o en distintas líneas de actuación.

Desde el año 2007, se financian actividades en el ámbito de la seguridad. Las Fuerzas de Seguridad son un elemento clave en este programa. Actualmente el programa que se llama Sociedades Seguras, ese es su objetivo; un programa que cubre soluciones para que podamos mejorar nuestro día a día.

Este programa, en el que participan los veintiocho Estados miembros que colaboran en la Unión Europea, tiene once años de historia. Me gusta empezar con un poco de historia porque seguro que todos recordamos dónde estábamos y qué hacíamos el 11 de septiembre del año 2001, porque ese es un momento que ha marcado un hito en el tema de seguridad, un antes y un después. Porque, aunque eso afectó especialmente a EEUU, la Unión Europea tomó, en ese momento, conciencia de que el terrorismo, los retos de seguridad en general, no eran un problema particular de un Estado miembro, que es lo que estaba pasando en España hasta entonces. Se veía el

terrorismo de ETA como algo regional, un problema de España; o el tema de Irlanda. Aquí sí que se vio que había una amenaza global y que podía afectar a nivel de seguridad y de economía, a muchos Estados miembros. En aquel momento, la Unión Europea tomó consciencia de este asunto y se iniciaron una serie de acciones que derivaron en el programa de seguridad. En esos días el alto representante en política exterior y de seguridad era Javier Solana, al que se le encargó que uniera a un grupo de personalidades entre las que se encontraban antiguos Ministros de Interior, primeros Ministros, etc., para que elaboraran una estrategia europea de seguridad y que se basara en qué riesgos, amenazas reales, había en ese momento a nivel de la Unión Europea.

Ese grupo de personalidades culminó una serie de operaciones que tenían que poner en marcha todos los Estados de la Unión Europea en común y además, se lanzó una línea preparatoria, como una línea previa de lo que sería después el programa de I+D+i en seguridad, que era la acción preparatoria en investigación de seguridad, donde se empezaron a financiar pequeños proyectos; hablamos de proyectos de máximo un millón de euros (1 M€), proyectos en coordinación, en consorcio con varios Estados miembros para ver en qué ámbito se podía colaborar mejor o en qué ámbitos había necesidad de interés común. Esta acción preparatoria se denominó PASR (*Preparatory Action for Security Research*).

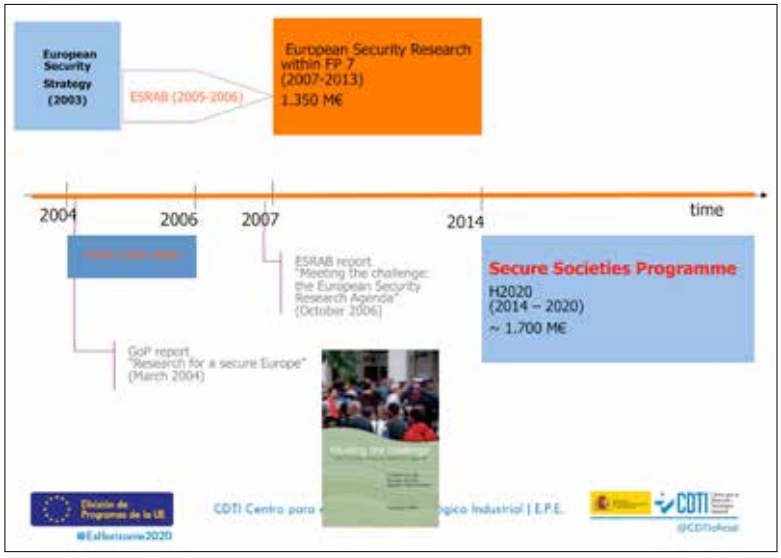


Figura 1

Paralelo a este PASR, se puso en marcha un grupo de expertos con perfil más técnico que se llamaba ESRAB (*European Security Research Advisory Board*), un grupo de asesores de la Unión Europea que desarrollaron más

en profundidad las líneas de trabajo y los ámbitos tecnológicos, principalmente, en los que se tendría que basar ese nuevo programa de investigación desarrollo e innovación en seguridad. Y eso derivó, finalmente, en que se encuadró un programa con mil trescientos cincuenta millones de euros (1.350 M€) bajo el paraguas del Séptimo Programa Marco de la Unión Europea que duró siete años (2007-2013) y en el que España participó con mucho éxito.

Quiero que se fijen en la foto de abajo (figura 1), ese informe Meeting the Challenge, donde el grupo ESRAB de expertos técnicos habían identificado las líneas prioritarias en las que se tenía que investigar. Es una foto del año 2006, pero prácticamente está vigente hoy en día, porque es verdad que las amenazas de seguridad van evolucionando, pero hay muchos componentes *drives* que realmente persisten en el tiempo. El crimen organizado sigue existiendo, hay distintas formas pero el crimen organizado está ahí, el terrorismo tiene distintas formas pero está ahí. Donde más lo hemos notado, últimamente, ha sido en el crecimiento espectacular del cibercrimen, ciberterrorismo, de las ciberamenazas, pero no deja de ser una forma más de amenaza a la seguridad. Este documento es interesante de consultar porque está vigente, y dado que el programa de seguridad en el FP7 fue bastante exitoso, este programa tuvo su continuidad en el Horizonte2020 que es el programa marco que está vigente actualmente y abarca desde el año 2014 al 2020. Además, el programa de seguridad va a tener continuidad a partir del año 2021, en el noveno programa marco que se va a llamar Horizonte Europa que ahora mismo está en planificación. Así pues, me voy a centrar en hablar del programa que está vigente actualmente para el que tenemos todavía tres años de convocatoria (2018-2019-2020) y que va a sentar las bases para el próximo programa. Este programa que se llama Sociedades Seguras o Reto Social 7, H2020.

SOCIEDADES SEGURAS (RS7) H2020

El programa marco de la Unión Europea I+D+i es el mayor programa de financiación a la I+D+i que existe en todo el ámbito europeo, sobrepasa las expectativas de cualquier programa nacional, se basa en subvenciones, siempre se van a dar subvenciones que pueden oscilar entre el 70 y el 100%. Para las administraciones públicas es al 100% siempre; además, hay unos costes indirectos que pueden ser de hasta el 25%.

Se estructura en tres grandes pilares que van desde la ciencia más fundamental, hasta la tecnología más aplicada que son los retos sociales; y es la columna de retos sociales donde se enmarca la investigación en seguridad, el programa actualmente se llama Sociedades Seguras. Y, al llamarse Sociedades

Seguras, veremos que nos vamos a centrar en un ámbito más focalizado en la tecnología y en los factores sociales y humanos de la seguridad. Nos vamos a encontrar diversos tipos de proyectos pero unos más centrados en la tecnología y otros en temas sociales y humanos.

La dotación presupuestaria es bastante elevada, mil setecientos millones de euros (1.700 M€) para el periodo 2014-2020. Es una dotación importante sabiendo que, prácticamente ningún país europeo, salvo ocho, tienen programa de seguridad I+D+i y que esta cantidad supone el 50% aproximadamente del dinero que, todos los Estados miembros, dedican a I+D+i en seguridad. Es un programa de mucha relevancia, y cuando se definió, la regulación donde se estableció el programa Horizonte2020, el epígrafe que aparece sobre seguridad es:

The specific objective is to foster secure European societies in a context of unprecedented transformations and growing global interdependencies and threats, while strengthening the European culture of freedom and justice.

- Europe has never been so peacefully consolidated, and the levels of security enjoyed by European citizens are high compared to other parts of the world. However, Europe's vulnerability continues to exist in a context of ever-increasing globalisation in which societies are facing security threats and challenges that are growing in scale and sophistication.
- The threat of large-scale military aggressions has decreased and security concerns are focused on new multifaceted, interrelated and transnational threats. Aspects such as human rights, environmental degradation, political stability and democracy, social issues, cultural and religious identity or migration need to be taken into account. In this context the internal and external aspects of security are inextricably linked. In order to protect freedom and security, the Union requires effective responses using a comprehensive and innovative suite of security instruments. Research and innovation can play a clear supporting role although it cannot alone guarantee security. Research and innovation activities should aim at understanding, detecting, preventing, deterring, preparing and protecting against security threats. Furthermore, security presents fundamental challenges that cannot be resolved by independent and sector-specific treatment but rather need more ambitious, coordinated and holistic approaches.
- Many forms of insecurity, whether from crime, violence, terrorism, natural or man-made disasters, cyber-attacks or privacy abuses, and other forms of social and economic disorders increasingly affect citizens. According to estimates, there are likely to be up to 75 million direct victims of crime every year in Europe (1). The direct cost of crime, terrorism, illegal activities, violence and disasters in Europe has been estimated at least EUR 650 billion (about 5 % of the Union GDP) in 2010. Terrorism has shown its fatal consequences in several parts of Europe and worldwide costing many lives and important economic losses. It also has a significant cultural and global impact.
- Citizens, firms and institutions are increasingly involved in digital interactions and transactions in social, financial and commercial areas of life, but the development of Internet has also led to cyber crime worth billions of Euros each year, to cyber-attacks on critical infrastructures and to breaches of privacy affecting individuals or entities across the continent. Changes in the nature and perception of insecurity in everyday life are likely to affect citizens' trust not only in institutions but also in each other. In order to anticipate, prevent and manage these threats, it is necessary to understand the causes, develop and apply innovative technologies, solutions, foresight tools and knowledge, stimulate cooperation between providers and users, find civil security solutions, improve the competitiveness of the European security industry and services, including ICT, and prevent and combat the abuse of privacy and breaches of human rights in the Internet and elsewhere, while ensuring European citizens' individual rights and freedom.

To enhance better cross-border collaboration between different kinds of emergency services, attention should be given to interoperability and standardisation. Finally, as security policies should interact with different social policies, enhancing the societal dimension of security research will be an important aspect of this societal challenge.

El programa se dirige a afrontar las vulnerabilidades que tiene Europa en medidas de seguridad, los problemas derivados de la globalización, a los aspectos migratorios, pero no desde el punto de vista de la migración, sino de seguridad derivada de la migración. También el programa aborda aspectos como operaciones civiles en misiones de paz, operaciones humanitarias como dar soporte a esas fuerzas multinacionales que actúan a veces fuera de las fronteras de la Unión Europea. Temas muy importantes como el terrorismo, todo el ámbito ciber, ciberterrorismo, ciberseguridad, va a aparecer y también se habla de todo lo relacionado con los aspectos humanos de la seguridad. Esto desde el año 2013.

A los dos años fue elegida la Comisión Juncker presidida por Jean-Claude Juncker. La Comisión presentó siete grandes ámbitos donde iba a centrar sus políticas y he destacado las más relacionadas con seguridad:

- Migración.
- Seguridad: terrorismo-radicalización-ciberseguridad.
- Lucha contra el cambio climático. Es importante porque hay un área en el programa de seguridad que es la gestión de crisis y desastres; y una parte muy importante de las crisis y desastres es el cambio climático. ¿Por qué hay más tormentas, por qué hay más inundaciones, por qué hay más olas de calor, por qué hay más incendios? Por el cambio climático, son retos de seguridad también.

SECURITY UNION (2015)

Asimismo, en el año 2015, en el discurso del Presidente de la Unión, Jean-Claude Juncker, destacó, muy importante, los retos de seguridad a los que se enfrentaba la Unión Europea. Y se elaboró la Agenda Europea de Seguridad. A continuación, se nominó un nuevo Comisario, dedicado exclusivamente al ámbito de la seguridad, Sir Julian King, que está de Comisario actualmente, y puso en marcha un grupo de trabajo: el Security Union.

Security Union no deja de ser un grupo en el que trabajan múltiples unidades de la Comisión Europea para valorar, elaborar políticas y poner en marcha temas técnicos y aspectos también de financiación, políticas de cualquier tipo o actividades, iniciativas, lo que sea, para mejorar la seguridad de la Unión Europea. Son ellos, este grupo de trabajo, los que han puesto en marcha todo el tema del registro de pasajeros, el PNR y todas las iniciativas que salen de la Security Union y que afectan a la seguridad de los ciudadanos europeos.

En todas estas reuniones mensuales, siempre hay una parte dedicada a investigación e innovación en seguridad; podemos hacernos a la idea del peso, de la relevancia que tiene la investigación de la seguridad a nivel de la Unión Europea.

SOCIEDADES SEGURAS: UN RETO SOCIAL

El reto Sociedades Seguras tiene dos vertientes, por un lado es un reto social; lo que busca es mejorar la seguridad de los ciudadanos ante un escenario de globalización y de amenazas crecientes en distintos ámbitos de la seguridad. También se menciona la garantía, no solo de la seguridad, sino de los servicios a los ciudadanos, de la garantía de que las infraestructuras y los servicios críticos de Europa para que sigan mejorando su prosperidad, su estabilidad política y su bienestar, a pesar de que haya ataques.

SOCIEDADES SEGURAS: UN RETO INDUSTRIAL

También es un reto industrial dado que, en el programa marco, uno de sus grandes objetivos es mejorar la competitividad industrial de la Unión Europea y el sector seguridad es relevante en un sector que está creciendo exponencialmente año tras año; se han hecho estudios en la Unión Europea de lo que supone como peso específico este sector, no hablamos de defensa sino de seguridad que incluye también ciberseguridad. En el año 2015, el sector empleaba a cuatro con siete millones de personas (4,7) en la Unión Europea con una facturación anual de aproximadamente doscientos mil millones de euros (200.000 M€) dividido en veinte subsectores.

Lo que busca el programa, a través de la financiación de proyectos, es mejorar la competitividad de las empresas del sector, sean microempresas, pequeñas empresas, o grandes multinacionales. Y nuestra labor, como administraciones públicas, es apoyar a estas empresas para que en un mundo global puedan demostrar que esas soluciones se pueden vender fuera de la Unión Europea.

El programa, actualmente, está centrado en el usuario final sabiendo que en el programa tienen que colaborar tres tipos de entidades: empresas privadas, universidades, centros de investigación, centros tecnológicos, asociaciones industriales y lo que llamamos actores institucionales, usuarios finales o *Practitioners* -aquellas entidades que practican una labor, en este caso garantizar la seguridad-.

Lo que busca la Comisión es que todo el programa se dirija a que todos esos actores institucionales utilicen las soluciones de seguridad que se desarrollan en el mismo.

OBJETIVOS Y ÁREAS QUE CUBRE EL PROGRAMA

El programa cubre las siguientes áreas:

- Lucha contra la delincuencia, el crimen y el terrorismo.
- Protección y resiliencia de infraestructuras críticas, modos de transportes y cadenas de suministro.
- Mejorar la seguridad y la gestión de las fronteras, en todas las fronteras, terrestre, marítima, aérea.
- Seguridad en el exterior, en misiones humanitarias, misiones civiles de paz fuera de las fronteras de la Unión Europea.
- Seguridad cibernética, en el séptimo programa marco no estaba incluido, estaba en el programa de tecnologías de la información y ahora está en este programa.
- Recuperación de Europa frente a crisis y desastres, tanto catástrofes naturales como provocados por el hombre.

- Aspectos sociales, éticos, de privacidad y libertad de los ciudadanos, serían los aspectos más humanos de la seguridad, y
- Estandarización e interoperabilidad de sistemas, por ejemplo hay ámbitos en que se desarrollan temas de estandarización de comunicaciones, estandarización de metodologías del ámbito forense, metodologías de investigación, etc.

PARTICULARIDADES DEL PROGRAMA

El programa marco Horizonte2020, lo pilota la Dirección General de Investigación (DG Research), pero en el programa de seguridad dos DGs aportan financiación: DG HOME (Anabela Gago es la máxima responsable del presupuesto) y DG Connect (Dirección general de Telecomunicaciones y sistemas de información en la Comisión Europea). DG Connect se centra principalmente en el área de ciberseguridad y protección de infraestructuras críticas y DG HOME en todo lo demás del programa de seguridad.

La orientación del programa es hacia el usuario final (*Practitioners*). La gran mayoría de los proyectos tiene que tener usuarios finales como socios de los mismos.

Los proyectos son muy cercanos a mercado, se termina la mayoría en pruebas de concepto, pilotos, demostraciones, prototipos, incluso a veces en cosas que podemos utilizar en nuestro día a día.

El programa es eminentemente civil, porque el programa marco dentro de sus bases tiene ese epígrafe: el programa marco es exclusivamente civil.

Algunos proyectos resultarán clasificados. Es una particularidad del programa, más o menos el 30% está clasificado y los niveles pueden llegar hasta EU-SECRET que es el nivel RESERVADO, y es muy habitual que haya ese tipo de proyectos, no es ningún problema.

Muchos de los proyectos lo que buscan es realizar demostraciones pilotos, estandarización de sistemas, tecnologías probadas en escenarios particulares. Se busca que la tecnología sea de utilidad.

Aspectos éticos de los proyectos. No hay que dejar de lado que los proyectos tienen un componente ético: de protección de datos, de privacidad de información, etc. y eso hay que tenerlo en cuenta cuando se planifica un proyecto.

EL "OTRO" GRAN RETO DEL PROGRAMA

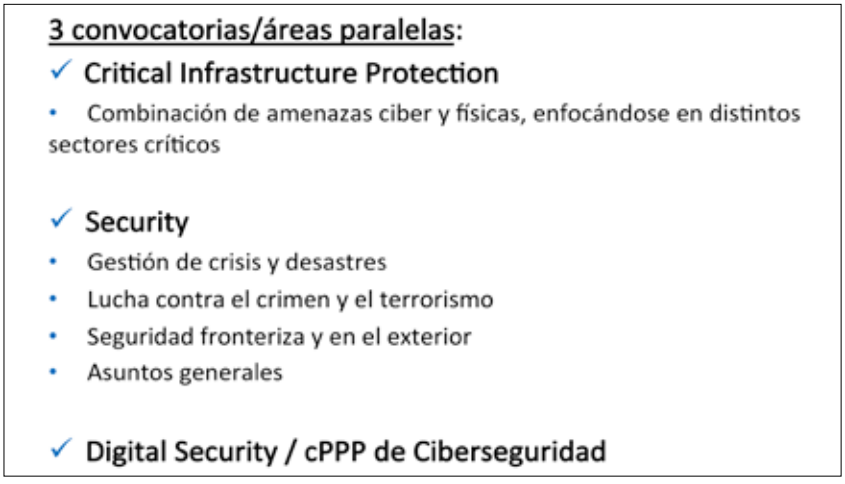
El programa, además del reto de integrar a usuarios, que todos cooperen con la industria y demás, tiene otro gran reto y es que es un programa a medio y largo plazo. Nuestra mentalidad tiene que cambiar y tenemos que pensar no en necesidades para mañana, sino para dentro de cinco años.

El ciclo de vida de un proyecto desde que se define un tópico (*topic* – tema que va a salir) y para el que se van a presentar propuestas, que derivará en la financiación de algunos proyectos; abarca desde que se identifica esa necesidad hasta que finaliza el proyecto, aproximadamente cinco o seis años. Algunas propuestas pueden cambiar en ese plazo en el sentido de que la idea puede evolucionar, se puede mejorar..., pero siempre tenemos que pensar en el más allá, no a corto plazo de un año, sino a cuatro años vista.

Para ello, tendremos que poner nuestra mente en blanco y decir: ¿qué puede ser una amenaza en cinco años? por ejemplo. ¿Los enjambres de drones pueden ser una amenaza? Pues sí. ¿Los vehículos autónomos pueden ser una amenaza? Pues sí. ¿Las empresas 3D pueden ser una amenaza? Pues sí. Todo esto son aspectos tecnológicos que pueden ser muy relevantes en la vida de los ciudadanos europeos dentro de cinco o seis años, pero también pueden tener una componente de amenaza, y todo son temas que pueden aparecer en el programa de seguridad. Entonces, nuestra mente tiene que ir hacia el futuro.

ESTRUCTURA ACTUAL DEL PROGRAMA CONVOCATORIAS

El programa actualmente se estructura en tres grandes convocatorias, son convocatorias anuales, todas en una única fase; es decir, lo que se presenta el día del cierre de la convocatoria es lo que se evalúa y es lo que se va a financiar si se aprueba. No tenemos varias fases, hay otros programas dentro del programa Horizonte2020 que son en varias fases, se desarrolla una idea preliminar y luego una idea completa; aquí no, es un programa en una única fase.



Hay tres convocatorias porque el dinero proviene de distintas unidades de la Comisión, por eso se ha estructurado en tres convocatorias, pero todas abren y cierran el mismo día. La presentación de las propuestas es siempre a nivel telemático, a través de portal web que está securizado por supuesto y, prácticamente, todos los proyectos tienen que ir en consorcio: al menos tres entidades de tres países distintos. Ese es el mínimo, lo habitual es que no sea tres, sino cinco, siete, ocho, diez, o más dependiendo de la envergadura del proyecto.

Las tres convocatorias se estructuran así:

- Critical Infraestructures Protection. Combinación de amenazas ciber y físicas, enfocándose en distintos sectores críticos. Protección de infraestructuras críticas. Es una de las grandes convocatorias, tiene pocos temas pero un presupuesto muy grande. Ahí se combinan el presupuesto de DG HOME con la DG CONNECT y abarca la seguridad física y la seguridad ciber.

- La convocatoria de Seguridad - Security- cubre las siguientes áreas:

  - Gestión de crisis y desastres
  - Lucha contra el crimen y el terrorismo
  - Seguridad fronteriza y en el exterior
  - Asuntos generales

La financiación viene exclusivamente de DG HOME y la última que es:

- Digital Security/CPPP de Ciberseguridad.

CONVOCATORIA: INFRAESTRUCTURAS CRÍTICAS CRITICAL INFRAESTRUCTURE PROTECTION

Tiene dos grandes objetivos, porque en realidad tiene dos grandes temas. No todos los años van a abrir todos los temas esto es la visión global de la convocatoria, pero habrá años que haya una convocatoria y otros años, otra. Pero hay que estar pendientes, podemos informaros tanto CDTI, como los servicios de innovación de Policía Nacional y de Guardia Civil, que tenéis a vuestra disposición.

- Objetivo 1: Prevención, detección, mitigación y respuesta ante incidentes/ataques cíber y físicos a infraestructuras críticas europeas. Aquí se cubren distintos ámbitos de las infraestructuras críticas como pueden ser:

- Diversos sectores objetivo: energía, transporte, financiero, salud, agua, infraestructuras de comunicaciones, E-commerce y cadena postal, Sites industriales sensibles, etc. De hecho hay una lista orientativa pero se podrían presentar otros sectores críticos que puedan ser identificados. Se financian grandes proyectos, hablamos de proyectos en torno a los doce, quince millones de euros (12-15M) con una participación muy activa de los propios operadores de las infraestructuras críticas de cada sector en particular. Cada proyecto se centrará en un sector. Aquí es donde tenemos que abordar la perspectiva de cuáles son las amenazas que sufren este tipo de infraestructuras en su día a día.

• Objetivo 2: Seguridad en *Smart Cities* y entornos urbanos. Garantizar la seguridad en los entornos urbanos y las ciudades inteligentes (*Smart Cities*). También se aborda toda la problemática de seguridad en grandes aglomeraciones, grandes manifestaciones, eventos deportivos, conciertos, etc. Se buscan soluciones integrales de seguridad para garantizar la seguridad de las personas en esos entornos.

Por esta razón vamos a encontrarnos dos tipos de proyectos uno más centrado en infraestructuras críticas y otro más centrado en *soft targets*: ciudades, ciudadanos, centros comerciales, etc. Tendremos soluciones de seguridad diferentes. Es verdad que ambas áreas se centran más en el ámbito tecnológico.

CONVOCATORIA: SECURITY (SEC)

A continuación pasamos al segundo gran bloque con más proyectos y más presupuesto que es el ámbito de *security*. Tiene 4 grandes áreas:

• DRS: Disaster-resilient societies

• FCT: Fight against crime and terrorism

• BES: Border and External Security

• GM: General Matters

DRS: Disaster-resilient societies

Objetivo: centrarse en buscar soluciones para minimizar los peligros, las amenazas, de grandes catástrofes o grandes crisis que puedan ocurrir. Se van a buscar soluciones sobre todo para usuarios de protección civil y emergencias y cualquier tipo de seguridad que actúe como primer respondiente

o como apoyo en cualquier tipo de catástrofe también se tiene que sentir como usuario de estas tecnologías.

Se cubren distintas áreas: gestión de crisis y protección civil, recuperación de desastres, amenazas NBRQ, comunicaciones seguras, etc. Y no solamente en el ámbito tecnológico sino que también en el humano y social. Igualmente se buscan temas relacionados con recuperación de víctimas, cómo se puede hacer apoyo psicológico a las víctimas, etc.

Busca básicamente tres grandes temas: dotar a unidades de protección civil y emergencias (o similares) de herramientas, tecnología, procedimientos, etc., en necesidades comunes, es decir una unidad de protección civil española y una unidad francesa que tengan requerimientos comunes y que puedan desarrollar una tecnología que les interese a ambas y les facilite la coordinación para hacer frente a crisis y desastres de una manera más eficiente. Hay aspectos sociales y humanos que no hay que dejar de lado, como los *topics* que se centran en ese ámbito y hay ejemplos de los diferentes ámbitos en que se ha centrado esta convocatoria.

FCT: Fight against crime and terrorism

La siguiente sub-área dentro de la convocatoria de security es la lucha contra el crimen y el terrorismo.

Objetivo: evitar incidentes o mitigar sus efectos, procedentes del crimen y el terrorismo. Se busca el desarrollo de tecnologías y capacidades para Fuerzas y Cuerpos de Seguridad, también prevenir el crimen y el cibercrimen, evitar el tráfico ilegal: de seres humanos, de mercancías, animales, de lo que sea. Asimismo, temas relacionados con terrorismo, así como temas sociales y humanos en el ámbito del cibercrimen y ciberterrorismo, incluidos los temas de radicalización. Todos los temas de radicalización desde el punto de vista social, también se cubren en esta convocatoria.

Cubre las áreas de: tecnologías forenses, capacidades para fuerzas y cuerpos de seguridad, explosivos, terrorismo y crimen organizado, cibercrimen y ciberterrorismo, lucha contra el blanqueo de capitales, lucha contra el tráfico de seres humanos y explotación sexual, financiación de redes terroristas y criminales, radicalización, extremismos, aspectos sociales/humanos de la seguridad, etc.

Todo esto en línea con los dos grandes temas que se identifican en la Agencia Europea de Seguridad que son, el terrorismo, el crimen organizado y cibercrimen. Son prioridades actuales para la Unión Europea no solo ahora, lo van a ser también en el futuro; porque el presupuesto para

seguridad va a aumentar mucho a partir del año 2021 y dentro del tema del cibercrimen es un ámbito boyante, desgraciadamente, para las redes de crimen organizado.

BES: Border and External Security

Objetivo: desarrollo de tecnologías y capacidades para mejorar sistemas, equipos, herramientas, procesos y métodos que permitan mejorar la seguridad de las fronteras. Hablamos de diferentes fronteras terrestres, marítimas, border checks en aeropuertos, *land borders*, *Smart bordes*, frontera regulada, frontera no regulada; es decir, cubrimos todo.

En relación con las fronteras exteriores, desarrollo de tecnología y capacidades para apoyar a las Fuerzas de seguridad de la UE que participan en apoyo a operaciones civiles en el exterior.

Cubre las áreas de: seguridad marítima, frontera terrestre, puntos de entrada y salida, seguridad aérea, identificación de personas, seguridad en la cadena de suministros y gestión de la información en el contexto de la seguridad exterior y prevención de conflictos y apoyo en operaciones de paz

GM: General Matters

Por último la sub-área de asuntos generales, donde se financian dos grandes áreas.

Objetivo 1: creación de redes y estructuras estables de *stakeholders* que trabajen en el ámbito de la seguridad: usuarios finales que trabajen en diversos ámbitos tecnológicos o geográficos, redes de laboratorios, redes de *think-tanks* en seguridad, etc.

Se ha mencionado la red I-LEAD, pues este es un ejemplo de una red de entidades policiales que colaboran entre sí y están amparadas por este *topic*, por el General Matters. Se pueden financiar redes en lo que sea, temas de ámbito forense, de extinción de incendios, temas de NBQ, etc.

Objetivo 2: acciones horizontales que permitan financiar PCPs (*Pre-commercial procurement*) en el ámbito de la seguridad, incluyendo CSAs (*Coordination and support actions*) preparatorias de dichos PCPs.

La compra pública pre-comercial es comprar tecnología, a través de un grupo de profesionales con una necesidad común y que ponen en común unos requisitos, lanzan una licitación y hay empresas, consorcios, o indi-

vidualmente presentan ofertas y se selecciona la mejor solución en relación calidad-precio. Esa tecnología se desarrolla, pagada por la Unión Europea al 100% y luego esos usuarios prueban la tecnología e incluso pueden adquirirla.

CONVOCATORIA: DIGITAL SECURITY (DS) CIBERSEGURIDAD.

La última convocatoria es la de ciberseguridad, que es un poco particular porque la I+D+i ciberseguridad, se financia en muchas partes de Horizonte2020. Aquí voy a contar la que se financia en el programa sociedades seguras, pero no solo vamos a encontrar ahí financiación, hay que tener el radar un poco abierto porque a veces nos van a surgir oportunidades en el programa de tecnologías de la información o en otros programas. Se financia también en el de transportes, salud, energía, bio-economía…, en definitiva, tenemos que estar alerta.

Objetivo: basado en la **Estrategia europea para la ciberseguridad,** esta convocatoria se dirige a desarrollar herramientas que aumenten la confianza en la seguridad digital y que apoyen a los usuarios finales de tecnología en el desarrollo de servicios confiables y seguros.

Ejecución de la **Estrategia Europea de Ciberseguridad** (2013) y del **Paquete legislativo en materia de ciberseguridad** (2017)

La ciberseguridad que se financia aquí es aplicada, lo que se financia en tecnologías de la seguridad es más de base, temas de criptología, criptografía y demás. En el programa de seguridad es un poco diferente.

En el año 2013 se lanzó la Estrategia Europea de Ciberseguridad y de hecho la convocatoria va en línea con lo que se definió en esa Estrategia que fue paralela con la Estrategia Nacional de Ciberseguridad española. Lo que se busca es dotar de herramientas a la sociedad, no solo a los usuarios, es más amplio, para mejorar la confianza en la seguridad digital. Aquí nos encontramos que los usuarios son muy variados, pueden ser asociaciones sectoriales, grupos de usuarios de Internet, personas individuales, hospitales, … puede ser cualquiera.

Además de la estrategia de ciberseguridad, en el año 2017, se lanzó un Paquete Legislativo en materia de ciberseguridad, porque las amenazas de ciberseguridad van en aumento de forma espectacular; por ello, la Unión Europea está viendo cómo dirigirse a todo este ámbito de forma eficiente ¿cómo se está haciendo? La parte de investigación se está abordando a través

del programa marco, aunque no solamente, también hay otros programas que van en paralelo y que a futuro van a ir en paralelo también donde se está financiando investigaciones en ciberseguridad.

En el año 2016 se lanzó una iniciativa público-privada de ciberseguridad a través de la cual, la Unión Europea se comprometió a poner encima de la mesa, más o menos quinientos millones de euros (500 M€) para financiar proyectos en I+D+i entre 2016 y 2020, bajo el paraguas de Horizonte2020. Este dinero, como pueden imaginar, es insuficiente; pero sí que se están movilizando fondos por otras vías, más fondos para la compra de tecnologías que no están en este programa, pero la idea es que se sienten las bases en materia de ciberseguridad en herramientas tecnológicas.

Se han lanzado distintos paquetes legislativos en ciberseguridad y a raíz de todo esto, la cPPP (*contractual Public-Private partnership)* de ciberseguridad, de la nueva regulación en materia de protección de datos, paquete legislativo de ciberseguridad, etc. se financian proyectos tanto en el programa de seguridad actual, como en el de tecnologías de la información, de salud, de energía, etc. En el de seguridad nos vamos a encontrar temas relacionados, por ejemplo, con: desarrollo de herramientas *cyber-ranger*, es decir, herramientas que nos sirven para monitorizar ciberataques, para formar a personal que, día a día, actúan frente a estos ciberataques, herramientas que puedan recuperar infraestructuras críticas en el ámbito de ciberataques sofisticados. Hablamos de sectores implicados como el financiero, el de transportes, el de salud y el de energía. Nos vamos a encontrar con este tipo de áreas donde se van a financiar proyectos.

De cara al próximo Horizonte Europa, la ciberseguridad se va a financiar en dos ámbitos, una financiación creciente en lo que será el programa de seguridad en el Horizonte Europa, pero también se va a lanzar un programa paralelo que se llamará *Digital Europe Programme*. Este programa va a estar dotado con mucho dinero y se va a financiar investigación y desarrollo en ciberseguridad.

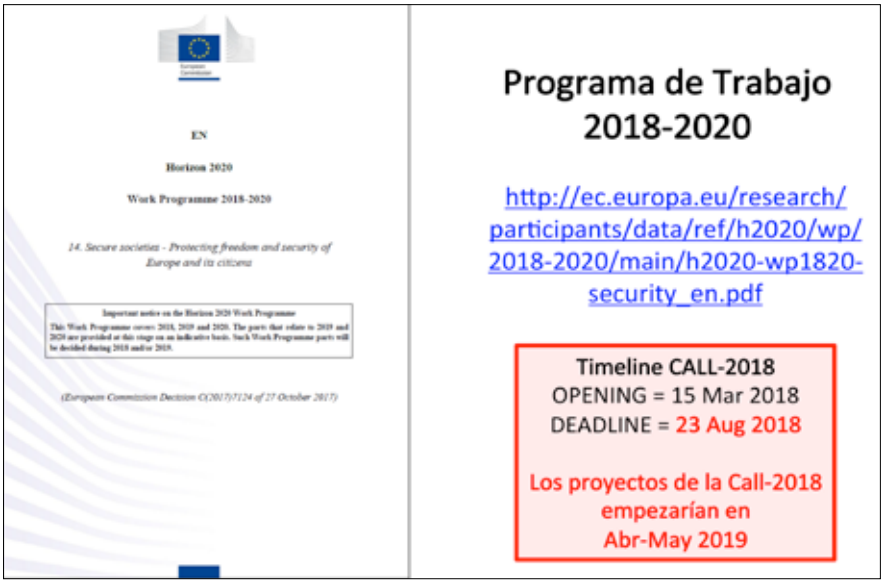
PARTICULARIDADES Y FILOSOFÍAS SOBRE EL PROGRAMA DE SEGURIDAD

La filosofía es no dar solución a temas particulares, sino a necesidades a nivel común, a nivel global, entre Fuerzas y Cuerpos de Seguridad de distintos países. Eso es la base del programa de seguridad; por lo que, cuando se piense participar en este programa habrá que pensar en cuál es la necesidad, -me consta porque estoy en un foro internacional, que hay compañeros de otros países- nos juntamos y lo ponemos en común. Esta filosofía nos la va a

proporcionar la Unión Europea, y esta es la filosofía del programa. Lo que se busca es que los usuarios piensen "a lo grande" y que esa tecnología pueda servir a todos, no solamente a uno en particular.

Desde el año 2016, se han instaurado unas condiciones para poder participar en estos programas que es lo que se llama las condiciones de legibilidad. Si no se cubren esas condiciones, no se puede presentar el programa y esas condiciones suponen que la gran mayoría de los temas que abren, que haya, al menos, un número mínimo de tres usuarios de tres países distintos como socios de las propuestas. Tengan en cuenta que esta es una condición *sine qua non* para participar. Lo mínimo es que sean tres, en algunos *topics* son cinco y en algunos casos son ocho.

Ejemplos: cada año cambian de manera que si entran en un *topic* para presentar una propuesta van a competir con las propuestas que se presentan a ese tema. A veces, hay pocas propuestas en un *topic*, tengan en cuenta que es un programa muy competitivo, en forma general, pero luego en particular, en algunos temas no es tan competitivo. Es decir, las opciones de resultar financiados no son tan bajas, de hecho la tasa de éxito del Ministerio del Interior en España es altísima, una de cada dos propuestas ha resultado financiada. El 50%, verdaderamente creo que es una oportunidad. Además, desde este año 2018, se ha creado una filosofía de programa que es dejar siempre todas las líneas tanto en la DRS, lucha contra el terrorismo y seguridad fronteriza, un *topic* que se llama *Open* (abierto) donde se puede presentar lo que

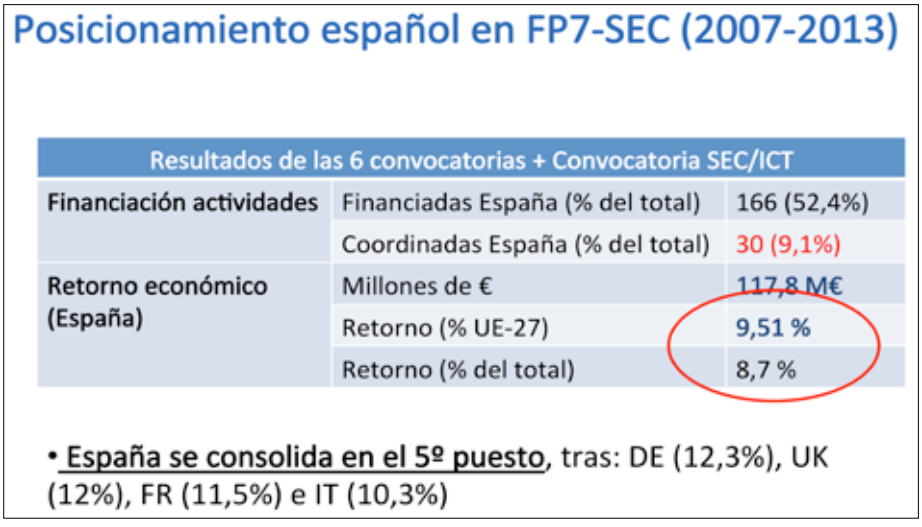


se quiera, siempre y cuando haya un mínimo de cinco usuarios finales como socios de la propuesta. Es decir, ese grupo son los que van a decidir en qué se tiene que investigar. La Comisión no nos va a decir en qué tenemos que investigar, sino que somos nosotros los que tenemos que decirle a la Comisión en lo que nos tiene que financiar para investigar. Es una gran oportunidad para que, si no vamos en ninguna línea y tenemos una necesidad detectada, nos podamos presentar.

El programa de trabajo 2018-2020 abarca tres convocatorias, la de este año que está abierta hasta el 23 de agosto, la del año 2019 que se abre en el mes de marzo pero su texto va a ser oficial a partir de finales de julio y unos títulos, no está desarrollado, pero sí están los títulos de lo que va a haber en el año 2020. De manera que podemos prever lo que va a salir en años futuros y planificarnos.

Importante, los proyectos que se presenten en agosto de este año serán evaluados entre agosto y final de año. Y, entre finales de diciembre principios de enero se sabrá el resultado de los proyectos y se intentará firmar los proyectos lo más rápido posible de manera que en el mes de abril o mayo como muy tarde estos comiencen, porque la evaluación es rápida pero no puede ser más rápida.

¿Quién evalúa estos proyectos? Un *pool* de evaluadores externos, independientes, identificados por la Comisión Europea.



Anabela Gago nos contó el posicionamiento español en este programa, posicionamiento bastante bueno en estos momentos. España ha subido mucho en el programa marco en los últimos cinco años, y estamos muy bien

acostumbrados a tener buenos resultados. Podemos estar contentos porque en seguridad en el año 2007 empezamos muy mal, tuvimos un retorno del 3,5% y ahora estamos en el 10%, hemos mejorado mucho.

En la primera fase del programa España obtuvo entre el año 2007 y 2013, el quinto puesto después de Alemania, Reino Unido, Francia e Italia; pero si miramos como estamos ahora, estamos en cuarto lugar, y ha cambiado el orden de los países: Italia, Reino Unido, Alemania, España, Francia. Reino Unido se va con el Brexit y España va a avanzar. Esto es un reto para todos al final, avanzamos pero también nos tenemos que implicar más y mejor.

¿Por qué tenemos un buen posicionamiento? Por muchos motivos y, sobre todo, porque han hecho mucho las Fuerzas de Seguridad para que el programa fuera bien. Realmente, somos una referencia a nivel europeo, la Comisión nos menciona constantemente en sus comunicaciones y España es un ejemplo de implicación súper activa en el programa de seguridad. Hay que reconocerlo porque lo hacemos como una labor que en el día a día es común, además de implicar a muchos tipos de entidades muy activas.

La gran diferencia entre una administración pública y una empresa, es que la administración no puede contratar a nadie para desarrollar ese proyecto, lo hacemos como una labor adicional a nuestro trabajo de día a día, es un esfuerzo adicional; una empresa sí puede contratar a alguien porque tiene más flexibilidad, por eso hay que reconocer la labor que hacen las Fuerzas y Cuerpos de Seguridad.

Motivos del éxito de España:

- Numerosos proyectos coordinados, aproximadamente cincuenta.

- Contribución activa a los programas de trabajo que son las convocatorias, mandamos temas de interés, comentarios a las convocatorias, y a través de los servicios de innovación hacemos muchas jornadas para ver qué ideas tienen, nos juntamos con otros países para poner en común ideas que tenemos y que podemos defender de forma conjunta.

- Preparación de propuestas con suficiente antelación. Preparamos notas, comunicaciones, meses antes.

- Buenas redes y contactos. Hemos desarrollado unas redes muy potentes a nivel nacional y a nivel europeo. Lo único que nos falla en España con respecto a otros países es el tema de los lobbies, pero no en el ámbito de los usuarios, sino en el de las empresas. Es decir, comparando con Ho-

landa, Alemania, Austria, veo que tienen unas asociaciones sectoriales super potentes, unos lobbies que se mueven muy bien a nivel internacional, y nosotros nos quedamos un poco cortos.

- Excelente implicación de usuarios finales. Sobre todo reconocer labor de las Fuerzas y Cuerpos de Seguridad con una excelente implicación de usuarios finales. De hecho, el año pasado, de todos los proyectos en los que apareció participación española, quizás en el 80% había usuarios españoles. Es una forma de destacar, hay un espaldarazo de los usuarios a las empresas y universidades españolas y eso es una labor de agradecer.

SOCIEDADES SEGURAS: 2019-2020 Y MÁS ALLÁ

El programa se abrirá en marzo del año 2019, la convocatoria estará disponible a finales del mes de julio del año 2018, ya la hemos votado y tiene que estar a punto de publicarse; algunos temas se van a excluir porque ya se habrán cubierto en el año 2018; y como va a seguir abierto este cajón que se llama "*open*" donde pueden presentar lo que quieran, os animo a que lo hagáis; cosas que pueden ser de interés y que tengan posibilidad; porque es algo que no solamente necesitan ustedes, sino también otros usuarios. Creo que habrá muchas oportunidades en este ámbito, la Comisión va a poner bastante dinero.

Se está preparando también la convocatoria 2020, tuvimos una reunión hace veinte días en Bruselas, primera toma de contacto y tenemos otra en septiembre y octubre del año 2018. Yo me voy a apoyar tanto en Policía Nacional como en Guardia Civil para este tema.

Se está planificando el próximo programa marco, nosotros estamos centrados en un área que se llama clúster. En la parte de sociedades seguras tenemos más presupuesto porque nos han mezclado con una temática que es más de ciencias sociales y humanidades. Esto es una propuesta de la Comisión, ya se verá si termina así, pero por lo menos vamos a estar ahí y va a haber presupuesto.

PROYECTOS FINANCIADOS

Uno en el que participó la Policía muy activamente es el **ABC4EU**, sobre temas en aeropuertos, los puntos ABC.

Es un ejemplo que se mostró hace ocho meses, en el mes de noviembre, y que fue todo un éxito. La Comisión se quedó sorprendida de los resultados del proyecto.

CLOSEYE: Coordinado por Guardia Civil.

SAURON: Coordinado por el puerto de Valencia sobre infraestructuras críticas.

ASGARD: Sobre análisis de Big Data en fuentes abiertas en el que participa muy activamente el Ministerio del Interior.

COMMUNITY OF USERS ON SAFE, SECURE AND RESILIENT SOCIETIES

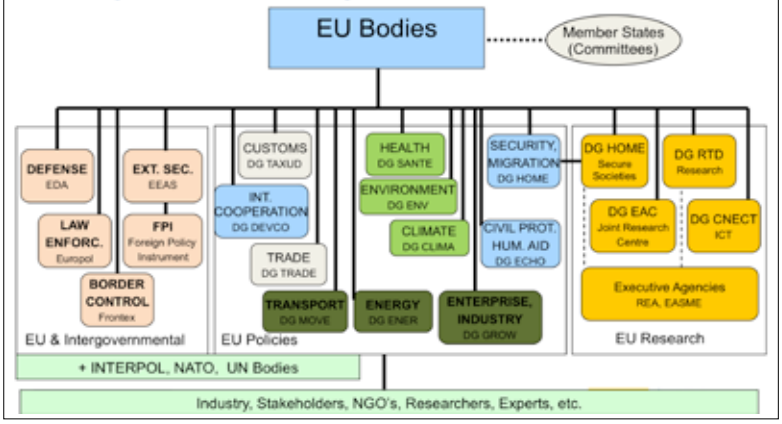
Por último, existe una comunidad de Usuarios, muy potente, que se reúne tres veces al año, se llama CoU y la próxima reunión es en diciembre. Se va a celebrar en paralelo con el Security y es muy interesante asistir porque es verdaderamente donde se reúnen los usuarios europeos en la temática particular. Es decir, si hablamos de Border Security, va a estar gente de aduanas, de fronteras, de todos los países europeos.

Definición de la CoU Europea

*The **Community of Users on Secure, Safe and Resilient Societies** is launched to become an efficient platform of exchanges among different actors of different branches of security and crisis management*

https://www.securityresearch-cou.eu/

A complex EU landscape: with similarities with MS



Objetivos de la CoU

1. <u>Que los resultados de la I+D+i lleguen al mercado</u>
2. Recabar necesidades de los usuarios (practitioners/end-users) y que éstas se reflejen en los programas de financiación Europeos (I+D+i, ppalmente)
3. Identificar herramientas y desarrollo con alto potencial y de interés para los usuarios
4. Apoyar la competitividad de la industria Europea de la Seguridad
5. Servir de puente entre la experiencia de los usuarios y la labor de los "policy-makers". Impacto en políticas
6. Facilitar la implementación de dichas políticas

En paralelo también se ha organizado una comunidad de usuarios, española. Ya lo sabéis os dejo el contacto de la persona que está conectando la red y actualmente hay más de ochenta usuarios españoles implicados, con lo cual, encantados de recibir a más miembros para participar. Va a haber once grupos de trabajo que comenzarán a partir de septiembre.

EL EQUIPO DE SOCIEDADES SEGURAS EN ESPAÑA

- Ramón Darder de Guardia Civil.
- José Francisco López de Policía Nacional.
- Marina Martínez, de nuestra oficina en Bruselas.
- Maite Boyero Egido en Madrid.

GESTIÓN DE INNOVACIÓN EN LA GUARDIA CIVIL Y H2020

RAMÓN DARDER COLOM
Teniente coronel de la Guardia Civil

Desde hace veinte años estoy cooperando, colaborando con Policía Nacional, con Policías Locales, con las que tienes que trabajar por compartir demarcación; y fruto de esa colaboración, hoy en día, tengo el placer de trabajar con el Servicio de Innovación y Desarrollo de la Policía Nacional. Pero también en mi pasado, tanto en Madrid como en Baleares, he tenido el placer de trabajar conjuntamente, en investigaciones, también con Policía Nacional. El súmmum llegó cuando el Jefe Superior de Baleares, el Comisario Antonio Jarabo, en una reunión me dijo que me había propuesto para una medalla y que mi coronel estaba de acuerdo. Fue una medalla la de American Policial, distintivo blanco. También, me premiaron con un curso de investigación económica y financiera en la División de Formación y Perfeccionamiento. Todo esto, lo cuento porque ahora mismo, desde mi posición en innovación tecnológica en Guardia Civil, dentro de la Jefatura de Servicios Técnicos, el día a día es colaboración y cooperación con Policía Nacional, con Policías Europeas, con Policías Municipales y Autonómicas españolas, con empresas españolas europeas, con universidades, etc. En este mundo no estamos solos y como veremos, tenemos que abrirnos; no podemos quedarnos encerrados en nuestras oficinas. Esta labor es muy abierta, es internacional.

¿Por qué tenemos un servicio de innovación tecnológica en la Guardia Civil? Tenemos que ir al mapa estratégico. Hace unos cuantos años el Estado Mayor de la Guardia Civil dibujó lo que era la dirección estratégica, los objetivos estratégicos y ahí teníamos que fortalecer relaciones con entidades nacionales e internacionales.

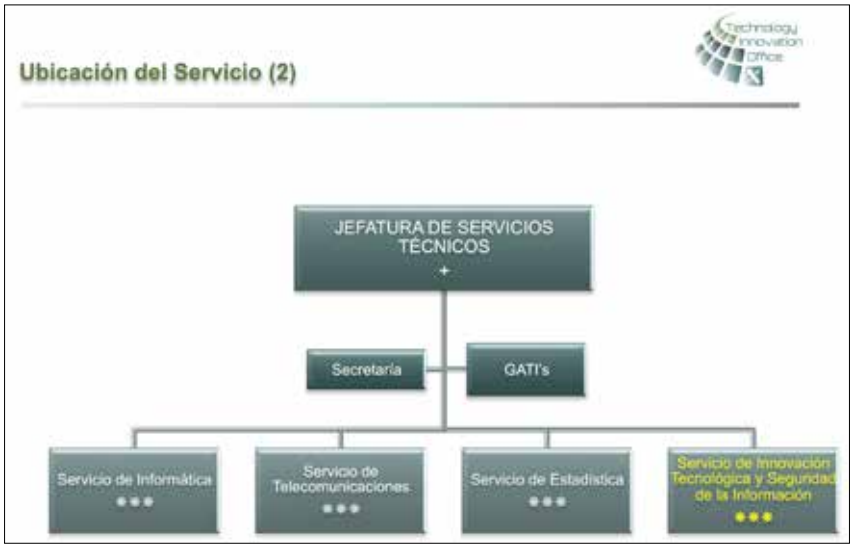
Potenciar la participación, en el ámbito de la Unión Europea, con lo que hacemos en innovación tecnológica, también colaboramos en impulsar las tecnologías de la información y las comunicaciones como herramienta fundamental para la prestación del servicio y el impulso de I+D+i.

Por eso existimos, y ¿qué base legal tenemos? En el año 2007-08 se creó una oficina de seguridad de la información que fue también el embrión de una oficina de innovación tecnológica, justo cuando en Europa se introdujo la I+D+i de seguridad en el programa de trabajo y la orden genera la actual, la que el servicio de innovación tecnológica tiene su fundamento, es la orden general que trata de la organización de la Jefatura de Servicios Técnicos de la Guardia Civil, y esta es la razón de ser del servicio, el órgano gestor y técnico encargado del estudio y análisis de nuevas tecnologías en el ámbito de la I+D+i susceptibles de ser utilizadas por el Cuerpo de la Guardia Civil; porque tenemos que usar lo que la tecnología disponible nos ofrece.

Desde la última remodelación que hubo de la Guardia Civil que se pasó de Subdirecciones a Mandos -la Jefatura de Servicios Técnicos dependía de la Subdirección General de Apoyo-, con la última reestructuración se le añadió la palabra Innovación; con lo que ahora dependemos del Mando de Apoyo e Innovación. Esta reestructuración fue similar en el seno de la Policía Nacional cuando se creó el Mando de Investigación con información y ciberdelincuencia. Vemos que tenemos un punto a nuestro favor, hemos puesto el apellido Innovación en el seno de la Subdirección General; es de-

cir, en el Mando, que en nuestro caso es un Teniente General. Y dentro de la Jefatura de Servicios Técnicos, nos encontramos la tecnología pura y dura; los dos servicios de los servicios centrales de los más potentes de la institu-

ción como el de informática y el de teleco que, entre ambos, suman más de doscientas personas y titulados en ingeniería superior; técnicos también hay bastantes. En nuestro edificio hay muchos ingenieros, de todas las escalas, incluso facultativas y funcionarios.



El Servicio de Estadística al que llegué hace cuatro años a Madrid, donde seguía colaborando con Policía Nacional en el seno del Gabinete de Estudios y Coordinación, es el Área de Estadística, Grupo técnico de trabajo del sistema estadístico de criminalidad, y en el que sigo haciendo algunas tareas. El Servicio de nueva central tecnológica está ahí encuadrado, en el organigrama general de la Guardia Civil, en un rincón, pero no podemos quedarnos en un rincón dentro de nuestra Dirección General y tener relaciones telefónicas por correo electrónico, tenemos que abrirnos a instituciones europeas; tenemos contacto con DJ HOME Connect, del que formo parte del Comité de programas. Trimestralmente, tenemos nuestra posición, nuestro puesto.

Trabajamos con Frontex, tenemos una Jefatura fiscal, también tenemos un servicio marítimo que ahora mismo está en torno a las sesenta patrulleras pequeñas y tres barcos de altura. Con Frontex tenemos mucha colaboración. Con Ministerios la relación es diaria, pertenecemos al mismo grupo de trabajo. Con universidades y con Organismo Públicos de investigación como el CSI, INTA y Ciemac, todos estos organismos que dependen del Ministerio de Ciencia e Innovación y Universidades. También, con empresas públicas, privadas, fundaciones, por ejemplo, estamos en un proyecto que lidera la Fundación Real Instituto Elcano.

Guardia Civil, tiene muchas Unidades e intereses en participar en este tipo de proyectos y, de alguna manera, hay que coordinarlos. Hay que informar con quién se colabora para no llegar al extremo de que la Guardia Civil sea competidora de sí misma. Si una Unidad por su cuenta establece contactos con una universidad u otro cuerpo policial extranjero y otra Unidad de Guardia Civil inicia contactos con otra empresa, se presentan a *topics* iguales en consorcios; tenemos que centralizar la actividad que todas las Unidades de Guardia Civil realizan en este sentido. No podemos llegar a que Unidades de Guardia Civil sean competidoras entre sí. De esta forma y desde el principio, vamos a dirigirlo desde la Unidad tecnológica.

En este punto, yo comentaba una anécdota de por qué innovamos, y hay personal de muchas Unidades nuestras que dicen estar satisfechas con lo que hacen, pero posiblemente estén anclados en sus procedimientos, en sus métodos; y, quizás, innovando se pueden conseguir los objetivos con más facilidad, en menos tiempo. La anécdota que cuento es la de vigilancia de costas: cuando mi padre llegó en el año 67 destinado a Mallorca, la costa se vigilaba con personas, muchas personas, todas las noches, a lo largo de la línea. Cuando yo llegó a Mallorca en el año 98, ya teníamos patrullas fiscales, con prismáticos de visión nocturna. Cuando dejé Baleares en el año 2013, teníamos una red de sensores fijos más camiones móviles, el SIDE, sistema de vigilancia exterior. Teníamos desplegadas por la costa Unidades de sensores de radar y electrónicos. Esa evolución es natural, no podemos seguir anclados porque hay que evolucionar. Seguramente, ahora conseguimos nuestros objetivos con más rapidez o con menos esfuerzo a nivel humano, porque las personas son nuestro bien más preciado, pues vamos a delegar ese trabajo en la tecnología, seguro que dará buen resultado.

Y si nos metemos a innovar más, evolucionaremos de tal manera que tendremos que hacer más departamentos: en ciberseguridad, en vigilancia de fronteras, en la parte financiera, en compra pública, etc. Este trabajo se complica más, ahora mismo en el Servicio de Innovación Tecnológica hay seis personas, conmigo siete; y algunas más nos vendrían bien, porque el trabajo va en aumento.

Dentro de Guardia Civil ¿quién se ha apuntado al carro de la innovación? Estas Unidades que nos ayudan mucho:

- La Jefatura Fiscal y Fronteras, muy activa, tiene la responsabilidad de temas marítimos.
- Servicio de Costas y Fronteras.
- Servicio Marítimo.
- Servicio Fiscal.
- La jefatura de Policía Judicial.

- UCO – con su equipo tecnológico de realizar seguimientos, escuchas, etc.
- Unidad Técnica de Policía Judicial.
- Servicio de Criminalística.
- La Jefatura de Unidades Especial y de Reserva.
- Servicio Aéreo.
- Explosivos y Defensa NBRQ, que en los últimos años está volviendo muy activo en proyectos.
- Servicio de Montaña.
- Agrupación de Reserva y Seguridad, realiza las mismas funciones que las UIPS.
- Unidad de Acción rural, está en Logroño y en los últimos años se ha vuelto muy activa en proyectos.
- Jefatura de Servicios Técnicos, a la que pertenezco tanto en informática como en telecomunicaciones, también está participando.
- Servicio de Informática.
- Servicio de Telecomunicaciones.
- Servicio de Innovación Tecnológica.
- Cecor-Vigmar.
- Centro de Análisis y Prospectiva, depende directamente de la Guardia Civil.
- UEI Unidad Especial de Intervención, similar a los GEOS.
- SEPRONA, Servicio Protección de la Naturaleza, en este tema tenemos que implicarnos mucho más.
- Jefatura de Información, también muy activa en estos campos.

Con todos ellos, nos relacionamos haciendo de distribuidor de juego, de ventanilla única hacia adentro y hacia afuera. Como decía antes, no podemos permitir que una Unidad de Guardia Civil sea competidora de otra Guardia Civil.

Hacemos Ventanilla única, contactamos con otras Unidades, les reiteramos que aunque son libres de gestionar con contactos, con "proveedores", con otras empresas; tienen que comentarlo. Porque somos muchos en Guardia Civil y tenemos que estar coordinados. Y si salimos al extranjero y descubrimos tecnologías novedosas, también se lo comunicamos a ellos. También nos ofrecemos para ayudarles en la parte administrativa financiera que es la más penosa; teníamos una persona ahora hay dos. Y es lo que a las Unidades les echa para atrás, los trámites administrativos; todo esto ahora se está centralizando y si las unidades saben que todos esos papeleos se los podemos hacer, ellos solo ponen su conocimiento en este ámbito de las telecomunicaciones marinas y nosotros hacemos los trámites administrativos; aunque nos suponga mucho trabajo, nos aseguramos de que esas unidades se lancen a la innovación tecnológica.

BÚSQUEDA DE FINANCIACIÓN

Cuando tenemos una Unidad que quiere algo, la ayudamos a buscar esa financiación; podemos ir a los fondos estatales, en los Presupuestos Generales del Estado tenemos una mínima parte y, a veces, se soluciona con eso.

En nuestra Jefatura de Servicios Técnicos, casi todos los días vienen a ver a los de informática, a innovación tecnológica, universidades ofreciendo enseñanza y, también, nos visitan unidades nuestras. Buscamos la financiación donde podemos, si hay dificultades en los fondos estatales, recurrimos a los

fondos europeos, el programa marco H2020, el futuro Horizonte Europa… el FP9 donde seguramente encontraremos una solución a la necesidad que nos solicitan. Si la necesidad es imperiosa, tenemos que buscar algo que está en el mercado, no podemos irnos al programa H2020, no podemos ir a buscar fondos de I+D+i, probamos con fondos de seguridad para ayudar, sino recurrimos a los fondos Feder o hablamos con Frontex.

Siempre es interesante saber que todo esto está disponible para satisfacer nuestras necesidades tecnológicas. Ahora mismo, en I+D+i, podemos ir a la página oficial de la Unión Europea, portal del participante y ahí tenemos todas las líneas de financiación que nos pueden ayudar en nuestra tarea. Donde más dinero tenemos para financiarnos es en H2020, principalmente; nosotros, como Guardia Civil, nos metemos en propuestas que se pueden materializar en un proyecto o no, en la temática Sociedades Seguras, con casi mil setecientos millones de euros (1.700M); pero no solo nos apuntamos a proyectos de esta temática, nos hemos presentado a Espacio. En Espacio hay dos programas con mucha proyección de futuro como son: Galileo, tema de geoposicionamiento; y Copernicus, programa de observación de la tierra con toda la red de satélites europeos que están en el espacio. También nos presentamos a proyectos de ICT, nos podemos presentar, aunque nuestra área favorita son Sociedades Seguras. En el Reto Social 6, también podemos presentarnos. De momento, no tenemos ningún proyecto, pero la Unión Europea lo ha definido como Focus Área de Seguridad.

Prácticamente son esos tres:

- Sociedades Seguras.
  - Protección infraestructuras críticas.
  - Resiliencia al desastre (Seguridad).
  - Lucha contra el Terrorismo/crimen (Seguridad).
  - Seguridad de fronteras y exterior (Seguridad).
  - Asuntos Generales (Seguridad).
  - Seguridad digital.

- Espacio.
  - Geoposicionamiento.
  - Observación de la tierra.

- Tecnologías de la información y las comunicaciones (Tic).

Estas son las tres áreas en las que ahora mismo nos movemos, sobre todo en Sociedades Seguras.

Las siguientes imágenes abarcan el programa 2018-2020. El programa 2018 se abrió en marzo y lo cerramos dentro de un mes y medio para presentar propuestas. En el programa 2019, hubo una enmienda porque nos desapareció un *topics* de fronteras por duplicidad, del que ya se encarga Frontex. Tenemos un sitio donde ir si hay una necesidad que la jefatura de Fronteras o el Servicio Marítimo requiera de esos fondos.

En la de DRS con sus acciones, sus *topics*, y sus *subtopics*, no nos presentábamos mucho pero últimamente sí, luego veremos los proyectos para los que estamos consiguiendo financiación.

Lucha contra el crimen y terrorismo, por lo visto es nuestro fuerte, donde más proyectos tenemos. Al igual que Seguridad de Fronteras y Exterior, donde nuestra Jefatura es muy activa en estos fondos de H2020 y en otros. Y en Asuntos Generales también, en este año estamos preparando propuestas y también tenemos propuestas de años anteriores.

En Seguridad Digital, estos temas también están a la orden del día. De hecho, en estos días, la mitad de mis compañeros de la Jefatura están en Santander en un curso de verano que versa sobre ciberseguridad. Defensa de los estados democráticos desde el punto de vista de la ciberdefensa, de la ciberseguridad.

Cuando una unidad nuestra se quiere presentar ya tenemos un consorcio y hacemos la propuesta, el *topic*, ¿cómo colaboramos nosotros en el ciclo de la innovación? Ese *topic*, desde el comité de programas, en el grupo del que formamos parte, puede ayudar de alguna manera, a definir el programa de trabajo. Se elevan a la Comisión Europea las ideas, necesidades, que tenemos en Guardia Civil, aportamos nuestro granito de arena, no modelamos el programa de trabajo, pero sí podemos influir en escribirlo, definir esos *topics*; los podemos defender. Para el año que viene, necesito que salga un *topic* en esta línea porque hay una unidad muy interesada.

Al escribir esa propuesta buscamos socios y si coordináramos la propuesta la tendríamos que escribir, tenemos que hacer una labor ardua de coordinación y de poner en común a muchos socios; igualmente tenemos que especificar qué parte del presupuesto necesitamos, hasta dónde nos vamos a implicar, qué cantidad de horas voy a trabajar en este proyecto. Luego, en el proyecto, tenemos que hacer tareas técnicas; las unidades que se van a implicar, son unidades operativas técnicas y son las que tienen que decir los requisitos del proyecto porque son los que lo tienen que defender.

Es posible que nuestra idea a lo largo de uno, dos o tres proyectos, acabe en la compra pública innovadora y eso es beneficioso, porque lo que quiere decir es que: de una idea que teníamos hace cinco años, prototipo y con unos niveles de desarrollo bajos, hemos podido ayudar a que ese prototipo esté casi en el mercado y al final tenemos un producto que vamos a comprar, que se ha puesto en el mercado y al que hemos ayudado a desarrollar, a que me salga más barato, en cuanto que me van a financiar parte de esa compra. Porque no será lo mismo que ir ahora al mercado y pagar el 100% por un producto; si nos hemos implicado en desarrollarlo, en definirlo en cómo lo queremos, desde Europa nos van a ayudar a comprarlo.

Por eso, ¿en qué roles podemos participar en un proyecto? Como *adviser role*, rol de asesor, no tengo presupuesto, solo asesoro a un socio; y como socio y porque tengo una parte del presupuesto, tengo que implicarme más, soy coordinador y mi implicación es mayor. Si nos ponemos a coordinar nos va a llevar casi el 100% del tiempo. También estamos como expertos en ese comité de programas, desde otro punto de vista.

PREPARACIÓN DE UNA PROPUESTA H2020

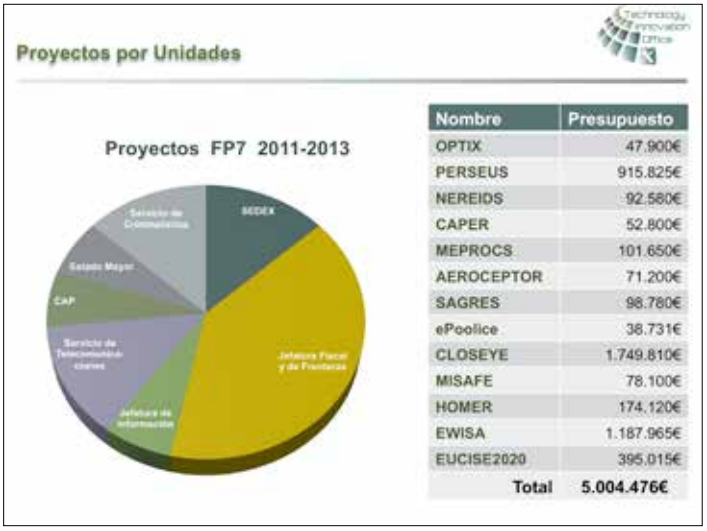
Las propuestas que vamos a presentar en H2020, la forma de inicio a través de las unidades de Guardia Civil que van a participar en una propuesta, tienen los socios con los que quieren ir o sino, en las reuniones a las que asistimos, hacemos contactos; y hay empresas, universidades, centros tecnológicos que nos exponen cuáles son sus intereses para colaborar con nosotros y, después, dentro de la institución, quién puede colaborar con esos organismos externos.

Esa imagen superior fue de la reunión Seren 3, celebrada en marzo del año 2017 en Bruselas, a la que asistí junto con el Inspector Chavo, como expertos. Estuvimos dos días defendiendo la posición española y estableciendo contactos con el resto de Europa.

Y, todo este trabajo que hemos tratado de contar en esta ponencia, en los últimos años se ha traducido en proyectos, ya terminados muchos, otros en marcha y otros que se tienen que iniciar.

PROYECTOS POR UNIDADES
Proyectos FP7 2001-2013

Del programa marco FP7, Closeye fue coordinado por Guardia Civil, por la Jefatura Fiscal y Fronteras, se tuvo que hacer una encomienda de gestión con Isdefe y terminó con éxito, es de vigilancia marítima y concluyó con una compra pública innovadora; productos que se probaron en el ámbito marítimo terminaron en el mercado.



Nombre	Presupuesto
OPTIX	47.900€
PERSEUS	915.825€
NEREIDS	92.580€
CAPER	52.800€
MEPROCS	101.650€
AEROCEPTOR	71.200€
SAGRES	98.780€
ePoolice	38.731€
CLOSEYE	1.749.810€
MISAFE	78.100€
HOMER	174.120€
EWISA	1.187.965€
EUCISE2020	395.015€
Total	5.004.476€

En la convocatoria H2020, solo pudimos obtener financiación para tres propuestas; tres terminaron el proyecto, todas de FCT, lucha contra el Crimen y Terrorismo. La más activa fue la Jefatura de Información con casi más de la mitad de la aportación en euros, con su proyecto *Law-Train*, y que ha finalizado hace dos meses. El Consorcio y la Comisión tenían interés en seguir con *Law-Train2*, gracias al nivel de desarrollo al que se ha llegado. Con realidad virtual se ha hecho un demostrador, que es un videojuego, que usa realidad virtual para hacer interrogatorios a sospechosos de terrorismo o de tráfico de drogas. Se ha hecho un demostrador informático y hay interés en seguir una segunda parte del proyecto.

En el año 2015, nos llevamos cinco; *Broadmap*, con Policía Nacional, y en los que se definieron unos requisitos en una segunda parte *Broadway*. Ahí, no solo nos centramos en FCT sino que nos abrimos a Fronteras, a DRS. La Jefatura de información se llevó gran parte de la financiación. En el año 2016, se llevó cuatro proyectos en los que estuvo muy activo el CAP de la Guardia Civil, Centro de Análisis y Prospectiva. Tres fueron de FCT y uno fue de fronteras. Este año nos hemos llevado seis en la última, ha sido la más exitosa y muy repartida: dos de DRS, dos de asuntos generales, uno de crimen y terrorismo; y uno de fronteras. El CUPS se ha llevado casi la mitad con dos proyectos: Copkit y Medea.

PARTICIPACIÓN EN OTRAS INICIATIVAS DE FINANCIACIÓN

Otras fuentes de financiación H2020 Espacio son, por ejemplo, el proyecto Marine-EO 2016; la Easme que es la Agencia ejecutiva para la pequeña y mediana empresa, y que tiene unos fondos EMFF europeos, marítimos y de fronteras.

También, tenemos proyectos no solo de vigilancia, sino también de comunicaciones. La Jefatura Central y Fronteras ha sido muy activa en estos fondos y ha conseguido toda esa financiación.

CONCLUSIONES

Para terminar unas breves conclusiones, desde nuestro punto de vista:

- Proyecto Innovador de interés del Servicio de Innovación Tecnológica. Dentro de Guardia Civil, todo lo que es innovador, es de nuestro interés.

- Promoción, uso nuevas tecnologías en la Institución. Porque nuestra labor es promocionar el uso de las nuevas tecnologías en todas nuestras unidades.

- Búsqueda de soluciones a los problemas y necesidades tecnológicos internas (Unidades G.C.). Si alguien tiene una necesidad específica, puede acudir a nosotros y plantearnos qué es lo que necesita.

- Punto de contacto ágil. Unidades Guardia Civil ↔ Organismos externos. Somos un punto ágil porque tenemos muchos correos al día, porque queda un mes y medio para cerrar la convocatoria y donde llevábamos diez propuestas, parece que vamos a hacer quince, en este último mes.

- Posicionar la Institución en Europa. A largo plazo vamos a conseguir posicionarnos, ganar prestigio en Europa,y de alguna manera influir en el futuro, no solo de nuestra institución, sino de la sociedad europea.

LA ACCIÓN PREPARATORIA Y EL FUTURO PROGRAMA EUROPEO DE INVESTIGACIÓN EN DEFENSA (EDRP)

JOSÉ RAMÓN SALA TRIGUEROS
Jefe de Área de Cooperación Internacional de la I+D de la Subdirección de Planificación, Tecnología e Innovación de la Dirección General de Armamento y Material.

INTRODUCCIÓN

Trabajo en la Dirección General de Armamento y Material, es la gran dirección del Ministerio de Defensa que tiene muchas funciones, entre otras la de conseguir los equipos y sistemas para las Fuerzas Armadas. En concreto estoy en el Área de Cooperación Internacional en I+D+i.

He dividido la presentación en tres partes, como sabemos las Fuerzas y Cuerpos de Seguridad del Estado participan en los programas marco, en Horizonte 2020, en diversos programas de I+D+i seguridad; la idea es hablar hoy, de la iniciativa paralela que se está realizando en el ámbito de la defensa y, por primera vez, en el marco de la Comisión Europea. Por eso, hablaremos de la acción preparatoria de investigación en defensa, la unidad PADR, que es como saben una preparación del futuro de un gran programa de investigación. Previamente, es interesante que conozcan la organización que tenemos de I+D en el Ministerio de Defensa y, en concreto, nuestra Subdirección General de Planificación, Tecnología e Innovación. Finalmente unas conclusiones que pueden dar pie a la mesa redonda posterior.

Empezando con la presentación y lo que es nuestra Subdirección General, siempre solemos poner el organigrama adjunto donde se señala que: del Ministerio de Defensa, de la Ministra, depende la Secretaría de Estado de Defensa, y de ahí la Dirección General de Armamento y Material.

Como decía, tiene diversas direcciones, por ejemplo, la Dirección de Gestión de Programas que lleva todos los grandes programas: helicóptero tigre, helicóptero NH90, las nuevas fragatas F110, programas de comunicaciones

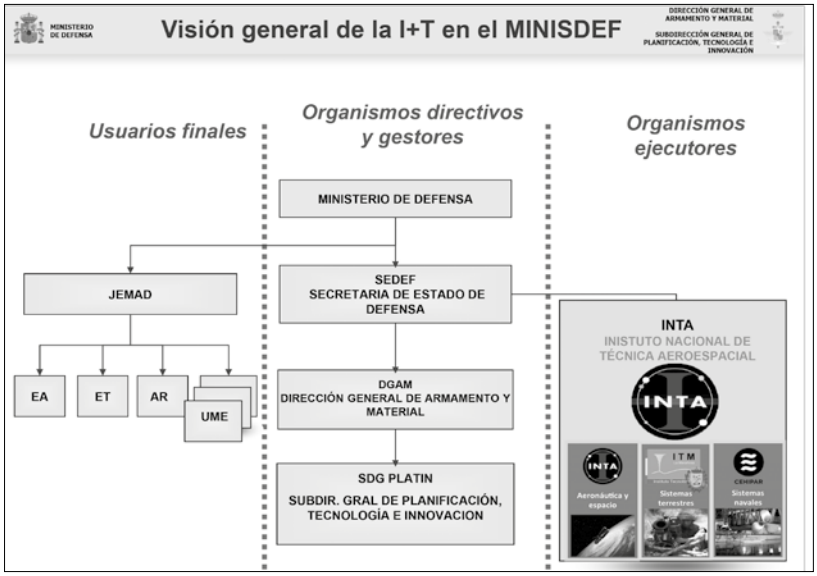


Imagen 1

por satélite, etc. Por nuestra parte, la Subdirección general de Planificación Tecnología e Innovación, se supone que debemos lanzar programas en diferentes ámbitos de investigación para dar servicio a esos sistemas que se desarrollarán, se fabricarán en serie, se probarán y entrarán en servicio. Solemos indicar la estructura de las Fuerzas Armadas, Jemad, Jefe mayor de la Defensa del cual dependen el Ejército del Aire, el Ejército de Tierra, la Armada y la Unidad Militar de Emergencia, porque en nuestro caso todos en la DGAM trabajamos para ellos. Esa distinción para conseguir, de alguna manera, una capacidad y que ellos tengan los sistemas que necesitan dentro de unos años, a diferentes plazos, es importante; no trabajamos para fomentar la industria de Defensa o para mantener puestos de trabajo, por supuesto es importante, pero nuestro primer cliente son lógicamente las Fuerzas Armadas.

Finalmente, como tenemos nuestros propios laboratorios que ejecutan programas y actividades de I+D, en concreto, el Instituto Nacional de Técnica Aeroespacial, hace algunos años aglutinó a todos los centros de investigación que tenía el Ministerio de Defensa: el polígono de experiencias de Carabanchel, el centro de ensayos de Torregorda (CET) en Cádiz, que estaba en el Instituto Tecnológico La Marañosa (ITM) y la parte de experiencias y hidrodinámicas para la Armada, probar modelos de buques a escala que está en el Pardo, el Cehipar; todo se integró en lo que llamamos coloquialmente el nuevo INTA. Ellos son un brazo ejecutor con muchos técnicos, científicos, ingenieros de los ejércitos que ejecutan programas. Nosotros seríamos organismos directivos y gestores, y a su vez como ahora veremos, contratamos también nuestros programas de investigación.

SDGPLATIN: QUÉ HACEMOS

Lo importante de nuestra Subdirección es:

- La planificación y programación de los recursos de I+D+i y de AM.

- El seguimiento y control de los programas de I+D contratados.

- La coordinación de la participación nacional en actividades de organizaciones internacionales de I+D de defensa: EDA, La Agencia Europea de Defensa; STO Organización de ciencia y tecnología de la OTAN, son foros de expertos agrupados en paneles con muchas actividades anuales y que investigan muchos ámbitos.

- La coordinación de la participación nacional en las actividades de I+D+i de la UE, en colaboración con los organismos nacionales responsables. En concreto, somos el punto de contacto nacional-PoC, para la participación de ciertas unidades, o iniciativas duales del H2020; de la Acción Preparatoria en Investigación de Defensa y del futuro Programa Europeo de Investigación en Defensa; que como decía antes, por primera vez hay dinero en la Unión Europea para investigación en Defensa, ahora la Comisión Europea ha decidido invertir en Defensa y así está empezando este programa; y nosotros somos el contacto del Ministerio de Defensa para, en caso necesario, canalizar la participación de usuarios finales del propio Ministerio.

- Los acuerdos internacionales con países, como por ejemplo con Estados Unidos, siempre insisto, en el ámbito de Defensa, y

- La Vigilancia y asesoramiento tecnológico e identificación de las capacidades tecnológicas de defensa del tejido industrial y de investigación nacional (SOPT – Sistema de Observación y Prospectiva Tecnológica).

La imagen siguiente (Imagen 2), resume las actividades de las que estamos hablando, tenemos un ámbito nacional en el cual contratamos a empresas o universidades, entidades nacionales con dinero del Ministerio de Defensa, hacemos contratos; coordinamos o estamos en contacto con el INTA, como gran ejecutor de programas, siempre bajo la dirección del Sedef y, finalmente, tenemos esos ámbitos internacionales. El de Unión Europea es el que va a centrar mi presentación.

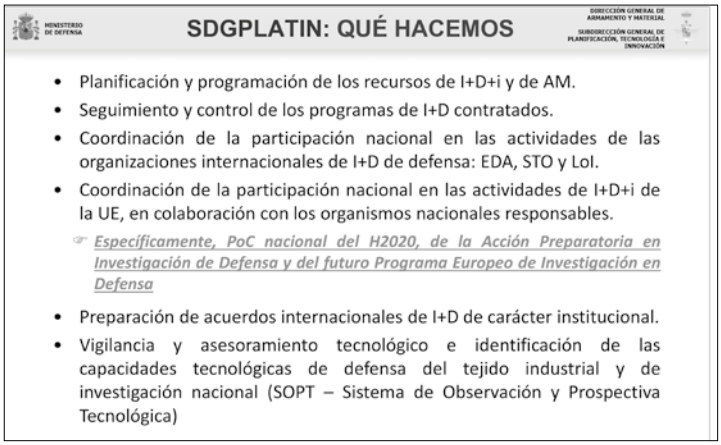


Imagen 2

Dentro del espacio europeo siempre, en el ámbito en que más hemos trabajado, es el de la Agencia Europea de Defensa que está en Bruselas EDA, la LOI es la asociación de seis países con más industria de defensa en Europa, entre los que está España, es un club cerrado a esos países y luego está el nuevo ámbito de la Unión Europea. Finalmente, tenemos la STO de la OTAN un ámbito muy interesante donde participan Estados Unidos, Canadá, Turquía y una serie de países europeos, y finalmente los tratados bilaterales.

SDGPLATIN: CONTACTO

En nuestra página web pueden encontrar lo que hacemos, los programas, iniciativas y noticias de interés para la investigación en Defensa.

- Portal de Tecnología e Innovación del Ministerio de Defensa: www.tecnologiaeinnovacion.defensa.gob.es

- Publicaciones:
  - Boletín de Observación Tecnológica en Defensa (trimestral).
  - Monografías.

- Contacto:
  - Para consultas relacionadas con cooperación internacional en I+D: cooperacionid@mde.es
  - Para contactar con el Sistema de Observación y Prospectiva Tecnológica: observatecno@oc.mde.es

Comentar, como punto interesante a estos efectos, que el Sexto Congreso internacional I+D en Defensa, se celebrará en noviembre de este año 2018 en la academia de caballería de Valladolid.

Imagen 3

GESTION DE PROGRAMAS

Los tipos de programas que hacemos, son los que contratamos en nuestra Subdirección General, y pueden ser programas nacionales que se contratan como Negociados sin publicidad, con determinadas empresas, que llamamos desarrollo nacional. Otros programas multinacionales en los cuales participamos como MIDS o Coalwnw, con otros países, se hacen con un acuerdo específico y cada país paga a su industria participante.

Tenemos,también, el ámbito de la EDA donde se lanzan programas con los países de la EDA que quieran participar en investigación.Y un concurso que publica el Ministerio de Defensa, al que llamamos programa coincidente, que se publica cada varios años y en el cual se hace una convocatoria para recibir propuestas de proyectos de investigación. Está dirigido sobre todo a Pymes, universidades, centros tecnológicos, no tanto a grandes empresas; y se invita a que presenten propuestas sobre una serie de temáticas; y se seleccionan igual que se haría en Horizonte 2020; se evalúan las propuestas recibidas y seleccionan las que puedan ser de interés.

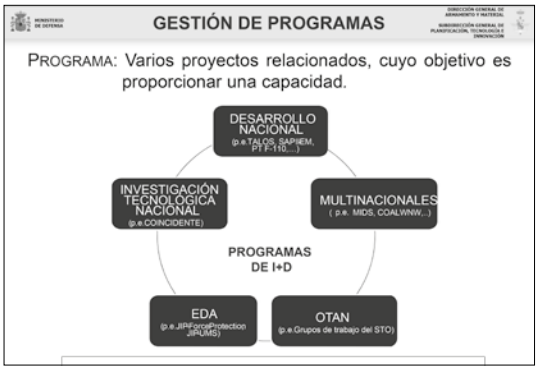


Imagen 4

Imagen 5

EJEMPLOS ANTERIORES COINCIDENTES

Una mención de la anterior convocatoria coincidente que puede ser de interés para fuerzas de seguridad, son los programas más pequeños, dirigidos a universidades:

- "Fusión de Información y explotación inteligente de datos en redes de sensores" (Finesens): fusión de datos de alto nivel. Se hizo un demostrador para vigilancia de un nudo de carreteras con información de diversas fuentes heterogéneas. La aplicación concreta era un nudo de carreteras pero esa fusión se podría aplicar a muchos ámbitos, porque la Universidad de Granada que hizo esto, trabajó mucho el tema de las deontologías. Policía y Guardia Civil seguro que trabajan mucho en fusión de datos, es un tema interesante, y nosotros hablamos con la universidad para presentárselo a Fuerzas de Seguridad por si tenían interés o les podía servir algún desarrollo adicional.

- "*Indoor and Tactical Purpose mini UAV"* (Indotac): Mini UAV para interiores. Sistema de navegación alternativo en zonas urbanas. Este mini UAV de dos kilos para que pueda operar en interiores, tiene un sistema de comunicación novedoso, por motas de comunicación, que permiten si entras por una nave, ya no pasan las comunicaciones, las ondas. Tenía el añadido de un sistema en situaciones de denegación de señal por satélite, mediante un despliegue de balizas *ad hoc* en una zona urbana, de combate; puedes tener un posicionamiento de tu vehículo, pero la clave está en la parte del *timing* que debe ser muy preciso en la medida del tiempo entre las balizas.

- *Drive-By-Wire* para el teleguiado de vehículos convencionales en misión de prospección anticipada del terreno y conducción preprogramada a través de *waypoints* (Remote Drive). Se aplicó a un vehículo multipropósito de las Fuerzas Armadas, Vamtac, y se hizo un demostrador de conducción remota que fue considerado de interés por los operadores, para evitar peligros personales por ejemplo en el caso de que haya dispositivos explosivos en la zona de operación.

  Este es otro programa que se aplicó a un vehículo Vamtac, para dotarle de tracción hibrida eléctrica. Los elementos básicos se han desarrollado en ámbitos de investigación civil pero la innovación consiste en aplicarlos a un sistema militare. Es decir, realmente no es novedoso hacer una tracción hibrida eléctrica pero aplicarlo a un Vamtac y estudiar todo el balance de combustible "desde el pozo hasta la rueda del vehículo", comprobar si realmente se ahorra, dado que tiene más eficiencia el sistema eléctrico al

operar el motor térmico en un punto cercano al óptimo es de gran utilidad; por ejemplo, en una base en Afganistán necesitar menos combustible es vital porque llevar el combustible allí es muy peligroso y cuesta mucho.

CONVOCATORIA COINCIDENTE 2018

Para que vean las áreas que menciona el Ministerio de Defensa, la nueva convocatoria del programa Coincidente, las temáticas del BOE de 26 de junio, son las siguientes:

- Armas de energía dirigida mediante láser de alta potencia, la Comisión está trabajando en ello.
- Tecnologías aplicables al guiado de municiones.
- Robótica aplicada a misiones militares, sobre todo sistemas terrestres es donde la robótica es todavía más difícil que en los sistemas aéreos.
- Detección y neutralización de IED en entornos terrestres y navales.
- Tecnologías para la mejora de los sistemas de protección pasiva del combatiente y de las plataformas militares (chalecos, etc.).
- Alerta y protección frente a amenazas NRBQ aplicadas a misiones militares.
- Sistemas inteligentes de análisis y explotación de información aplicado a la resolución de problemas militares -tema muy dual en el cual las Fuerzas Armadas están muy interesadas incluso en el análisis de fuentes abiertas de noticias falsas-.
- CIBER -Soluciones innovadoras en ciberdefensa-.

ESQUEMA FONDO EUROPEO DE DEFENSA

Estos programas coincidentes que he mencionado, pueden tener una financiación, dependiendo de si es una PYME o una Universidad, se financia más que si fuese una gran empresa; a lo mejor es un programa de trescientos mil (300.000) euros, doscientos mil (200.000), pero se financian más. Otros programas en el ámbito de la EDA pueden llegar a ochocientos mil (800.000) euros, o un millón, pero generalmente de ahí no pasamos salvo los programas tecnológicos de la nueva fragata, la F110, para que se hagan una idea de la magnitud de programas que lanzamos.

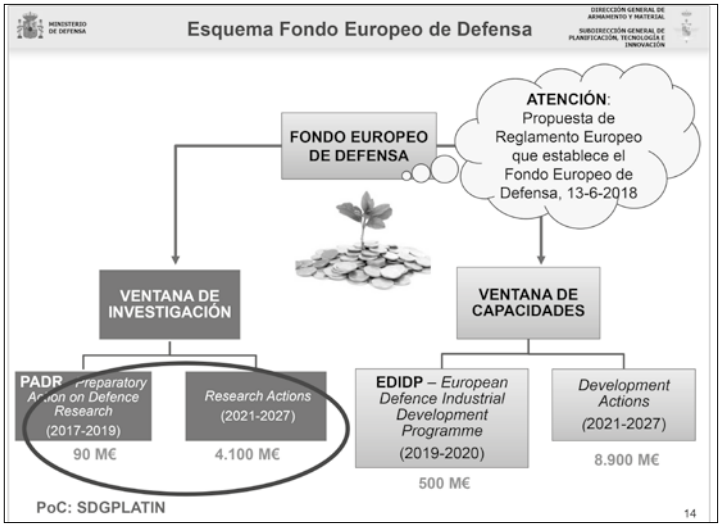


Imagen 6

VENTANA DE INVESTIGACIÓN

Acción Preparatoria sobre Investigación en Defensa (PADR).

228 Como saben, en Europa ha habido un cambio de mentalidad y se necesita invertir en Defensa. La Comisión Europea, que es la que tiene el dinero, necesita invertir en defensa porque todo el mundo está diciendo que Europa no hace lo suficiente; por otra parte, la industria de defensa europea está quedando desmantelada porque no hay programas importantes.

La Comisión Europea decidió actuar venciendo las reticencias de determinados ámbitos o corrientes políticas que recomendaban no gastar en temas puramente de defensa. El Fondo Europeo de Defensa, lo hemos estado presentando durante los dos últimos años, pero la diferencia con lo que os presento hoy aquí es que ya hay una propuesta del reglamento europeo, muy reciente que, de alguna manera, aunque falta todavía mucho para que se apruebe, se discutirá en el Parlamento Europeo, en el Consejo Europeo, pero ya sistematiza lo que será el Fondo Europeo de Defensa y, básicamente, quizá sea diferente con lo que se hace en Horizonte 2020.

Tiene una ventana de investigación dedicada a investigación y tecnología y una ventana de capacidades; donde la idea es conseguir realmente un nuevo caza europeo, un nuevo vehículo blindado, un nuevo tanque..., sistemas que ya se fabriquen, se desarrollen y se certifiquen; con lo cual, eso es lo que se llama ventana de capacidades y, de esa manera, conseguiríamos pasar del papel o de pequeños prototipos a algo que le sirva realmente a las Fuerzas Armadas. La ventana de investigación, a su vez, ha tenido la acción

preparatoria, que está ya en marcha, con un carácter de inversión limitada y después vendrá el futuro programa de investigación que es parte del título de esta ponencia.

El orden de magnitud de lo que se está hablando, del que habla el reglamento es el siguiente: la actual acción preparatoria tiene noventa (90M) millones, pero el futuro programa de investigación tendrá probablemente unos quinientos ochenta millones (580M) anuales y aunque es para toda Europa, eso es mucho para los órdenes de magnitud de inversión que hay en el mundo de la defensa; hay esperanzas de que se dé un vuelco a la investigación en defensa y se obtengan capacidades porque, a su vez, en la ventana de capacidades, el *Development Actions* tendrá ocho mil novecientos millones (8.900M) que habrá que definir en su momento.

De acuerdo con este esquema voy a comentar lo que se está haciendo ahora en la ventana de investigación, que consta de las dos partes que he mencionado: la acción preparatoria que no está en marcha todavía, no se ha aprobado el presupuesto de 2019, pero se aprobará; y luego los objetivos de esta acción preparatoria. Igual que en su día hubo acción preparatoria en los programas marco y, precisamente, en el caso de investigación de Defensa con más motivo; porque nunca se ha hecho ver los problemas que surgen cuando dedicas dinero en la Comisión Europea en colaboración a I+D de Defensa. Si sale bien, se seguirá con el siguiente programa global; por eso, es fundamental que tenga resultados positivos en cuanto que fomentará la cooperación y preparará el lanzamiento de ese programa entre el año 2021 y 2027; gran programa específico de Defensa.

SISTEMAS NO TRIPULADOS DEMOSTRADOR TECNOLÓGICO PARA CONCIENCIA SITUACIONAL MEJORADA EN ENTORNO NAVAL

Les comento brevemente lo que ha ocurrido en la convocatoria del año 2017, usando información pública de la Comisión Europea. Esta convocatoria salió en julio del año 2017 y el 5 de octubre, acababa el plazo para presentar propuestas. Básicamente había tres áreas.

El programa más importante, que convocó la Comisión Europea era el hacer un demostrador tecnológico en el entorno naval, se lleva una gran parte del presupuesto de la acción preparatoria, cinco millones (5M) de euros y se trata de hacer maniobras reales con armadas de distintos países. Que se vean cosas, que los políticos europeos puedan ver que esto tiene resultados positivos, que se transmite información, que los sistemas funcionan...,

sobre todo sistemas no tripulados, tanto aéreos como navales, submarinos, etc. El consorcio ganador, el Ocean2020, tiene un número de entidades realmente impresionante, cuarenta y dos entidades de quince Estados miembros, incluyendo armadas de distintos países, Ministerio de Defensa, etc.

En ese consorcio hay varias empresas españolas bien posicionadas, incluyendo una PYME que hace un vehículo submarino el SeaDrone; y como novedad, el Ministerio de Defensa participa como miembro del consorcio. Tenemos poca experiencia en estas participaciones, a pesar del séptimo Programa Marco de la participación de la Armada; pero esto, para nosotros, es una novedad. También participará como miembro del consorcio, personal de nuestra Dirección General y personal de la propia Armada. Se prevé hacer dos grandes maniobras, una en el Mediterráneo y otra en el Mar Báltico demostrando cómo se mejora la conciencia situacional con sistemas no tripulados.

PROTECCIÓN DE LA FUERZA Y SISTEMAS AVANZADOS DEL SOLDADO

En la convocatoria de protección de la fuerza y sistemas avanzados del soldado, había tres *subtopics*. En el Ministerio de Defensa hay un *topic* que es el combatiente futuro, en esa línea se hizo:

A) Arquitectura abierta genérica de sistemas de soldado, comunicaciones, control de su confort, etc. El consorcio ganador, Gossra también lleva empresas españolas, pero ahí, el personal del ejército de tierra y de la DGAM, participan con equipo consultivo.

B) Protección balística y CBRN, ha ganado un consorcio: Vestlife coordinado por Aitex, único programa que está coordinado por una entidad española.

C) Camuflaje adaptativo. Nuevos métodos novedosos que, de alguna manera, hagan invisible al soldado a diversos sensores. En el consorcio ganador no hay participantes españoles.

PROSPECTIVA TECNOLÓGICA ESTRATÉGICA (CSA)

Algo muy importante en la convocatoria del año 2017, una llamada de prospectiva tecnológica, importante a efectos de ver qué tecnologías de defensa habría que trabajar en el ámbito de la Comisión Europea. Lo ganó un consorcio liderado por una ingeniería italiana, no hay ningún participante español.

LECCIONES APRENDIDAS

1. Gran interés por parte de las entidades españolas en participar en la PADR:

   - Retorno para España 2017: 12,5%. La aportación de España al presupuesto de la Unión Europea 2017, es el 8,46%.
   - En total hubo veinticuatro propuestas presentadas a los tres *topics*, con ciento ochenta y seis (186) entidades europeas integrando esos veinticuatro consorcios. Porcentaje de éxito: 33% en DT, 18% en FP y 33% en STF.
   - España, tercer país con mayor número de entidades en los consorcios presentados a las tres convocatorias.
   - Apuesta de futuro por experiencia adquirida de cara al futuro EDRP.

2. Importante, preparar los consorcios, y después las propuestas con tiempo.

   - No hay que esperar a las convocatorias. La Comisión Europea, transmite información con anterioridad -el programa de trabajo se publica antes, aunque en 2018 ha habido una diferencia de solo unos días-.
   - Evitar el trabajo a última hora -impacta en la calidad de la propuesta y dificulta la participación de usuarios finales-.

3. Usuarios finales:

   - Es posible la participación de unidades de las FAS en las propuestas, tanto como asesores "advisory board" como socios del consorcio.
   - Sdgplatin canaliza solicitudes de participación.
   - Importante para las entidades: dirigir solicitudes de participación con la suficiente antelación. Deben ser propuestas de interés para los ejércitos, la armada o cualquier otro usuario implicado. Es decir, las solicitudes se dirigen a nosotros y nosotros las canalizamos.

4. Coordinación participación nacional:

   - Muchas de las entidades participantes en las convocatorias del año 2017 han informado a Platin de dicha participación.
   - Conocer esta información facilita al MDEF realizar una labor de coordinación en caso necesario. Se recomienda informar de la participación incluso una vez cerrada la convocatoria.
   - Pueden contactar con nosotros en cooperacionid@mde.es

5. Evaluadores: también les damos difusión, hay un cambio con respecto a H2020 y es que los evaluadores que se inscriben en la base de datos que selecciona la Agencia Europea de Defensa, que es quien gestiona la acción preparatoria en nombre de la Comisión Europea, tienen que estar validados; les tenemos que dar una carta, aparte de tener habilitación de seguridad, que hay poca gente que lo tenga; nosotros los validamos, nos mandan el currículum, etc. Así se ha puesto en esta iniciativa para evitar que entre, en temas sensibles de Defensa, personal que aunque tenga la habilitación de seguridad, no se pueden tener otras implicaciones. Todo esto hace que sea difícil encontrar expertos para evaluar este tipo de convocatorias.

   - Ha habido una serie de candidatos validados por la Sdgplatin para la bolsa de evaluadores de la EDA.
   - También ha habido evaluadores inscritos pero que no han solicitado validación a la Sdgplatin -rechazados por la EDA-.
   - Dificultades por necesidad de habilitación EU Secret, conflictos de intereses y balance geográfico.
   - La EDA indica que es difícil encontrar expertos en determinadas áreas técnicas y que cumplan el resto de requisitos. Seguir impulsando en próximas convocatorias la presencia de evaluadores españoles.

Página de la EDA:
https://www.eda.europa.eu/docs/default-source/procurement/padr-call-forindependent-experts.pdf

CONVOCATORIAS DE 2018

En las convocatorias del año 2018 hay *topics* que serán clasificados, luego el evaluador tiene que ser secreto, porque hay *topics* que van a ser de clasificación: Secreto Unión Europea. La convocatoria que está ahora en curso, que terminó el 28 de junio, tiene de nuevo tres *topics*

- PADR-EDT-02-2018: European high-performance, trustable (re)configurable system-on-a-chip or system-in package for defence applications. (Hasta 12 M€).

- Sistemas en *chip gate array* -matriz de puertas- programables en campo que se llama FPGA, que es una carencia que tiene Europa depende de sistemas extranjeros para equipos militares, al final necesitan llevar unos chips de dudosa procedencia y seguridad.

- PADR-EF-02-2018: Towards a European high power laser effector. (Hasta 5,4 M€). Es intentar poner las primeras piedras para hacer un arma laser de alta potencia, y finalmente.

- La segunda parte de prospectiva tecnológica. PADR-STF-02-2018: The European Defence Research Runway – part II. (Hasta 1,95 M€)

En la convocatoria de SIP, se buscan sistemas con una gran capacidad de procesado que aguanten temperaturas, condiciones medio ambientales más duras, que otras del mundo civil. Y, finalmente, que las fuentes de suministro sean europeas, o que se pueda restringir la exportación. Aspecto importante para la industria, no se puede exportar un sistema que EEUU se niega a aceptar, otro aspecto también de autonomía importante.

LÍNEAS DE TRABAJO

En las líneas de trabajo, lo importante es esta parte en la cual, probablemente, intervenga el centro Criptológico Nacional. Se trata de que la securización hardware, no solo software, de esos chips permitan su uso y manejar, en el mismo, información secreta. Para lo cual, hace falta seguir las recomendaciones; si hay usuarios finales, en el caso de España sería el Centro Criptológico Nacional.

CONVOCATORIA - EFECTORES

La siguiente convocatoria es la de efectores, llamada así en lugar de armas para el láser de alta potencia. Debido a la falta de fuentes de alta potencia para láseres continuos, no serán pulsados, pues Europa está retrasada con respecto a otros países, EEUU, Rusia, etc. Hace unos días vimos una noticia de un rifle en China que dispara láser y quema objetivos a una cierta distancia. Por lo tanto, no se va a conseguir aquí el arma pero es la primera piedra para llegar a conseguir esa capacidad; para lo cual, se hará un mapa de criticalidad, un road map y, después, se harán una serie de actividades puramente de I+D intentando conseguir esas fuentes láser. Aparte, también se trabajará en los sistemas de apuntamiento desde una posible torreta, pero lo fundamental es la parte del generador del láser.

Algunas entidades españolas han pedido apoyo a usuarios militares -ejército del aire, tierra, etc-. Porque lo dice la convocatoria y para que definan escenarios en los cuales se usaría esa arma. Entonces, ahí va a haber una participación importante de usuarios finales.

CONVOCATORIA
PROSPECTIVA TECNOLÓGICA ESTRATÉGICA

Finalmente, la siguiente convocatoria del tercer *topic*, prospectiva tecnológica, muy centrada en ver qué tecnologías deberían trabajarse o qué fuentes de materiales serían interesantes. Para hacer demostradores se deberían trabajar en Europa para no depender de regulaciones y restricciones, para el tráfico de armas internacionales. Es el aspecto de autonomía el que se busca con el Fondo Europeo de Defensa.

PREVISIÓN CONVOCATORIAS 2019

Para el año que viene se prevé que se convoquen en el año 2019, de acuerdo con la matriz que elaboró la Comisión Europea, por ejemplo, para el tipo de acción TD (Demostrador Tecnológico), CDT (Tecnologías críticas de Defensa), FEDTs (Tecnologías Emergentes) etc. y la matriz indica dónde se hacen las actividades o bien los sistemas no tripulados, el demostrador naval, protección de la fuerza; C4ISR que serían los sistemas de chips o armas como el arma láser.

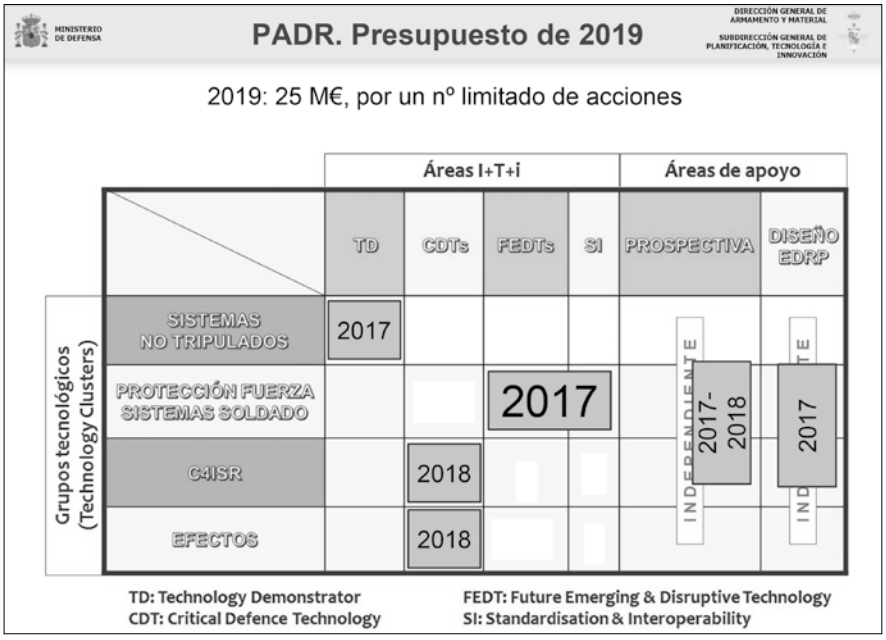


Imagen 7

Finalmente, esta acción preparatoria con las tres convocatorias que he mencionado, su objetivo es el que hablábamos, el futuro programa de cuatro mil millones de euros (4.000 M€) entre 2021 y 2027.

Imagen 8

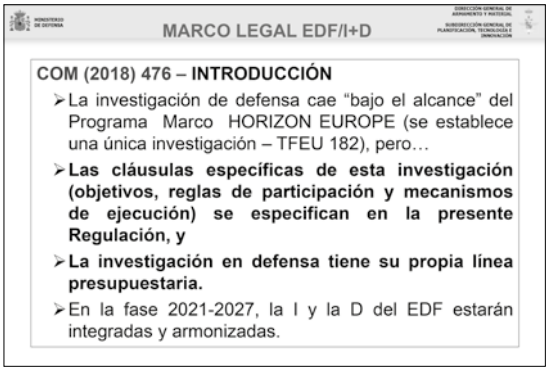


Imagen 9

FONDO EUROPEO DE DEFENSA

Es interesante comparar los puntos principales del reglamento con el Horizon Europe, y las especificidades que se prevén para ese programa de Defensa que se intenta sea lo más parecido a lo que ha sido el Horizonte 2020, en cuanto a muchos aspectos. Las partes específicas que tiene son:

- El Fondo Europeo de Defensa, esa propuesta de reglamento, no habla de un programa de investigación y desarrollo; habla de Development action y Research action. Se menciona que la investigación en defensa cae "bajo el alcance" del Programa Marco Horizon Europe (se establece una única investigación). Nosotros hemos abogado siempre porque estuviera separado de la investigación civil y aunque dice que está bajo el alcance del Marco financiero plurianual, está metido de alguna manera en la investigación global europea.

- Las cláusulas específicas de esta investigación (objetivos, reglas de participación y mecanismos de ejecución) se especifican en la presente Regulación.

- La investigación en defensa tiene su propia línea presupuestaria, separada de la de Horizonte Europa, una comunicación de la Comisión lo detallaba. Muy importante las dos ventanas de investigación y desarrollo, la idea es que al estar en el mismo reglamento estén coordinadas y hagamos todo el ciclo que comentaba antes hasta conseguir el avión o el tanque definitivo.

- Es importante centrarse en investigación aplicada. Considerar agenda estratégica de investigación (u OSRA) de la Agencia europea de De-

fensa (EDA); pero también sin descuidar lo que es investigación disruptiva, cuanto más se baja de nivel más se acerca a la investigación básica civil, y más solape hay.

- Sinergias con otras iniciativas de la Unión Europea en I+D civil (singularmente Horizon Europe) para evitar duplicidades y garantizar la "fertilización cruzada".

- Importancia especial de ciberseguridad y ciberdefensa. La investigación en Defensa no quiere abandonar las líneas de tecnologías disruptivas que, en el pasado, de alguna manera, la investigación militar ha liderado en los desarrollos y eso ahora no ocurre tanto, ya se ha quedado con presupuestos más bajos, hasta cierto punto casi retrasada la investigación de Defensa.

- Importancia también a los PYMEs-MidCaps, se menciona específicamente los temas de ciberdefensa y se habla de que la gestión directa la hará la Comisión Europea y no la Agencia Europea de Defensa que ha hecho la acción preparatoria.

DISPOSICIONES COMUNES

- Presupuesto. El presupuesto es de trece mil millones (13.000 M€) de euros total, cuatro mil cien millones (4.100 M€) de euros en investigación, quinientos ochenta y cinco coma siete millones (585,7 M€) de euros al año más ocho mil novecientos millones (8.900 M€) de euros en desarrollo, y se reserva un 5% para tecnologías disruptivas.

- Elegibilidad entidades:

  - Subsidiarias europeas controladas por un tercer actuando los EE.MM. Como patrocinadores.
  - Infraestructuras del beneficiario localizadas en territorio de un tercer país no asociado.

- Elegibilidad acciones:

  - Tres entidades legales de al menos tres Estados miembros o asociados. Al menos tres de estas entidades elegibles establecidas en al menos dos Estados miembros o asociados no estarán controladas directamente ni indirectamente por la misma entidad y no se controlarán entre sí. Lo que llaman la clausula anti Alemania-Francia de alguna manera.

• Criterios de adjudicación:

- Excelencia o potencial disruptivo en defensa.
- Innovación y desarrollo tecnológico y competitividad de la EDTIB. Intereses de seguridad y defensa de la Unión.
- Cooperación transfronteriza de entidades, sobre todo PYMEs.

• Financiación:

- Al haber dos ventanas, es importante un cambio con lo que se hace en las Fuerzas y Cuerpos de Seguridad en investigación civil. El 100% en investigación la CE. Necesaria cofinanciación (% variable) en desarrollo.

• Costes indirectos:

- Tarifa plana del 25% de los costes directos elegibles totales excluyendo costes directos de subcontratación (pero se anuncia flexibilidad para mejorar cobertura) Las empresas se quejan de que los costes indirectos no cubren los gastos reales, porque en Defensa son superiores, y se está discutiendo cuál es el que se pondría de gastos indirectos, para que en el Fondo Europeo de Defensa se eleven con respecto a lo que se hace en el mundo civil.

• Otras formas de financiación:

- Además de *grants (incluye lump sums) procurement y prizes*, con ciertas restricciones.

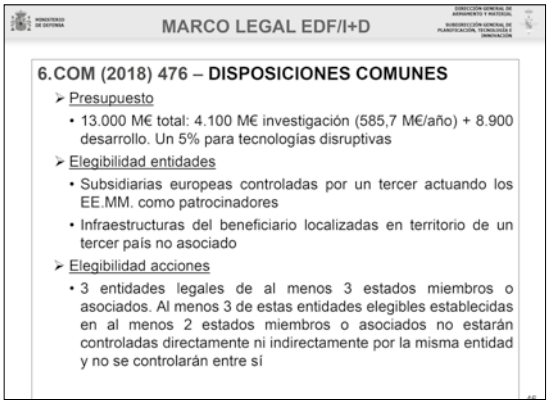


Imagen 10

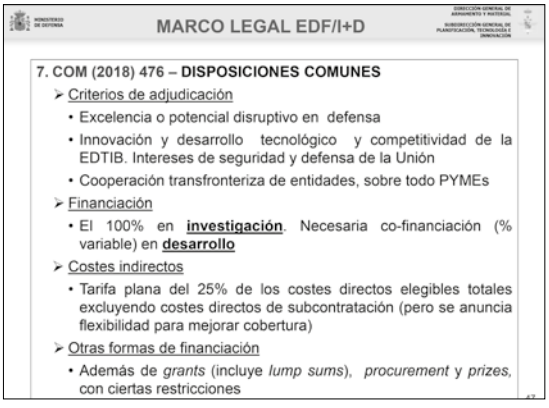


Imagen 11

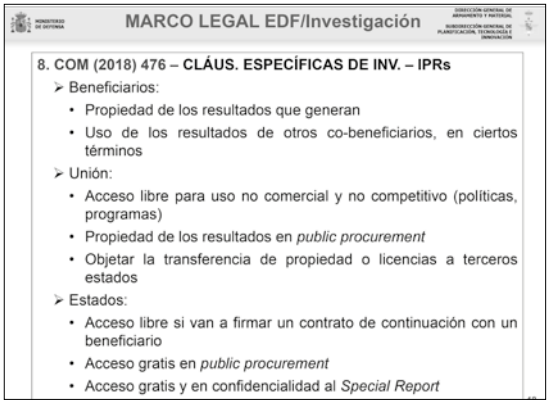


Imagen 12

CLÁUSULAS ESPECÍFICAS DE INVESTIGACIÓN. IPRs

Las cláusulas IPRs son básicamente parecidas a las que se hacen en el mundo civil.

• Beneficiarios:

- Propiedad de los resultados que generan: son los propietarios de los resultados, pero los Estados pueden tener un acceso libre, si van a continuar, a esos derechos de propiedad intelectual.

- Uso de los resultados de otros cobeneficiarios, en ciertos términos.

• Unión:

- Acceso libre para uso no comercial y no competitivo (políticas, programas).
- Propiedad de los resultados en *public procurement*.
- Objetar la transferencia de propiedad o licencias a terceros Estados.

• Estados:

- Acceso libre si van a firmar un contrato de continuación con un beneficiario.
- Acceso gratis en *public procurement*.
- Acceso gratis y en confidencialidad al *Special Report*.

CONCLUSIONES

- La preparación y gestión de la Acción Preparatoria de Investigación en Defensa está siguiendo en lo posible las pautas del H2020. La acción preparatoria está siguiendo las pautas hasta donde es posible H2020.

- Gran interés de las entidades españolas para preparar propuestas (aunque el sector específico de defensa es mucho menor que el civil). Sin embargo, hay pocas oportunidades de financiación. Ha habido mucho interés de entidades españolas, a pesar de que hay muchas menos que en el mundo civil; pero la acción preparatoria con tan pocos programas que se financian, muchos se han quedando a las puertas después de un gran esfuerzo.

- El 12.6% del presupuesto de la PADR 2017 va a retornar a entidades españolas (8,46% fue la aportación de ES al presupuesto de la UE en 2017). Pero, no se pueden echar las campanas al vuelo hasta que no termine 2018 y 2019, porque un pequeño golpe de suerte puede variar ese porcentaje.

- En nuestro caso, se va incrementando el interés tanto en la acción preparatoria PADR como en posibles programas duales del H2020 de los usuarios finales militares que como sabéis son variados: Ejércitos de Tierra y del Aire, Armada, Unidad Militar de Emergencias, Mando Conjunto de Ciberdefensa, Unidades contra IED (artefactos explosivos improvisados) etc.

  La unidad está en la comunidad de usuarios que creó el Ministerio del Interior donde nosotros enviamos una comunicación a todos los ejércitos, diciendo que participen en la comunidad de usuarios que es interesante. Ahí hablará con Policía, con Guardia Civil, Policías Autonómicas, para buscar temas de interés común. Si tenemos suerte, en el tema del láser, habrá usuarios militares este año si alguna de las convocatorias resulta seleccionada.

- Escasez en la PARD de evaluadores que cumplan los requisitos en la base de datos manejada por la Agencia Europea de Defensa (EDA).

- Necesidad de que los evaluadores cumplan con los requisitos (habilitación de seguridad y validación por el Ministerio de Defensa).

- El programa de Investigación en Defensa, empieza a definirse (borrador de Reglamento publicado en Junio de 2018) Oportunidad de optimi-

zar su formato final, aprendiendo de la experiencia general del H2020 y la específica de la PADR.

- Como he comentado, hay dos programas de Prospectiva Tecnológica contratados en la PADR de 2017 y 2018. El de 2018 es muy importante tiene 1,9 millones de euros, podría ser un inputs para decidir cómo nos gastamos los cuatro mil millones (4.000 M) de euros.

- La Agencia Estratégica Global de Investigación (OSRA) de la EDA también se considerará para la definición de los programas de trabajo que, en todo caso, tienen que ser específicamente militares.

- ¿Cómo determinar la parte de inversión en tecnologías más básicas (que por definición tienen carácter más dual) y la parte dedicada a tecnologías más maduras (para conseguir capacidades operativas concretas)? El EDF asigna un 5% a tecnologías disruptivas para defensa.

- Inevitable cierto solapamiento con temáticas civiles, especialmente para investigaciones más básicas (TRL bajos).

- Cuando estén los dos programas en marcha, ¿cómo evitamos los solapes cuando hay cientos de propuestas muchísimas convocatorias? ¿Cómo evitar duplicidades de propuestas presentadas al Horizon Europe (civil) y al EDF (militar)?

- En todo este proceso, la DGAM pretende continuar contando, lo hemos hecho desde el principio, con la estrecha colaboración y asesoramiento del CDTI e incrementar los contactos con usuarios finales nacionales del Sector de la Seguridad.

TURNO DE PREGUNTAS

Pregunta en sala: José Francisco López Sánchez, Inspector Jefe del CNP, Jefe del Servicio de Innovación y Desarrollo de la Jefatura Central de Logística e Innovación. Me han llamado la atención varias cosas de la presentación, una de ellas es que coincidimos en cosas en las que tenemos los mismos intereses y he apuntado varios temas de robótica porque aunque directamente no tenemos interés, es un tema que a nivel europeo se está moviendo mucho en el ámbito civil de seguridad.

Neutralización de IEDs y RNBQ es un tema que nuestras unidades, tanto Guardia Civil como Policía estamos participando incluso en proyectos conjuntos, son CSAs y que tratan de unificar de alguna manera; son redes de puntos nacionales o de policías de los Estados de la Unión Europea, no recuerdo cuantos participan, precisamente donde se van a debatir estos temas y con una idea de prospectiva. Es decir, es casi lo mismo que podéis hacer vosotros en el ámbito EDA. Combatiente del futuro, algunas veces lo hemos hablado y por qué no hacer también el Policía del futuro. A todos los desarrollos de integración, de tecnología mismamente, los uniformes dan un campo de posibilidades enorme, por no pensar en cómo va a ser el Policía del futuro dentro de diez años. En las fuerzas policiales este tema se está tratando, me imagino que el objetivo será diferente, pero la tecnología va a ser la misma.

Mi pregunta es por qué esperar a que, a nivel europeo, se empiece a hablar de estos temas cuando en el programa coincidente, podemos aunar fuerzas; porque si los intereses son comunes podemos hacer punto de conexión entre programa coincidente y nuestros intereses también o incluso buscar en la Secretaría de Estado nuestra la forma de coincidir en determinadas temáticas a nivel nacional.

La otra pregunta es relativa al tema de prospectiva. Con el SPOT estamos en contacto con ellos para el tema de prospectiva porque hemos hecho unos contactos, estamos llevando un proyecto en el que participan Policía y Guardia Civil relativo a prospectiva en un montón de temáticas totalmente diferentes; es decir, se van a crear veinticinco grupos de trabajo en cinco años; España está liderando cinco grupos de trabajo y somos los encargados de la realización y puesta en marcha del radar tecnológico. Son muchos puntos en los que coincidimos ¿por qué no colaborar en esos puntos? La pregunta es tema de colaboración a nivel nacional o intercambio de información.

Responde: José Ramón Sala Trigueros

Muchas gracias, me parecen preguntas muy procedentes y son las que, de alguna manera, he comentado en la presentación. En cuanto a prospec-

tiva, como habéis visto, tenemos un sistema que llamamos observatorios tecnológicos, pero esto es a nivel nacional, Ministerio de Defensa; nosotros estamos en la calle Arturo Soria, y este personal se dedica a escanear y a ver los programas del CDTI, a ver lo que ha salido de los estudios de prospectiva que ha hecho la Comisión Europea, a ver lo que está haciendo la STO, intentando precisamente evitar eso, que es lo que todos queremos evitar: las duplicidades, los solapes, hacer lo mismo…

Nosotros siempre hemos tenido reuniones con la Guardia Civil para innovaciones, y lo que yo quiero transmitir es que hay que trabajar más, colaborar más, sin esperar nada, pero en cualquier caso, en esos temas se tiene en cuenta la parte civil, se intenta; es decir, exclusivos improvisados. Hay exclusivos que no son improvisados pero, de alguna manera, atacar vehículos, puertos, submarinos, etc. Esto es, se intenta siempre cuando se trata de esas temáticas duales o de protección NBQ. Por ejemplo, será necesario poner protección NBQ en el nuevo vehículo 8x8, vehículo sobre ruedas que está haciendo la DGAM tiene que llevar un sistema de protección NBQ. Ese es un caso en el cual la tecnología es la misma, pero ponerlo en el 8x8, no es trivial, hay que hacer algo, hay que trabajar: como en el caso comentado antes, si hay que hacer un Vamtac, darle una cierta tracción o… Eso es una parte de lo que hacen los coincidentes y se espera, igual que la protección del soldado, los diferentes ámbitos de arquitectura abierta del soldado, que no se duplique o se aproveche lo que ya se ha hecho.

Pero, en el caso del coincidente el objetivo es: cosas que se hayan hecho en otros ámbitos adaptarlas al mundo militar, no es tanto la investigación más básica como el tema de la fusión de información. Todo el mundo trabaja en fusión de información, la Policía y Guardia Civil seguro que más que nadie, pero a lo mejor hay que hacer un sistema que permita proteger una base provisional o un despliegue que se haga, o si se va a pernoctar, poner unos sensores que protejan. Hay que darle un matiz, puede que sea una misión que no es exactamente la que ahora hace ese sistema, aparte de que en el mundo de la fusión hay muchas tecnologías nuevas, aunque se llamen igual.

Estoy totalmente de acuerdo y por eso he mencionado diversos puntos en los cuales sé que en el ámbito de seguridad, se trabaja en algo parecido; con lo cual, la conclusión, por supuesto a nivel nacional, es que tenemos que aumentar los contactos y, a nivel del futuro programa europeo, hay que poner los mecanismos de los que estamos hablando para que, cuando se saque el programa de trabajo, ya esté diferenciado. No es fácil porque somos tantos cientos de personas trabajando en toda Europa, hay tanta información, que hay que tener un buen sistema y la idea sería replicar lo que ya se hace en los programas actuales para evitar que ocurran esos problemas.

Interviene: José Francisco López Sánchez.

Desde mi punto de vista lo que tendríamos que averiguar son los ámbitos que nos puedan interesar, pero también fijar otra punto y es que a nosotros como seguridad no nos interesa participar en TRLs bajos, nos interesa un TRL 5 o un TRL 7, 8; es decir, en esos puntos vosotros tenéis que invertir pero a nosotros nos da lo mismo, porque esperamos a que crezca. Entonces, quizás habría que fijar de alguna forma, dentro del Ministerio de la Secretaría de Estado, alguna forma de buscar sinergias, y hablando de lo que dijo ayer E. Belda, dinero hay, si buscamos cosas de intereses comunes la Policía, Guardia Civil y Ministerio de Defensa, donde consigamos unos TRLs próximos a mercado, a partir de ahí, el TRL 8 y 9, vosotros los podéis dedicar a una materia de tecnología y nosotros a otra; o incluso definir un 80% de lo que sería la nueva tecnología con especificaciones comunes y un 20% de adaptación. No tiene por qué ser el mismo objetivo para todos, poner una serie de bases de acuerdo y que nos podamos beneficiar todos de lo que hacemos en ambas partes. Esa es la idea que quería transmitir.

Responde: José Ramón Sala Trigueros

Estoy totalmente de acuerdo y para eso la participación en la comunidad de usuarios del Ministerio del Interior es de gran interés a esos efectos; porque allí están los usuarios hablando precisamente de estos temas con usuarios militares de ese ámbito; es decir, por ejemplo, en el ámbito NBQ, lógicamente, se trabaja mucho; pero puede ser que el NBQ del ejército de tierra no tenga las mismas misiones que la protección NBQ que hagáis vosotros, entonces al final necesita su propia línea de acción y aprovechar lo que hagan los demás, pero tiene sus funciones y sus misiones, que son un poco diferentes.

La conclusión final es que hay dos ámbitos que has comentado, primero tienen que estar usuarios finales del ámbito que sea, en la mayoría de los programas, pero la otra parte es lo que decías de los TRLs altos, también los usuarios militares quieren TRLs altos pero cuando resulta que, por ejemplo, China tiene unas comunicaciones cuánticas entre submarinos que no se pueden interceptar, se nos pregunta que por qué no se empezó hace diez años, para tenerlo ya, ahora, esa tecnología, porque sino habrá que esperar otros diez años más. Ese balance es importante.

Pregunta en sala: Maite Boyero Egido, representante de los intereses de España en el Comité de Gestión del programa Sociedades Seguras en la Unión Europea. Si me permites José Ramón, os voy a poner un ejemplo de algo que me pasó. Yo he comentado esta mañana que llevo diez años en esta temática y hace unos meses me invitaron a una jornada, un grupo que se llama RE LAB, que es un grupo de laboratorios y de alertas anti amenazas bioló-

gicas que hay en España y que en realidad se creó hace diez años; se puso en activo a raíz del caso del ébola, que fue uno de los casos que tuvieron que tratar. En la RE LAB, básicamente su objetivo son temas de investigación en amenazas biológicas; participan Fuerzas de Seguridad como vosotros, TEDAX, NBQ..., pero también gente del ejército para la parte de TRLs bajos y para la parte de operativa en misiones humanitarias y cosas parecidas. Era la primera vez que yo iba a la reunión y antes de ir me preparé en base a los temas que tratan sobre armas biológicas y que es la parte realmente específica del programa H2020. Hay bastantes proyectos, alrededor de quince o veinte y ahí claramente han explorado las sinergias, la colaboración común; es un ejemplo claro de colaboración. Si tenemos que replicar para cada cosa una red diferente, es una barbaridad, pero tampoco hay tantas cosas en las que coincidimos, de hecho yo había hecho una lista para la mesa redonda y, efectivamente, son las que has mencionado tú: hablamos de explosivos, de NBQ, de Drones, de robótica, de inteligencia artificial, pero son duales, se usan en los dos ámbitos. Sí que existen iniciativas de colaboración cruzada, pero tampoco suficientes, falta todavía por profundizar.

Intervención en sala: vosotros tenéis un dinero para contratar o hacer un contrato de investigación con una empresa y encargar lo que queréis, o sois parte de un consorcio normalmente, o vais al albor de un programa europeo; es decir, ¿tenéis programas puramente nacionales?

Interviene: José Francisco López Sánchez.

Nosotros, programas nacionales en los que participamos, no tenemos; lo que es verdad es que aunamos intereses entre Policía y Guardia Civil con Secretaría de Estado; nos han dicho muchas veces que están dispuestos a invertir lo que haga falta. Al fin y al cabo, es un tema de coordinación, no es la primera vez que hacemos algo conjuntamente y, también, podemos buscar el mecanismo, podemos empezar algo que hemos pedido hace tiempo, que es el tema de la compra pública innovadora que en su momento estuvimos tanteando con el Ministerio de Economía y competitividad; la posibilidad de meternos en los mecanismos de compra pública innovadora, incluso llegaron a decirnos que nos reservaban treinta millones de euros (30M). Nos pusimos en marcha, Policía y Guardia Civil, llegamos a un acuerdo de presentar más o menos diez iniciativas de I+D; por desgracia, con cambios de subdirectores, rehacer fichas, con partes que se podían considerar como secretas, o que por la Ley de Contratos iban a ir por secretas,… Al final, fue un maremágnum que nos estuvo mareando dos años, las firmas de los acuerdos entre los Ministerios de Economía y del Interior, fue un desastre. El mínimo que nos pedían por cada proyecto, eran entre cinco y seis (5 y 6 M) millones de euros y nuestros proyectos, la mayoría, no llegaba a cuatrocientos mil euros (400.000). Teníamos claro el objetivo, y teníamos claro lo

que queríamos, pero necesitábamos pensar un poco más a lo grande en cada objetivo. Entonces, la idea que quiero plantear es que nosotros el dinero para un proyecto determinado, lo podemos conseguir, podemos movernos para impulsar otros mecanismos externos pero, evidentemente, tiene que existir el apoyo de Secretaría de Estado y si conseguimos que vosotros podáis aportar una parte para mejorar ese proyecto de I+D, podría ser interesante; porque el beneficio puede ser conjunto, teniendo en cuenta clarísimamente la división; es decir, vosotros tenéis unos objetivos, nosotros otros, por eso he planteado el tema del 80% de especificaciones conjuntas y un 20% de adaptación, o un 70 - 30 o un 60 - 40. El tema es buscar sinergias para apoyarnos o intentar beneficiarnos mutuamente de cosas que podemos sacar desde el ámbito civil.

Pregunta en sala: ¿Tenéis algún documento que especifique las metas tecnológicas o desarrollos que os gustaría conseguir?

Responde: José Francisco López Sánchez.

Eso es lo por lo que llevamos luchando desde hace tiempo, en el año 2010 por parte de Secretaría de Estado se montó una iniciativa muy interesante, se llamó Gisec. Esta iniciativa consiguió -dentro de Policía y Guardia Civil, creo que también participó tráfico y protección civil y el CICO entonces- movilizar casi cien personas, todos expertos en diferentes materias. El objetivo era precisamente hacer eso, identificar las necesidades tecnológicas de todo el Ministerio y sacar un documento priorizado con necesidades. Además de otra serie de objetivos que fueron aprobados por el CEMU en su momento, incluso uno de los objetivos clave, además de hacer una estrategia e innovación del Ministerio, era conseguir una entidad o empresa pública paralela al Ministerio en el que se pudiese empezar a mover el dinero de las inversiones y rentabilizar los retornos. Es decir, nosotros hacemos I+D con las empresas, y las ventas de esas empresas, la parte de la propiedad intelectual que nos venga en retorno para volver a invertir; es decir, empezar a mover una rueda de inversiones dentro del Ministerio en I+D. Se consiguió un presupuesto para I+D, cambió el Gobierno y tuvimos problemas para ejecutar el millón (1M) de euros que nos pusieron de presupuesto porque cambió la ley; se avecinaban elecciones generales, ya nadie quería mover nada; por lo que, esa iniciativa se eliminó. La intención que hemos tenido ahora con los *couch* que has mencionado es precisamente el revitalizar toda esa actividad; por eso, una de las reuniones de expertos que va a haber ahora es la identificación de necesidades tecnológicas dentro del Ministerio. Para volver a reintentar tener un presupuesto y el priorizar necesidades de todo el Ministerio, al fin y al cabo los grandes aportadores de necesidades, posiblemente seamos Policía y Guardia Civil; y buscar sinergias dentro del Ministerio, que no invertir conjuntamente. Por eso, ahora mismo te digo

que no tenemos, pero la idea es que los *couch* que has mencionado, dentro de tres años podemos conseguir una cosa más o menos clara y que se pueda publicitar a las empresas incluso a nivel nacional para intentar potenciar la empresa española. Ese es el objetivo, que no tengamos que comprar producto exterior y lo hagamos con I+D interior nacional.

Interviene en sala: Anastasio González, Secretaría de Estado. Ayer estuvo nuestro Subdirector General y entre otras dijo que ahora mismo hay ciento treinta y siete proyectos en marcha para todo el Ministerio. Temas de fronteras, de instituciones penitenciarias, tráfico, protección civil, Policía, Guardia Civil, etc. Nosotros, por ejemplo, yo estoy en la inspección, tenemos varios abiertos, uno que está a punto de terminarse es la digitalización de todos los libros oficiales que hay en las oficinas de Policía y Guardia Civil; es decir, que ya no están los libros de papel sino la digitalización. Otro es la digitalización de los archivos, aunque solo sea por motivos de seguridad, que los archivos pesan y a veces están en sitios altos. Creo que es el momento de priorizar por que, cómo se manejan ciento treinta y siete (137) proyectos, en una Subdirección que no es muy grande. Simplemente quería aportar este dato que nos dio el Sr. Belda ayer. Gracias.

MESA REDONDA: SOCIEDADES SEGURAS: PROTEGER LA LIBERTAD Y LA SEGURIDAD DE EUROPA Y SUS CIUDADANOS

Modera: Maite Boyero Egido.
Participan: Ramón Darder Colom; José Ramón Sala Trigueros

Interviene: Maite Boyero Egido

Hay muchos temas que quiero compartir con vosotros porque cuando estábamos preparando la sesión de hoy, titulada Horizonte 2020, al final se han abordado muchos otros temas que son complementarios al programa Horizonte 2020.

Horizonte 2020, lo que nos aporta, es una estabilidad, continuidad en la financiación y una estructura; es decir, nos da un marco de referencia para trabajar en él. Pero luego, vemos que los compañeros de Defensa están tomando iniciativas de ámbito nacional y Europeo con las que podríamos cooperar, o coparticipar, o incluso copiar, porque nos pueden venir bien sus ideas.

Y, por otro lado, vemos que en el marco del Ministerio del Interior no se ha tratado de organizar, adecuadamente, las actividades de I+D que existen, no están estructuradas al estilo Horizonte 2020 u otro programa marco. Eso, en algunos países, se hace y al final es una forma de organizarse; es decir, yo trabajo en el ámbito de drones y mi tema es este y aquí hay cuarenta millones de euros (40 M€), pues vamos a ir tirando de ese presupuesto.

Además, en la sesión del día de hoy, hemos visto varios programas, principalmente dos: Horizonte 2020 y el programa de Defensa; que son complementarios y no son los únicos, de hecho hay un apunte que creo que lo has comentado tú José Ramón, del programa específico y el reglamento que ha

aparecido de la Unión Europea. Yo estoy trabajando estos documentos que son bastante pesados de leer, toda la regulación de los nuevos programas Horizonte Europa y, precisamente ayer, porque tenía que enviar comentarios a la representación permanente en Bruselas (Reper), me leí uno que tiene un anexo que se llama Sinergia, o sea sinergias de todos los programas de I+D con otros programas europeos y, en la parte del *cluster* 2 de Horizonte Europa que va a aparecer a partir del año 2021, se mencionan las sinergias con el EDRP (*European Defence Research Programme*), y no se mencionaban sinergias con el ISF (*Internal Security Fund*), ni tampoco con el *Integrated Border Management Fund*, que es el fondo de fronteras. Pedí expresamente, en coordinación con otros países, que pongan esas sinergias porque, efectivamente, son programas con los que se desarrollarán sinergias.

Claramente hemos visto que entre civil y defensa, existen sinergias: ciberseguridad y ciberdefensa. Ha salido en la presentación esta mañana, por parte de José Ramón, los NBQ, los TRL más bajos los trabajáis vosotros, y los TRL más altos Interior; vigilancia de fronteras, vigilancia marítima; hay más ámbitos para patrullas militares otros para civiles; y por supuesto explosivos, drones, inteligencia artificial, tenemos múltiples ejemplos.

Quería hacer varias preguntas, claramente lo de las sinergias está ahí, lo tendremos que trabajar, creo que la comunidad de usuarios va a ser un punto de partida. La comunidad de usuarios nos tiene que servir para organizarnos mejor para que conozcamos y sepamos que hay cosas que no hay que duplicar y que, efectivamente, se duplican; para aprovechar mejor el dinero. Se ha hablado de la dificultad de participar, de ayudarnos los unos a los otros, pero también y, sobre todo, de hacer una labor que, como autoridades públicas, tenemos la obligación, que es la de dinamizar la industria. O sea, la industria de Defensa y Seguridad son diferentes, y ahora sí me gustaría que abordaseis el tema.

¿Cómo veis vuestra participación en las comunidades de usuarios? Porque la industria está necesitada de que nosotros le digamos lo que necesitamos. Oferta y demanda, es una reclamación que nos hacen constantemente. Lo que quería saber es cuáles son las expectativas sobre todo de cara a los que están aquí hoy y que quizás no se han acercado a esa comunidad de usuarios, ¿qué recomendaciones podéis hacer sobre cómo lo veis vosotros?

Interviene: Enrique Belda Esplugues

Obviamente, en esta comunidad de usuarios que empezó a caminar todavía no hace un año, se han definido diferentes grupos de trabajo. Cada grupo tiene que estudiar un ámbito, una temática. Puede que unos tengan más sinergia con la parte de Defensa y otros menos. Es posible que tengamos que definir si en esas deliberaciones que los grupos de trabajo van a tener

que realizar, tendrán que determinar cuáles son las necesidades tecnológicas en Defensa, en seguridad; las que tenemos los usuarios finales españoles; y podríamos decirles que si son capaces de encontrarla que indiquen también esas posibles sinergias con finalidades militares, con finalidades de Defensa.

Ambos programas tienen finalidades distintas, la misión militar y la misión policial son distintas. Se ha hablado de la industria en cuestiones de Defensa y de industria en cuestiones de Seguridad. Viendo la presentación de José Ramón Sala, he encontrado que el 80% de las empresas que son socios en las ACES, por parte de Defensa, son las mismas empresas que están en nuestros proyectos de seguridad. Todas tienen su rama de Defensa, todas tienen su rama de Seguridad en el fondo; ellos también deben tener un bagaje, un conocimiento, en ambos sentidos, de cómo está más la I+D en Defensa y cómo está la I+D en Seguridad. Las que he visto en tu presentación son las mismas con las que colaboramos nosotros, son las mismas que cuando vamos a un evento o feria de seguridad como Sicur, o Milipol en París, son las mismas empresas.

De cara al futuro, como dicen desde la Comisión Europea cuando se les pregunta por estos temas, hay que identificar esas tecnologías duales y hay que establecer sinergias, pero en estos grupos de trabajo que tenemos hay que definirlo mejor, de una manera más detallada y en qué podemos coincidir estas dos partes.

Interviene: José Ramón Sala Trigueros

Respecto a esto que estáis comentando, efectivamente, primero la industria, como decía antes en la presentación, la parte de industria de Defensa es muy pequeña y evidentemente en muchos casos son las mismas industrias pero hay un matiz: en Indra, por ejemplo, la parte de dirección de Defensa tiene una estructura que trabaja en Defensa y luego puede haber una parte de ingeniería que venga de otros departamentos de Indra, pero la diferencia fundamental como sabéis y por eso el Fondo Europeo de Defensa tiene características especiales, es porque para esas direcciones de empresas, el cliente es uno, que es el Ministerio de Defensa y es un cliente que en los últimos años no tiene un gran presupuesto y que está sujeto a posibles cambios de decisiones o de normativa

Aunque el nombre sea el mismo, es muy difícil que una empresa que sea pura, absoluta y únicamente de Defensa porque necesita diversificar clientes y mercados. Ahora bien, os pongo ejemplos de sinergia, como Airbus y su sistemas UAV Atlante, que tiene usos también para vigilancia en el sector de seguridad, lo llevan a las ferias, se lo presentan a las fuerzas de seguridad, etc. Entonces ¿qué ocurre? Para el Ministerio de Defensa, puede haber requisitos para un UAV táctico, por ejemplo posibilidad de llevar armamento, que seguramente no sean necesarios para las Fuerzas de Seguridad porque ellos quieren

vigilancia, vigilancia costera; y al llevar armas te complica, tienes que ponerle puntos duros en el ala, tiene que llevar unos sistemas de SM de guerra electrónica que complican el tema de alimentación eléctrica, el posicionamiento de antenas, etc. Hace muchos años recuerdo que ya la Guardia Civil probó el Camcopter. Nosotros, teníamos un programa de predicción de periodos quiescentes del mar, para el momento en el que el buque está estable y aterrice el AV o incluso helicópteros tripulados, porque a lo mejor tienen que operar en el mar y el estado de la mar está muy alta; pero esas misiones quizá no sean necesarias en la vigilancia costera de la Guardia Civil, porque a lo mejor en ese momento no hay lanzaderas porque la mar está mal.

Ese es el pequeño plus, en el que te gastas un montón de dinero, un plus donde hay que buscar una parte común que sirve para todos y otra militar, armado, etc.. Ese es el reto, como decíamos, la parte común civil y el plus militar. Yo os invito a que escribáis artículos en las revistas, en los boletines que tenemos; que nos reunamos y hablemos de todo esto; aparte de la comunidad de usuarios puede haber otros ámbitos en los que trabajemos en esta línea tan beneficiosa.

Interviene: Maite Boyero Egido

Yo quería abordar un tema diferente porque creo que puede ser de interés de las personas que están hoy aquí. Me gustaría que contaseis, además, lo que habéis abordado brevemente en vuestras intervenciones, valorar cómo ha sido cualitativa y cuantitativamente vuestra participación -de vuestras unidades-, en los programas marco. El Ministerio de Defensa, por ejemplo, participa desde el año 2013 en un proyecto que ahora se llama EUCISE 2020, Guardia Civil tiene una experiencia dilatada sobre vuestra participación; y me gustaría que contaseis sobre todo ¿a qué se enfrenta una unidad cuando se plantea participar en el sentido positivo y en el negativo y, sobre todo, a corto, medio y largo plazo, qué pasos tienen que dar, cómo los tienen que dar, qué recomendaciones les haríais y que ventajas o desventajas puede tener su participación? Siempre en el contexto de vuestra experiencia.

Intervención en sala.

Empezaré por las dificultades que podemos encontrar. Hace como diez u once meses nos reuníamos con unidades nuestras para un proyecto específico, y hubo una pequeña discusión en la que alguien dijo: "es que yo no veo ningún interés en participar, porque si necesito este producto, no voy a esperar tres o cuatro años para tenerlo". Esta no es la finalidad de H2020 estamos en un programa de I+D en seguridad, si queréis un producto de mercado hay que ir a otros fondos, a buscar otra financiación.

Aquí, estamos intentando que participen unidades nuestras, en proyectos de I+D; porque, a la larga, aporta beneficios. No nos cuesta dinero, toda

la financiación que vamos a recibir de estos proyectos es al 100%; vamos a tomar dinero de la Unión Europea, vamos a ganar en prestigio y vamos a estar integrados en un consorcio que va a estar formado como mínimo por seis países Estados miembros. Ya estás metido en un consorcio, ya eres visible en el resto de Europa, no a nivel global, pero por lo menos tienes una visión que si te quedas en tu despacho no la tienes, si te quedas en tu unidad no la tienes. Esa dificultad para cambiar de forma de pensar de algún Jefe de Unidad que es reacio, que no quiere que su gente pierda tiempo haciendo otras labores; en el fondo no es perder el tiempo, es primero: cumplimentar uno de los objetivos estratégicos que tenemos en nuestro mapa estratégico que tenemos que impulsar la I+D+i todos, no solo desde el servicio de innovación tecnológica, tenemos que hacerlo desde todas las unidades.

Esa es la primera dificultad que nos encontramos, esa concienciación. Tenemos suerte porque ya hay muchas unidades que se han vuelto activas, que han visto esa ventaja, ese beneficio. A corto plazo es difícil cuantificarlo; para una unidad cuando se mete en un proyecto ya es visible en muchos foros, ya es visible en Europa; tiene que estar viajando para reuniones en consorcio, para el *kick-off*, la primera reunión inicial, de alguna manera, va ganando cierto prestigio. A medio plazo, es el tiempo que dura el proyecto, tres, cuatro años; pero a largo plazo, en la distancia, toda esta experiencia que vamos acumulando, después de todos estos años, estamos viendo que, solamente por participar, está dando un plus, un caché en instituciones europeas, o sea somos conocidos. En otros Ministerios de Interior como en Austria, Francia, Alemania, también somos conocidos, sobre todo somos gente a la que pueden buscar cuando tienen una necesidad. Podemos decir que nos estamos posicionando, buscando un hueco en Europa y la verdad es que es muy valioso y nos sirve no solo a nosotros, que nos movemos en el ámbito de la I+D, sino que puede servir a cualquier otra unidad. Cuando voy a estos eventos, que normalmente se celebran en Bruselas, o eventos de *brockers,* nos reunimos durante dos días, universidades europeas, empresas, policías, bomberos, ambulancias, las fuerzas de emergencia de primera respuesta; somos buscados, ya tenemos cierto caché y cuando en Europa alguien está buscando socios para montar un proyecto, un consorcio, nos buscan. Queda un mes y medio para cerrar la convocatoria, nos están diciendo: este es un proyecto de este consorcio, el *topic* está montado, está todo hecho, ¿os metéis? Nos hace falta un cuerpo de policía europeo. Es una satisfacción saber que cuentan con nosotros. Pero no nos vamos a meter en todos los proyectos, evaluamos los que nos lo solicitan, distribuimos las peticiones, sondeamos las unidades…, hay unidades que se han hecho un nombre, incluso hay unidades en Guardia Civil que han hecho un pequeño equipo de I+D como la jefatura de información, o el servicio de criminalística. Esos jefes de unidad han tenido una mentalidad muy abierta, muy positiva en este sentido y no han pensado que van a perder dos personas en un departamento de I+D, sino que han visto que es ganar, a largo o medio plazo, pero ganar.

Interviene: José Ramón Sala Trigueros

Por nuestra parte, la Armada participa, pero en aquellos tiempos cuando entraron el Ministerio de Defensa no tenía un sistema reglado de participar en el Horizonte 2020 o en los programas antecesores. Pero en cualquier caso, creo que están haciendo un buen trabajo por lo que yo sé y el problema de ellos y del resto de unidades es de falta de recursos para participar. Siempre es difícil encontrar expertos que puedan participar en estos programas y normalmente tienen gran carga de trabajo al participar en muchos grupos de trabajo de la OTAN, tienen que asistir a operaciones, etc. Pero ahora sí tenemos un sistema reglado que ya está en el BOE, una orden del Secretario de Estado de Defensa diciendo que se puede participar en Horizonte 2020 y dando un procedimiento, y rápidamente distingo entre el ámbito civil -Horizonte 2020- y el de la acción preparatoria. En el caso de Horizonte 2020 está ocurriendo lo que comentáis: nos piden que participe por ejemplo, la UME (Unidad Militar de Emergencias), nosotros tenemos un procedimiento de tal manera que, cuando hay una solicitud de empresas de participar, tenemos un procedimiento rápido para que ellos lo puedan evaluar si les interesa o no.

La reacción general de los usuarios es que es un problema añadido, pero como he dicho en la presentación, se está incrementando su interés porque, sobre todo, en la acción preparatoria en la parte de investigación y defensa es una manera de influir en los posibles resultados que se obtengan después. Ya hay grupos de trabajo, la manera de empezar a hacer camino es participando. Problemas importantes, los del día a día a los que nos enfrentamos, el cómo cobrar los costes; hemos hablado con Guardia Civil a este respecto pero, en el caso de Defensa es más complicado porque incluso se pertenece a Secretarías de Estado diferentes. Pero estamos preparando un procedimiento que creemos va a funcionar.

Interviene: Maite Boyero Egido

Yo creo que estáis en la fase en que estaban Guardia Civil o Policía Nacional en el año 2008-2009, cuando estaban empezando a rodar en el programa, y los temas que había que afinar a nivel administrativo, y algunos que todavía colean, pues lleva su tiempo. Si os sirve de consuelo, nosotros en el CDTI también tenemos dificultades. Si me permitís, una última pregunta para ir terminando. Ha hablado Ramón de cuando se os llama para participar; quiero que afinéis un poco más en ese ámbito y tratéis de dar algún tipo de recomendación desde cómo se analiza una propuesta, es decir, una oferta de participación en un consorcio por parte de una universidad o empresa española porque, a veces, os invitarán de un consorcio extranjero, pero lo más probable es que alguno de vosotros tenga una empresa con la que trabajáis habitualmente, sobre todo de cara a unidades con poca o ninguna experiencia en esto, ¿cómo valoráis el participar o no y cuáles son los pasos que dais antes de decir sí o no, a una propuesta?

Intervención en sala.

La propuesta cuando nos llega, hay que mirarla a fondo y pensar a quién le puede interesar, quién está trabajando en eso. Como tenemos un contacto muy fluido con nuestras unidades ya sabemos qué le interesa a cada uno porque nos lo comentan en las conversaciones que mantenemos. Si la empresa, la universidad o el centro de investigación, es español, se le suele dar prioridad, apoyando a la competitividad de la empresa española, a las universidades. Y, muchas veces, le encaja mejor a una unidad que a otra, porque es más proclive, tiene más experiencia. Y, si acepta, le pedimos a su jefe una carta de compromiso de horas o esfuerzo y que estén definidas; una carta en la que se va a comprometer el jefe a que su gente realice el esfuerzo.

En alguna ocasión, nos hemos encontrado que la unidad ideal para este proyecto es una unidad que no puede adquirir el compromiso por la carga de trabajo, porque no tiene recursos suficientes, porque no son tan proclives a participar en estos proyectos, o porque su jefe dice directamente que no le ve ninguna rentabilidad. Ahí empieza nuestra labor de comercial dentro de nuestra propia institución, una labor de tratar de convencer. Si se niegan, no podemos hacer nada y tenemos que decirle a esa empresa o a esa universidad que lo sentimos, que no hay interés. Muchas veces es esta la contestación.

¿Qué se le puede decir a una unidad para tratar de convencerla? Si se mete en ese proyecto, por lo menos va a tener unos socios, españoles algunos, y va a empezar a hacer contactos que seguramente en el futuro, para cualquier otra necesidad que tenga, van a tener consecuencias positivas y, como consecuencia, no va a tener que hacer una prospectiva en el mercado de buscar esas empresas pues ya las ha encontrado. Por poner un ejemplo, hace unos años en el servicio de estadística, teníamos que organizar cursos de estadística en universidades por toda España ¿Cómo se hace? Si llevas un bagaje de I+D, ya sabes qué empresas o qué universidades están en este tipo de tecnología. En definitiva, te metes en el mundillo que nunca sabes cuándo te va a hacer falta de cara al futuro.

Entonces, si la unidad tiene recursos suficientes, si no tiene problemas, algún tipo de incompatibilidad con la empresa o la universidad; lo positivo es participar, meterse en el proyecto y, como decimos, una recomendación que desde nuestra unidad también hemos tenido que decir, si tienes dificultades en esa parte administrativa, contacta con el servicio de innovación tecnológica que vamos a ayudar al 100%.

Intervención en sala.

Por nuestra parte, creo que de momento, tanto en la parte civil de Horizonte 2020 como en la acción preparatoria, ha habido pocas oportunidades hasta ahora, el factor que más prima por el momento es apoyar a la industria

española, si el tema es interesante. Quizás, lo ideal es lo que comentabas, que es liderar un consorcio o hacer de germen de lo que quieres, conseguir aglutinar. Sin embargo, esa parte, de momento, la veo difícil; porque por la carga de trabajo que hay, en el caso de los usuarios, pueden decir que no es su labor principal el hacer un programa de I+D.

En su momento, cuando llegue el programa de Defensa quizás lo ideal hubiese sido conseguir dirigir las propuestas desde el principio. Eso, sin embargo, es difícil; porque con tantas carencias decir realmente lo que quieres, a veces, es difícil; o priorizar o elegir uno de los campos de acción que tienes, sería lo ideal, pero de momento, lo que más se está haciendo es participar.

Intervención en sala.

En un evento de brókeres en Bruselas, coincidimos con Francisco Andrés que es un investigador del Instituto Elcano. Elcano lidera, coordina, el proyecto MINDb4ACT en el que está la Guardia Civil, es un proyecto de prospectiva no tanto tecnológico. Y, hablando con Francisco, le comentaba lo difícil que es coordinar, porque hay que poner entre quince y veinte socios; y me respondía: el primero cuesta más, ya llevo cinco, el quinto sin problemas.

Entonces, tanto para las unidades, como para los que quieran entrar como socios, que le pregunten a la unidad de fiscal y fronteras, que les dirá, que el primero cuesta y el décimo se hace con los ojos cerrados. Esa es la idea que quiero trasmitir a los aquí presentes si quieren participar como socios.

Interviene: José Manuel Rabadel

Estoy en el departamento de proyectos europeos y me gustaría hacer hincapié en una cosa: cuando nosotros nacimos teníamos un jefe, el equivalente, la persona responsable de la Policía Nacional de Madrid, entonces era todo puente de plata; quiero decir, nos atrevimos a presentar un proyecto que íbamos a coordinar nosotros. En ese momento, teníamos todos los apoyos, teníamos más personal del que tenemos ahora, pero el problema que tenemos actualmente, y esto entronca con la problemática de la Administración, es que ahora no se ve así, estamos vendiendo, haciendo el *lobby* interno de manera permanente para justificar por qué tenemos que estar en proyectos europeos. Ya sé que suena extraño en este foro, pero es algo que nosotros entendemos como fundamental para el futuro de los ciudadanos y de nuestra ciudad; en el caso de Madrid, pensar en presente y pensar en futuro de las necesidades que va a tener la Policía Municipal de Madrid, en este caso, creo que es convergente con la Policía Nacional y la Guardia Civil, porque, además, estoy totalmente de acuerdo con lo que dice Pepe y es que convergen, hemos tenido trabajos de prospectiva y estamos en la misma línea todos, lo que pasa es que somos los más "pequeños" de este sector.

Cuando comentaba Maite el tema del ébola, algunos de nosotros hemos entendido que ese es un riesgo crítico para las ciudades y ahora sí que incardina con el planteamiento de no entender que tengamos investigación básica y que dentro de la Administración tengamos pasillos en los que Guardia Civil, Defensa, Policía Nacional, Policía Local, Samur, Protección civil, tengamos contacto; sepamos que vosotros tenéis NBQ, lo tiene Guardia Civil, y nosotros solo tengamos uno, lo tiene Samur; el que la Administración no esté en cajas estancas que no se conocen y por eso es tan importante, porque empezamos a ponernos caras y traspasamos esas barreras físicas o mentales, que tenemos.

Son problemáticas horizontales que nos traspasan a todos, desde lo local o municipal, porque al final Defensa me puede solucionar un verdadero problema de seguridad pública. Solo la experiencia es positiva para trabajar en proyectos europeos: imagen, mentalidad, el tener como socio a una persona del MIR que aparentemente son los *cracks* de la Policía del mundo y aunque sean unos cracks, nosotros tampoco estamos tan mal, incluso podemos aprender de ellos pero también podemos enseñarles. Así que os animo a todos los que estáis.

Intervención en sala.

La verdad es que después de lo que has dicho tienes toda la razón y estamos de acuerdo. Lo de liderar es complicado, nosotros entramos siempre como socios, normalmente vamos a poner de media, cada cinco proyectos añadimos uno más pero nada más, es un tema en el que la gente no quiere implicarse y nosotros lo que hacemos es medir el nivel de implicación de las unidades. Nos cuesta mucho implicar a las unidades. Es decir, vamos a medir en qué quieres participar, cuál es tu interés dentro del proyecto, léete los paquetes de trabajo y dices en qué paquete te interesa participar, cuánto te interesa participar, en cuáles te interesa participar. Nos vamos midiendo con ellos de forma que sean ellos los que elijan: la cantidad de personas y de horas de trabajo que van a implicar en cada proyecto, porque eso está medido. Se nos han dado casos como el proyecto que ha mencionado Maite esta mañana, ABC4EU, en el que se nos vino dado todo y hemos tenido que justificar casi cuatro mil horas de trabajo; eso es una auténtica burrada. Estamos hablando de que lo normal en un proyecto en el que participamos, sea una justificación de ochocientas, novecientas horas de trabajo. Ese tipo de cosas ahora las medimos mucho y también es la forma de implicarles. Y si ellos toman la decisión de en qué parte del proyecto se van a meter, ellos son los que dan el primer paso para la responsabilidad. En ese sentido, entramos siempre como socios y, evidentemente, la segunda parte, lo de liderar, yo he estado liderando un proyecto a medias y, sinceramente, acabé hasta un poco deprimido; porque fueron tres meses de mi vida, veinticuatro horas al día; con unos niveles de estrés importantes, porque de repente los israelitas desa-

parecen, los alemanes se van de vacaciones una semana antes de presentar los papeles... Ejercer el papel de líder, echando la bronca a gente que se supone que son responsables, me resulta bastante molesto. Por eso, acabé estresado, y en la segunda fase que es Broadway hemos cambiado los papeles, vamos aprendiendo. Liderar es complicado, hay que tener ganas.

Interviene: Maite Boyero Egido

Rematando el tema de liderar, yo solo recomendaría liderar a una Administración pública cuando sea un tema estratégico, clave y básico para el funcionamiento de su día a día, de otra forma el liderazgo es tremendo y uno acaba como dice Pepe, estresado, deprimido y, además, el tema es que el que coordina tiene que tener control del tiempo; si el proyecto se presenta hoy, tenemos que tener la garantía de que ese señor o señora, se queda cinco años ahí, no va a abandonar el barco a la mitad. En la Administración pública, a veces, no se puede garantizar. En ese caso, no se coordina, y tiene que haber un apoyo desde el nivel más alto de la Dirección General.

Por mi experiencia, en los proyectos que he presentado los beneficios son plausibles en cuanto al acceso a tecnología, a prototipos, a valorar demostraciones reales, que eso funciona o no; modular que lo que se ha aprobado ahí se basa en lo que yo he dicho y se lo voy a comprar después, porque sé que me va a dar garantías, pero otro no lo voy a comprar y todo esto pagado por la Unión Europea. Por lo tanto, valoremos que nos van a hacer desarrollar tecnología para lo que nosotros necesitemos y de alguna forma, las empresas como necesitan usuarios, facilitan la vida a estas unidades para desarrollar la tecnología *ad hoc*. Es muy positivo en la parte de proyectos.

Cuarto panel: futuras oportunidades para la policía nacional en i+d+i

IDENTIFICACIÓN AUTOMÁTICA DE PERFILES ANÓNIMOS EN REDES SOCIALES MEDIANTE TÉCNICAS DE BIGDATA PARA RECONOCIMIENTO SEMÁNTICO

CASIMIRO NEVADO SANTANO
Inspector del Cuerpo Nacional de Policía

Agradecer a todos los miembros de la Fundación Policía Española no solo el hecho de haberme invitado hoy a presentar el premio que ganamos hace tres años, sino por el trabajo que hacen todos de poder hacer jornadas como esta, poder sacar adelante becas para gente, que investiguen miembros del cuerpo, que es muy importante para todos y, por supuesto, por el premio, que incentiva la labor de investigación que podamos tener los miembros del Cuerpo Nacional de Policía.

Han pasado ya tres años desde la concesión del premio, tres años, dicho así, parece que no es mucho tiempo, pero es que utilizar magnitudes clásicas para medir el tiempo, ya no son válidas. Tenemos que hablar de que han pasado tres modelos de iPhone distintos desde que ganamos el premio. Entonces, esto marca mucho la distancia; entre esos tres modelos anteriores de un iPhone con su procesador, al actual que tenemos y que se presentará dentro de un par de meses.

Nuestro título del trabajo era bastante largo "Identificación automática de perfiles anónimos en redes sociales mediante técnicas de BigData para reconocimiento semántico". Me gustaría destacar cuatro o cinco términos de este título para intentar hacer ver que no íbamos mal encaminados hace tres años teniendo en cuenta hacia donde se dirigen las investigaciones y el desarrollo de la tecnología. Identificación automática, automatismos, inteligencia artificial, perfiles anónimos, perfilado, redes sociales, redes, todo está

en las redes; técnicas de BigData, el que no hable de BigData no gana absolutamente nada y reconocimiento semántico o reconocimiento facial, … y que está ligado con el tema de la identificación y de los perfiles anónimos.

De estas expresiones me gustaría destacar sobre todo la de perfiles anónimos. Qué problema principal nos encontramos nosotros en el ciberespacio? El problema principal no es que nos ataquen, es que nos ataquen y no nos enteremos. Eso es mucho más grave de que nos ataquen. Si logramos enterarnos de que nos han atacado, el siguiente problema que vamos a tener va a ser es el de la atribución. No vamos a saber quién nos ha atacado, quién ha cometido una ciberacción en el espacio y que haya atacado nuestra institución, nuestra empresa, …

El problema de la atribución es muy grave, y es lo que nosotros queríamos solucionar con el tema de la identificación de perfiles anónimos en redes sociales. Como en cualquier otro campo de la investigación de la Policía, estamos buscando la aguja en un pajar y eso es complicado. Y, cuando sacas el tema de la identificación, de la atribución, de la identidad personal que podamos llegar a tener un día en la red, que ahora mismo no la tenemos, se están estudiando varias formas de lograrlo, seguramente conocen el tema del *blockchain*; pues, cuando en un foro hablas de identificación y previamente te has identificado como Policía lo primero que piensa la gente es que vamos a cortar sus libertades, que les vamos a tener controlados, que vamos a saber en todo momento dónde están, que vamos a tener cámaras en las calles, que os vehículos van a tener cámaras, … Y, todo para lograr conseguir una atribución y decir : estas personas son las que han cometido esta acción en el ciberespacio, en las redes, …

Imagen 1

Por supuesto, nos vamos a escandalizar y vamos a ver cosas en la prensa como las de la imagen 1. La dystopian en la sociedad china, y hemos visto, seguramente todos, las grabaciones, los videos de como se van moviendo los ciudadanos chinos, como los tienen controlados, como son capaces de reconocer, como son capaces de hacer toda la ruta que han hecho durante todo un día, semana, mes, totalmente controlado. Y esto, nos da miedo. Es identificación, es automatismo, es hacia donde va el desarrollo de la tecnología.

Es coartar las libertades de las personas, ya no responderé yo a esa pregunta porque entraríamos en el problema de la seguridad y la intimidad y son derechos que, por supuesto, están al mismo nivel.

Todos nos imaginamos, por tanto, situaciones como estas (D-7). Y si se lo hacen a ciudadanos chinos nos parece mal, pero si nos lo hacen a nosotros nos parece peor ¿Nos lo están haciendo ya? ¿Hay ciudades europeas que lo están haciendo ya? Por ejemplo, el metro de Londres ¿Se hace ya? Se es capaz de identificar a una persona que va por el metro de Londres a través de los metadatos de su dispositivo, móvil, conectado al wifi del metro de Londres ¿Se es capaz de reproducir la ruta que ha hecho una persona a través del metro de Londres? Yo lo dejo ahí y no voy a decir ni que sí ni que no. Lo que está claro es que el tema de la identificación es muy importante, es importantísimo que todas las empresas que están dispuestas a pagar lo que sea para averiguar quién ha sido el que le ha robado la información estratégica de su desarrollo.

Cualquier Estado quiere averiguar qué otro Estado ha sido el que ha entrado en sus redes informáticas, el problema de atribución es muy grave. Por supuesto, es absolutamente necesario desarrollar técnicas de inteligencia artificial porque no vamos a encontrar ninguna persona que sea capaz de estar monitorizando cien mil monitores a la vez, es imposible, entonces habrán desarrollado en China inteligencia artificial que sea capaz de identificar y de atribuir cualquier acción, aunque se haya cometido a una persona o ciudadano en concreto. Esto nos da miedo porque si vemos imágenes, vemos reportajes, vemos videos; el nivel de identificación es asombroso y el nivel de control de movimientos también. Absolutamente cada detalle, cada longitud, el peso, los gestos que hacemos… Cuando hablamos de personas hablamos de vehículos, de cualquier recorrido que se haya hecho por la ciudad …Y, por supuesto, nos va a salir esta imagen que posiblemente sea la más famosa de todas cuando hablamos de inteligencia artificial y monitorización y atribución de cualquier acto que se pueda cometer en las calles o en el ciberespacio (Imagen 2)

Imagen 2

¿La Policía tiene que tender hacia esto? Pues no lo se, posteriormente el representante de la logística nos dirá si algún día tendremos esas gafas tan chulas como las de la diapositiva y nuestros patrullas sean capaces de llevar equipos portátiles avanzados.

Lo que sí está claro es que nos escandalizamos mucho, nuestra sociedad se escandaliza, cuando ve cosas como estas y salen artículos como este (Imagen3), presionando Amazon porque ha puesto a disposición de la Policía de su país la tecnología de reconocimiento facial. Y la gente se escandaliza porque la Policía puede tener acceso a una tecnología de identificación fácil cuando verdaderamente nos tendríamos que escandalizar porque el que la

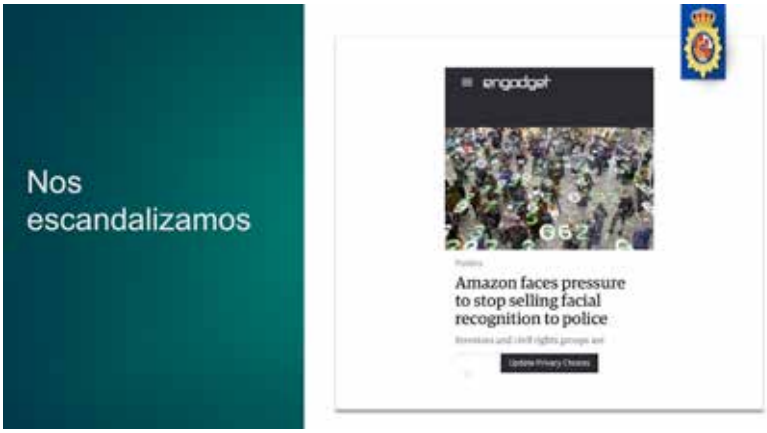


Imagen 3

tenga sea una empresa privada y que es Amazon ¿Por qué nos escandaliza que Amazon se lo ceda a la Policía que es una institución pública, pagada con dinero público que representa a la sociedad y que va a defender a la

sociedad; y no nos escandaliza que esa tecnología la utilice Amazon que es una empresa privada que se debe a sus accionistas principalmente? Esto es lo raro, el tema de la atribución e identificación, las empresas punteras, las tres grandes empresas tecnológicas son las que van en cabeza. Google sabe lo que buscamos, Facebook como somos, nos identificamos nosotros a través del Facebook y Amazon sabe cuales son nuestros intereses, sabe lo que queremos comprar y sabe el número de nuestra tarjeta de crédito principalmente. Si unen estas tres circunstancias, estamos absolutamente identificados pero, en cambio, nos escandaliza que la Policía nos pueda poner una etiqueta en una cámara en una red social, etc.

La intimidad es importante, por supuesto, fundamental, todos queremos tener intimidad, sobre todo en ese escenario. Si fuese todo trasparente la convivencia sería mucho más complicada. Pero una cosa no esta reñida con la otra, por supuesto que el anonimato es un derecho, pero el anonimato está bien cuando es el gatito que se esconde debajo de la piel del lobo (Imagen 4), pero cuando es al revés, cuando es el lobo el que simula ser un gato ¿está

Imagen 4

bien el anonimato o ya no nos parece también el anonimato y queremos elevar la cuota de porcentaje de importancia de la seguridad? Esa es la discusión, nadie discute que el anonimato es un derecho pero claro, pasamos de ser una sociedad totalmente infantil cuando nos muestran una imagen como esta (Imagen 5) y nos dicen que nos va a atacar las hackeres rusos, y

Imagen 5

vemos a un chaval con un portátil y su capucha. Y esto, ya, nos da miedo y queremos que predomine la seguridad sobre la intimidad. Es importante, creo yo, la identificación y etiquetar las cosas que suceden en el ciberespacio igual que sucede en la vida analógica, porque nos podemos encontrar cosas como estas (Imagen 6). Piezas creadas a través de una impresora 3D de un arma de guerra, totalmente funcional. Y este arma no tiene ningún tipo de registro y lo puede hacer cualquiera en su casa si tiene un poco de dinero para comprar una impresora 3D.

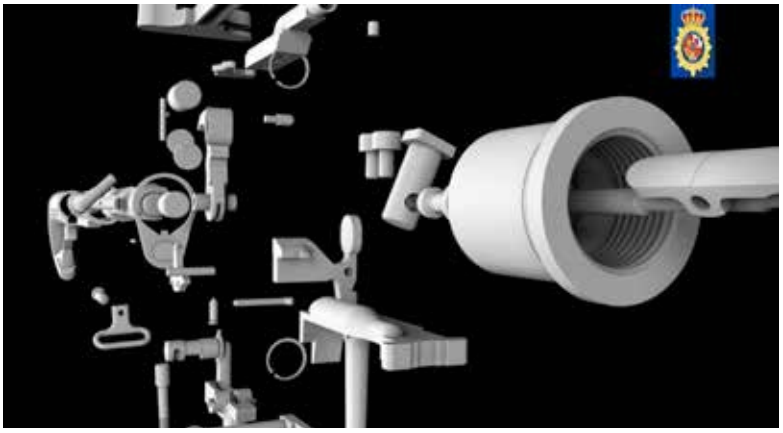


Imagen 6

¿Nos interesaría tener identificadas todas las armas por el bien de la sociedad o preferimos el anonimato y que cualquiera pueda imprimir un arma totalmente funcional y la pueda tener en su casa y utilizarla? ¿qué nos conviene más? Estamos hablando de seguridad de intimidad de anonimato, sí o no, es esa la cuestión. Con una impresora 3D, que tampoco cuesta mucho dinero, podemos crearnos un arsenal; y ya se lo han creado estas personas (Imagen 7). Estas personas acaban de ganar una sentencia en Estados Unidos

Imagen 7

que les ha dado la razón y pueden vender todos los prototipos que quieran y los formatos CAD por Internet para que cualquiera pueda imprimir el arma en su casa. La justicia americana les ha dicho que sí pueden, que tienen ese derecho y que pueden comercializar ese proyecto. Cualquiera podrá pagar por un formato CAD descargárselo y su impresora 3D podrá imprimir el fusil que hemos visto en la diapositiva. De hecho, ya la tienen, por tanto, es importante etiquetar lo que sucede en el ciberespacio igual que etiquetamos lo que sucede en la vida analógica en nuestra calles. Yo creo que es fundamental, sobre todo por el hecho de atribuir algo a alguien, es decir necesitamos saber quién es el que ha cometido esa acción porque sino no vamos a poder tomar medidas y, sobre todo, no vamos a poder retirar de la circulación a esa persona. Y, sobre todo, vamos a jugar a un juego que me gusta mucho a mí que es el de encontrar al humano, porque ¿cuál es el porcentaje de automatismo, de inteligencia artificial, que tenemos ahora mismo circulando por el ciberespacio, por las redes? bastante menos del que vamos a tener esta tarde o mañana. Y vamos a intentar encontrar detrás de todas esas tecnologías, de todas esas acciones, en el ciberespacio, quién es el humano que está manejando todo.

Este es un artículo que ha salido hace poco de las granjas de Bosch en China que han demostrado que, aparte de tener voz digital tienen voz humana, y son los que están manejando al final los miles y miles de teléfonos móviles, cada uno con sus perfiles en redes sociales que crean estaciones en el ciberespacio (Imagen 8).

Imagen 8

Tenemos un proyecto con la Universidad Autónoma de Madrid, cuyo representante Álvaro de Ortigosa formaba parte del grupo con el que ganamos el premio, en el que estamos intentando reconocer cuál es el comportamiento humano detrás de cualquier robot automatizado. Y, lo que estamos

intentando hacer es encontrar a la chinita esta, que está en la diapositiva, que tiene miles de teléfonos y los está manejando. Podemos saber, podemos encontrar un patrón que nos determine que detrás de esos teléfonos, de esas cuentas automatizadas hay una persona, hay un ser humano que lo está utilizando. Yo creo que sí, es mucho más fácil saber, por lo menos saber, dónde está esa persona; sabemos que esos robots los están utilizando en la granja "x" en una ciudad de China. Decir que ha sido esa persona, ya va a ser más complicado. Llegar a intentar que esa persona lo haga, es complicado.

Son muchas las imágenes que vamos a ver, vamos a creer que tenemos perfiles en redes sociales donde todo el mundo tiene la buena voluntad, igual que nosotros, de contar nuestras vacaciones, lo que hacemos en el trabajo, o el transporte que tomamos o salimos del trabajo, etc. Y, vemos que un amplio porcentaje de cuentas en redes sociales son falsas, están automatizadas, hoy Twitter implementa una tecnología que va a reducir las cuentas anónimas, y ayer publicó un mensaje diciendo que todos veremos afectados nuestro número de seguidores hoy, porque va a eliminar este tipo de cuentas anónimas. Veremos si es efectivo o no.

Es muy importante etiquetar, etiquetar una acción, una persona; porque nos va a llevar a poder aprender y poder diseñar, en un tiempo, una inteligencia artificial que será la que finalmente tenga que identificar y detectar esa presencia, esa acción en el ciberespacio. Vemos artículos, como el científico de datos, que la lucha contra el fraude es muy importante por el hecho de detectar y monitorizar el comportamiento de defraudadores en la red.

¿Cuántos atracos se cometía en Madrid en los años ochenta cada día? Creo que bastantes ¿Cuántos se cometen ahora? Prácticamente ninguno, porque es mucho mejor cometer ese atraco a través de la red. Un defraudador va a correr mucho menos riesgo que intentando entrar o defraudar con tarjetas de crédito que cogiendo un revolver y yendo a la sucursal y, por supuesto, va a tener más beneficio a través de la red que entrando en la sucursal con una pistola ¿Cómo vamos a identificar estas acciones? porque no solo va a afectar a una sucursal una acción en el ciberespacio, va a afectar a varias entidades bancarias, que puedan compartir datos, a varios países que comparten el sistema de pago de tarjetas ¿Cómo se identifica eso en tiempo real? porque no es lo mismo acometer y frenar esa acción ahora que dentro de quince segundos, la diferencia puede ser de miles de millones de euros ¿Qué humano es capaz de hacer eso, qué humano va a identificar el patrón de miles y miles de acciones de fraude en quince segundos o diez segundos o en tiempo máquina, real? Pues es imposible, necesitamos nosotros, previamente, identificar y etiquetar lo que es una acción falsa, lo que es un fraude en la red para que una inteligencia artificial pueda aprender eso y lo pueda

detectar en tiempo real.Y ya no solamente vamos a ver cosas como lo de las entidades bancarias, los fraudes de tarjetas, etc.

Estamos viendo como en Estados Unidos y en China también se están cometiendo acosos manejando la domótica de una vivienda y no dejando salir a esa persona de casa, por ejemplo. Un pirata informático o la expareja de una señora que accede a través de la red domótica propia de ese domicilio e impide que su expareja salga de la casa ¿Cómo detectamos ese patrón y cómo actuamos en tiempo real? Para acotarlo y centrarnos en el proyecto que presentamos hace tres años, nuestra idea era trasladar todo esto a un campo que es el de las redes sociales virtuales, principalmente Twitter, se puede trasladar a cualquier red social, o a Internet. Estudiábamos la redes sociales virtuales con tecnología actual, o de hace tres años basándonos en los estudios del análisis de redes sociales clásicos y trasladándolo al análisis de redes virtuales. Nuestro propósito era identificar a la persona que está dentro de esa red. Cuando hablábamos del análisis de redes sociales nos vienen cosas a la cabeza como esta (Imagen 9) Un grafo con nodos y con relaciones. Yo doy clases de análisis y lo primero que te piden los alumnos es aprender a

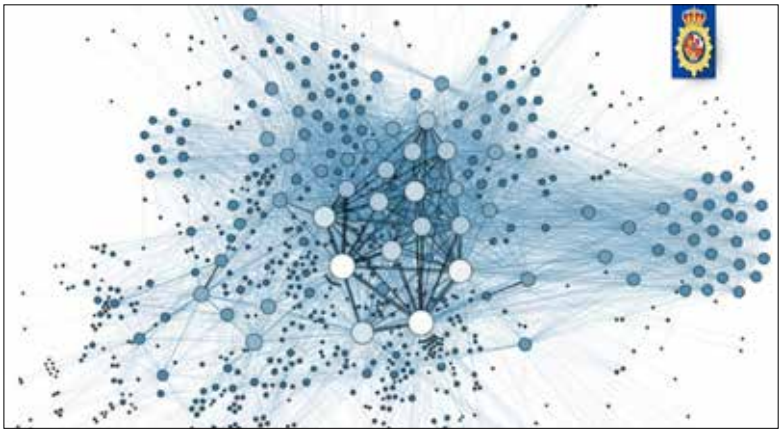


Imagen 9

hacer una cosa como esa, y a lo mejor esto es lo menos importante de todo, porque tener un informe de inteligencia en el que nos dicen que la comunidad que utiliza esta etiqueta dentro del Twitter es muy amplia como se ve en la imagen ¿de qué nos sirve a nosotros eso? ¿Qué nos quiere decir eso? Lo importante es intentar averiguar dentro de esa red de nodos: cuáles son los nodos que nos interesan, cuáles son los nodos que están movilizando al resto de la red, cuáles son los que están pasando la información, cuáles tienen una centralidad en la red mucho mayor que otros, cuáles son los que están difundiendo propaganda. Eso es lo que nos interesa en un análisis de redes sociales.

Nosotros llegamos a ese punto y vimos que al final los nodos que estaban haciendo eso eran cosas como estas (Imagen 10). El huevo de Twitter. El malo es malo pero no es tonto, se esconde detrás de una máscara y qué mejor máscara que en Twitter que tener una cuenta absolutamente anonimizada, sin foto y sin ningún dato, unas cuentas como estas (Imagen 11) con nombres inventados.

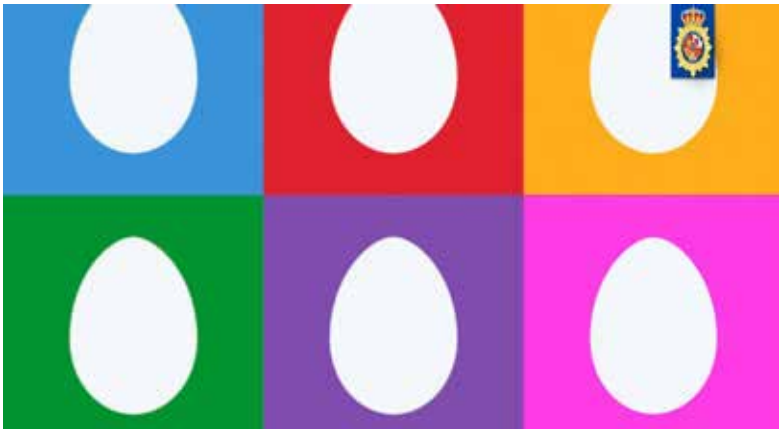


Imagen 10

Imagen 11

Ya sabemos que este nodo, este perfil de Twitter está movilizando y está cometiendo tal acción, y ahora qué hacemos con él si no sabemos como se llama, y si se llama "meng fan 316" ¿Cómo actuamos ahora? ¿Se lo decimos a Twitter? Twitter no nos va a hacer caso; y ya no solo para temas como los que pueden ser los trols. Me están acosando en Twitter, son trols, son perfiles anónimos … Nos encontramos con situaciones en que la expareja está acosando a su exmujer a través de las redes sociales y lo está haciendo con perfiles anónimos ¿Cómo podemos nosotros atribuir esa acción de un perfil

anónimo a un perfil con nombre y apellidos y DNI? Esa era la cuestión que planteábamos nosotros.

Con los miembros de la UFAM, les trasladamos el proyecto, la aplicación que desarrollábamos y, en principio, la idea era utilizarlo para identificar en los casos de acoso en las redes sociales, de víctimas de violencia de género que estaban siendo acosadas por exparejas a través de perfiles anónimos. Pero, también se implementó, por ejemplo, en el I3 de información, porque el que está difundiendo una determinada ideología no lo hace con su nombre y apellidos, lo hace con una identidad supuesta y esto nos puede llegar a determinar que la misma persona que era un combatiente en Siria y regresó a España y en Siria tenía una cuenta en la que publicaba fotografías suyas, en la batalla, es la misma que ahora se ha cambiado de nombre y está escribiendo en Twitter, con otro nombre distinto, y está difundiendo propaganda. Podemos asimilarlo con la tecnología que desarrollamos en esta aplicación.

También, se pueden detectar acciones en el ciberespacio simulando aplicaciones informáticas, aplicaciones móviles que realmente lo que están haciendo es monitorizando tu actividad en un teléfono móvil. Los soldados israelíes se descargan aplicaciones de contactos y de seguimiento del mundial de futbol que había creado, supuestamente, una organización como Hamás. Pero cómo llegan a condicionarte a ti, para que te descargues esa aplicación, pues lo hacen a través de redes sociales simulando un acercamiento y que son otro tipo de persona para conseguir convencer que se descargue la aplicación en su móvil. No deja de ser el esquema clásico de ataque de intrusión suave; yo canalizo tu perfil y que lo estás publicando todo en Twitter, una vez que tengo analizado tu perfil voy a crear un perfil falso que se pueda asimilar a tus gustos, a tus intereses, etc. Y una vez que tengo ese perfil falso me pongo en contacto con este, voy a desarrollar una amistad y voy a lograr convencerte de que tú, ejecutivo de la empresa más importante de España, o soldado del ejército israelí, te descargues esta aplicación y lo que realmente te está haciendo es monitorizar tu actividad real en el móvil.

Esto no se va a poder evitar como se hacía antes el poner una muralla en nuestro sistema informático y que ahí no entre nadie, eso ya no se puede hacer, porque, además, no conviene al modelo de negocio actual de las tecnológicas ¿Qué se está haciendo ahora? Se levantan las murallas y se deja pasar a todo el mundo a tus propios sistemas, lo que tienes que ser es precavido y capaz de monitorizar las personas, los perfiles, los individuos que se están moviendo en tu red, la gente que está dentro de tu ciudad, eso es lo importante. No puedes evitar que la gente entre en tu red, lo que tienes que saber es qué gente está entrando y qué está haciendo en cada momento. Y eso, solo se hace monitorizando y con perfiles y etc.

Estamos viendo en la *face new,* quién está difundiendo este tipo de información y que tanto daño puede hacer en sociedades como la India que se están cometiendo asesinatos por culpa de los bulos que se están difundiendo ¿sucederá eso algún día en España, se cometerán asesinatos porque se ha difundido algún bulo que afecte a alguna organización, algún grupo social en concreto y se vea atacado y se quiera defender? Pues no lo sabemos.

Al final, lo que tenemos que hacer es identificar siempre a una persona y atribuirle una acción ¿Qué nos planteamos nosotros para intentar darle una solución? Que cuando yo cojo un teléfono, cojo otro, hablo de la misma manera con este teléfono que con otro. Pues nosotros creíamos que sí, que no cambiamos el tono de voz y eso lo trasladamos a las redes sociales. Porque en estas se pueden simular muchas cosas pero tu forma de expresarte y de escribir no la puedes simular. Tu vas a colocar siempre tus expresiones, tus palabras de una determinada manera; y eso, se puede averiguar y es muy difícil de simular, lo hagas con un perfil tuyo o lo hagas con otro perfil anónimo. Siempre vas a utilizar las mismas expresiones y vas a escribir de la misma manera.

Desarrollamos con una serie de tecnología que es libre y se puede acceder, y métodos de bolsa de palabras para comparar textos en base a vectores y convertirlos en vectores, un sistema que por cada palabra genera un vector y lo coloca en una gráfica. Somos capaces de colocar en un mismo vector palabras que semánticamente están relacionadas como en el caso, por ejemplo, del país con su capital. Vemos que comparten vector. Esta tecnología lo que hace es analizar esas palabras y las va relacionando. Es importante porque se puede utilizar para cualquier tipo de idioma: para castellano o para inglés. Nos va a colocar en el mismo vector las mismas palabras que están relacionadas semánticamente. Pero esto no nos permite identificar a la persona que ha hecho un texto. Entonces, tuvimos que dar un paso más y mediante la tecnología que desarrolló Google y que no es accesible pero que sí existe una versión que sí lo es podemos atribuir un vector y no solo a una palabra, sino a un texto determinado y entonces, ya podemos comparar palabras y textos, y ya tenemos distintas funcionalidades como la de comparar un texto que escribe una persona en redes sociales con otras redes sociales u otros perfiles. Búsquedas verticales, en las mismas redes sociales, vamos a comparar distintos perfiles y si escriben igual. Búsquedas horizontales, en distintas redes sociales; y búsquedas paralelas, nos sirven para identificar personas que están hablando sobre una misma cosa.

Resultado, pues teníamos cosas como esta, una simple búsqueda es por ejemplo, probando con el perfil de @policía, veíamos que nos devolvía un informe la aplicación en la quinta posición nos identificaba a Carolina, hasta

hace unos días la *Community manager* de la Policía, como que era una persona que escribía exactamente igual que el perfil de Policía y, efectivamente, Carolina no puede simular cuando escribe en el perfil de @policía, que cuando escribe en el suyo personal, una forma de escribir, unas expresiones que no utiliza. Es totalmente artificial y no nos sale. Esta herramienta es capaz de identificar esto.

Perfiles relacionados con el yihadismo, vemos que tantos perfiles se pueden resumir en dos, y la aplicación nos devuelve un porcentaje bastante alto cero nueve, cero diez, cero once de similitud entre varios perfiles; y de ocho o diez perfiles que tenemos los podemos reducir a dos.

También utilizamos indicadores de similitud como puede ser: cojo el móvil y voy a publicar en mi perfil personal, y ya que estoy, voy a publicar en mi perfil falso. Entonces se veía una correlación temporal entre la publicación del perfil artificial y el perfil real, era una suma más. Y, por supuesto, utilizábamos los meta datos, no hasta el nivel de una investigación que se publicó hace unas semanas, en la que se afirma que se puede identificar a una persona por los meta datos de sus redes sociales al noventa y nueve coma nueve por ciento de fiabilidad. Pero utilizábamos también los meta datos.

Al final no dejan de ser todo indicios y todo se tiene que documentar y basar en el atestado policial, y el juez lo tendrá que valorar como cualquier otro indicio; pero sí estamos intentando, nos estamos acercando a la atribución que estamos buscando detrás de esa máscara que es el anonimato y que se puede encontrar en las redes sociales.

No me gustaría terminar sin llamar la atención sobre una cosa que está relacionada con todo esto que estamos hablando. Estamos viendo que las empresas punteras están desarrollando sus propios microchips para sus propias aplicaciones y su propio harward. Apple, Huawei, Samsung …, incluso Facebook quiere implementar sus propios chips para las redes sociales para inteligencia artificial ¿Qué quiere decir esto? Que la guerra en el ciberespacio es tan enorme que nadie se fía de nada. Aquella empresa o institución que no se crea capaz de desarrollar su propia tecnología va a depender de terceros y de la buena voluntad de estos. Nos van a vender una tecnología muy cara y no sabemos lo que se esconde detrás de esta tecnología, porque perfectamente puede tener una puerta trasera y esa empresa nos está obteniendo todos los datos de la Policía y nosotros no nos estamos enterando. Porque lo hemos comprado y nos fiamos de la palabra de una persona de una empresa; y la empresa, al final, mira por sus accionistas y por sus intereses. Es muy importante desarrollar proyectos y desarrollar tecnología y no esperar a que venga una empresa a vendernos algo, sino nosotros teniendo

nuestras propias ideas, desarrollar esas ideas y colaborar con universidades o empresas y saber, en todo momento, lo que se está haciendo y evitar que nos implementen una puerta trasera en cualquier tecnología.

TURNO DE PREGUNTAS

Pregunta en sala: José Francisco López, Jefe del servicio de innovación de logística. Quería hacer un comentario respecto a los aspectos éticos. Realmente la preocupación por los aspectos éticos y todo lo relativo a I+D no es que sea creciente es que es una condición de legibilidad absoluta. Todos los proyectos que se están haciendo ahora mismo a nivel europeo y se intentan hacer a nivel nacional, incluso deberíamos tenerlo en cuenta, y se ha nombrado a nivel de la Policía, deberían de tener un componente de aspecto ético altísimo, ético legal, llamémoslo como queramos pero teniendo en cuenta la ética detrás. Incluso se está intentando dar un paso más que es incorporar a la sociedad civil dentro de los proyectos de I+D en tema de seguridad. El aspecto ético es muy importante, el comentario que hacías respecto a que nos están monitorizando, lo de los chinos va a llegar aquí. Realmente la sociedad va hacia eso, si no ha llegado ya, los centros comerciales nos monitorizan desde que entramos en ellos, desde que entras por la puerta ya tienen captado tu teléfono y están captando dónde te paras, porque es la forma en la que luego van a cobrar más de alquiler a esa parte del centro comercial. Si juntaran eso con las cámaras que tienen y tuvieran un sistema de reconocimiento facial perfectamente nos tendrían monitorizados, e identificados también, si quieren; pero monitorizados seguro que sí. Me refiero a esto por una cosa muy sencilla, a nivel europeo, por ejemplo, la Policía de Alemania tiene grandes problemas para aplicar sistemas de reconocimiento automático de placas de matrícula. En cambio, en el Reino Unido tanto los sistemas de reconocimiento facial como de placas de matrícula lo tienen totalmente automatizado y centralizado en todo el Reino Unido. Cada sociedad va a un nivel diferente. Es difícil saber si esto se va a conseguir dentro de España dentro de unos años. Realmente ¿no existe una fórmula de identificar a alguien anonimizado en DARK WEB ?

Responde: Casimiro Nevado

Es complicado atribuir a una determinada persona, pero identificar un patrón, un comportamiento, sí lo puedes identificar; puedes intentar atajar ese comportamiento, ese patrón, pero identificar, atribuir la identidad de qué persona está realizando ese patrón en DAR Web, a mí, no me preocuparía tanto la DAR Web, porque hay tantas investigaciones analizando la DAR Web que dentro de poco, a este ritmo, encontramos una solución; a mí me preocupa más, por ejemplo, el DAR Internet, ese sí es más complicado. Cómo acceder a una red que no está dentro de Internet ¿sabemos diferenciar entre Dar Web y Dar Internet?, porque si nos conectamos todos nuestros móviles con Bluetooth y apagamos el resto de conexiones, hemos creado una red igual que puede ser Internet, y nos estamos pasando información y ¿cómo entramos ahí? La única solución es el modelo clásico, infil-

trar a alguien dentro de esa red, porque, evidentemente, cualquier terrorista sabe que ahora mismo, las fuerzas y cuerpos de seguridad están intentando monitorizar y patrullar la Dar Web y a lo mejor va a ser mucho más precavido, y va a crear su propia red o te va a hacer la propia acción en Internet superficial, porque esa es otra posibilidad también.

Hay una corriente de pensamiento dentro de Internet, dentro de esta temática, que dice que si tu utilizas aplicaciones encriptadas llamas mucho más la atención que si lo hablas públicamente. Y yo estoy de acuerdo con eso. Si la Policía entra en un registro y se encuentra mil pendrives y solamente uno de ellos tiene un teclado para meter la clave de acceso ¿cuál va a ser el primer pendrives al que va a analizar la Policía?, fijo que el del teclado. Entonces, ya estamos llamando la atención. Pero si tienes un millón de pendrives ¿vas a tener tiempo para analizar un millón de pendrives? Hay gente que utiliza las redes sociales sin ni siquiera captar ese perfil, sin poner el candado de Twitter, para emitir mensajes, publicar mensajes; y te lo están haciendo en la cara pero de una manera que pasan desapercibidos, dentro de toda esta magnitud de información que podamos ver en Internet. Me preocupan más estas opciones, el Dar Internet que la Dar Web aunque esta también es importante.

SISTEMAS OLFATIVOS ARTIFICIALES PARA LA DETECCIÓN DE AGENTES PELIGROSOS

JOSÉ MIGUEL SÁNCHEZ ESPAÑA
Inspector del CNP, Jefe del Tedax de Badajoz

Dicen que una imagen vale más que mil palabras (Imagen 1). Como verán son dos recortes de prensa, una de EL PAIS, un recorte de la secta Aum Shinrikyo cuando atentó con gas sarín, en el metro de Tokio, un lunes 20 de marzo del año 1995, con resultado de doce muertos y miles de heridos. Y el otro recorte es el ataque químico en Duma de abril de este año 2018, la cual tendría que modificar pues parece ser que cuando ha ido la OPAQ (Organización para la Prohibición de Armas Químicas), han confirmado que efectivamente no había gas sarín en el ataque. Se analizaron más de cien


EL PAIS

Los 'siete grandes' no abordarán la crisis monetaria hasta abril

Un atentado con gas letal siembra el pánico en el metro de Tokio

Ataque químico en Duma deja decenas de muertos y causa indignación

Según un vídeo difundido anoche por los "cascos blancos" algunas de las víctimas mortales echaban espuma por la boca y padecían cianosis, una coloración azulada de la piel que se produce por falta de oxígeno.

Imagen 1

muestras tanto en víctimas como en hospitales y muestras que se recogieron en el escenario y en ningún caso se descubrió que había sarín. En cualquier caso el recorte de prensa me servía para decir que es un tema de actualidad y no solo de ahora sino desde 1995 e incluso anterior el ataque con agentes de naturaleza NRBQ-E que significa: nuclear, radiológico, biológico y químico y también con explosivos.

La última incidencia con explosivos es la que pasó más recientemente en agosto del año 2017 (Imagen 2) en Alcanar Platja (Tarragona), imagen que muestra como quedó la casa de Alcanar donde tenían pensado fabricar más de doscientos cincuenta kilos de TATP. El TATP (triperóxido de triacetona) es un explosivo improvisado, artesanal, que se hace con productos que se pueden adquirir en un comercio, y así es como quedó el piso.

Imagen 2

Si no hubiera explosionado el TATP, habrían cometido un atentado mucho mayor que lo que al final hicieron que fue una cosa a la desesperada, cogieron las furgonetas y atropellaron gente, cuando la idea inicial era meter el TATP en la furgoneta y atentar con ella. También, se recuperaron más de ciento cincuenta bombonas de butano que tenían como objetivo aumentar todavía más los efectos de la explosión del TATP.

En cualquier caso lo que quiero demostrar con estas imágenes es la necesidad que tiene no solo la Unión Europea, sino también a nivel internacional, de poder contar con detectores o identificadores de este tipo de sustancias ya sea, como digo, NRBQ o de explosivos.

En este sentido, ahora hablo como Jefe de Grupo de los TEDAX-NRBQ de Badajoz de lo que tenemos en la especialidad. Veremos los detectores con

los que cuenta la especialidad y luego los mejores del mercado. Son detectores, el de la izquierda es un detector químico y el de la derecha, también es un detector químico, hablo de detector químico no de explosivo, sino de sustancias químicas. Como la propia palabra indica dice detector y no identificador, con lo cual, lo que te detecta es una sustancia química. No te dice qué sustancia química es ¿Pero qué es lo que existe actualmente en el mercado? Los detectores que poseemos en dotación rondan los tres mil o cuatro mil euros.

Imagen 3

Son tecnologías caras, son tecnologías de análisis químico. Entre los mejores detectores que existen en el mercado (Imagen 3) se encuentran el FirstDefender y el True Defender; digamos que son detectores más caros porque están basados en una tecnología más cara, otro tipo de técnica de análisis químico más potente, el precio de estos aparatos rondan los treinta mil euros. Estos te identifican sustancias químicas, explosivos, sustancias narcóticas…, de ahí que el precio sea también mayor pues no sólo detectan sino que también identifican. Imaginemos que tenemos que dotar a todas las unidades del Tedax de este tipo de detectores, supone un desembolso económico importante a nivel de empresa privada y a nivel de institución pública es complicado.

Aquí planteamos lo que es el sistema olfativo artificial (Imagen 4) o nariz electrónica. ¿Qué es lo que se trata con esto? Simular el funcionamiento de

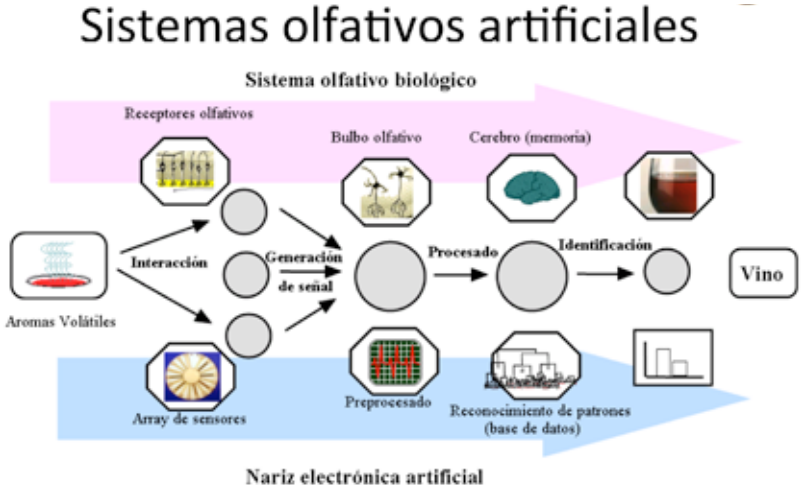


Imagen 4

la nariz biológica del ser humano o de un perro a la electrónica. En un principio lo que se tiene es el olor, ese olor en el caso de la nariz humana o de un perro, pasa a los receptores olfativos, interacciona con esos receptores, se genera una señal; esa señal cuando llega al bulbo olfativo, se almacena en forma de recuerdo en el cerebro, y se identifica, en este caso, por ejemplo, vino.

Similitud entre la nariz biológica y la nariz electrónica, en vez de receptores olfativos hablamos de array de sensores como los que tenemos, por ejemplo, en un parquin para los detectores de gases. Estos arrays de sensores cuando llega la sustancia volátil se genera una señal eléctrica, esa señal se procesa y mediante un reconocimiento de patrones se obtiene al final una señal que se identificará con la sustancia en concreto, en este caso sería vino.

El funcionamiento es el mismo y el entrenamiento, lógicamente, como podéis imaginar, es también necesario. Pensemos en los catadores profesionales de vino. Si ahora mismo a mí, me ponen un montón de vinos para catar, no sabría distinguir un vino de otro, pero si llamamos a un catador, este sí los distinguiría. Es decir, la pregunta es si él huele mejor que yo, o simplemente tiene la nariz más entrenada ¿Qué hacemos con la nariz electrónica? Exactamente lo mismo ¿Cómo lo hacemos? Haciendo un montón de medidas

Cuando hacemos muchas medidas, por ejemplo, con sustancias químicas, explosivas, cincuenta medidas con amoniaco, cincuenta con cloro, cincuenta con acetona; le decimos al sistema: cuando te dé esta señal es amoniaco, cuando te dé esta otra es acetona y cuando te dé esta es explosivo. Esto viene resumiendo muy someramente lo que es la nariz electrónica (Imagen 5). Los compuestos volátiles llegan a la nariz biológica y electrónica -fíjense en el tamaño de la electrónica-, una vez que se detecta se transmite vía inalámbrica bien por wifi o por radio frecuencia o Bluetooth a un móvil o a un dispositivo portátil como puede ser una tablet o un ordenador.

Imagen 5

¿Cuáles son las partes que tiene una nariz electrónica? (Imagen 6) Básicamente, el olor, esa muestra que tiene un olor, que desprende un olor; se extrae mediante un sistema de extracción de aroma que sería la primera parte, ese aroma se hace llegar a los sensores, sensores de gases; se genera una señal eléctrica, se mide, se obtienen unos datos, se procesan esos datos y mediante técnicas de reconocimiento de patrones se clasifican e identifica. Te dice si es un explosivo o si es una sustancia química. Se trata de reducir unos datos a otro conjunto de datos pero ya clasificados.

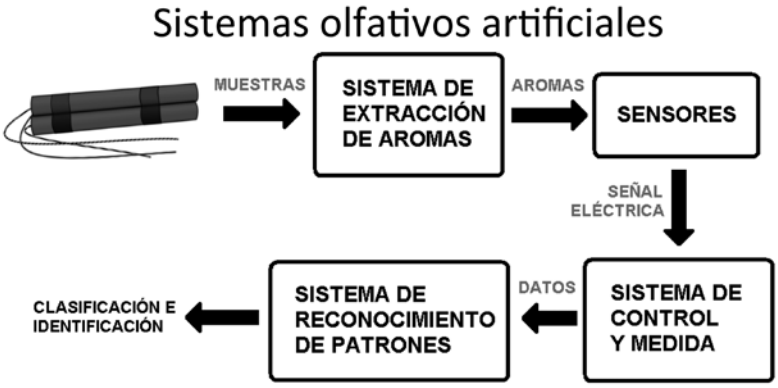


Imagen 6

Dispositivos desarrollados: el primero es el Winose (nariz electrónica inalámbrica) (Imagen 7). Básicamente tiene estas partes: una entrada de aire con un filtro de carbón, por un lado entra el aire y por otro la muestra que queremos analizar, bien de un explosivo o de una sustancia química. La electroválvula le permite el paso hacia el interior del sistema donde se encuentran los sensores y donde se generará la señal, luego se obtienen unos datos y a continuación se procesan esos datos y se identifica la sustancia en cuestión.

Imagen 7

Otro dispositivo que se ha desarrollado (Imagen 8), el anterior era por wifi mediante una antena que transmitía a un ordenador. Este es igual pero en vez de ser la transmisión por Wifi, es por Bluetooth y puede ir conectado a un móvil, es decir, yo no necesito acercarme a la sustancia en concreto para determinar qué tipo de sustancia es; puedo llevar, por ejemplo, la nariz al sitio, bien con un dron o robot o incluso lo puedo llevar en la mano a modo de dispositivo portátil. Y, ese dispositivo mediante Bluetooth me envía la información que ha obtenido a un móvil. Yo estoy aquí y el aparato está allí midiendo, con lo cual, eso da mucha seguridad al interviniente. Para los Tedax es muy importante no acercarse al peligro, con lo cual ahí ganamos ya bastante; y si encima sabemos a lo que nos vamos a enfrentar, ya sabemos qué nivel de protección podemos utilizar; si se puede o no respirar, según nivel de oxígeno detectado, es decir, una serie de información muy útil y necesaria para saber cómo afrontar la intervención.

Este es el tamaño del dispositivo (Imagen 8). Es prácticamente el tamaño de una tarjeta, cuadrada, de sesenta por sesenta milímetros, con lo cual, si comparamos los detectores que son comerciales y que pesan algunos más de medio kilogramo y que tienen un volumen considerable, pues no se concibe acoplarlos a un dron. Sin embargo, esto es una plaquita, muy fina, pesa poco, lo puedes acoplar a un dron, a un robot, con lo cual, aumentamos las ventajas. Aparte, estas técnicas no tienen nada que ver con las técnicas de análisis químico, lo que hemos visto antes de los detectores comerciales es análisis químico puro y duro, basado en tecnologías de análisis químico muy caras que encarecen mucho el producto, desde los tres mil euros para que me detecten la sustancia a los más de treinta mil si queremos que a su vez la identifique. Los componentes que conformarían la nariz electrónica rondan: veinte euros la placa, diez euros cada sensor; con lo cual, ganamos bastante

Imagen 8

en precio y, luego aparte, lo podemos configurar como nosotros queramos con el entrenamiento adecuado.

Esto es la base de funcionamiento, (Imagen 9) lo más importante realmente; porque si no fuera por esto no funcionaría el aparato. Es una técnica adaptada al análisis matemático que es el análisis de componentes principales, básicamente es: tenemos muchos datos, imagínense una nariz electrónica con muchos sensores (ocho por ejemplo), cada sensor tiene una tecnología diferente. Por cada medida que haga voy a obtener ocho señales, una por cada uno de los sensores. Cómo llevo todas esas señales que obtengo en un espacio multidimensional y las convierto en un espacio bidimensional, es decir, de dos dimensiones, de forma que pueda ver esa información que tenía proyectada a modo de puntos agrupados en un plano. Con lo cual, reduciendo la dimensionalidad de estos datos, puedo ver en un plano, que esos

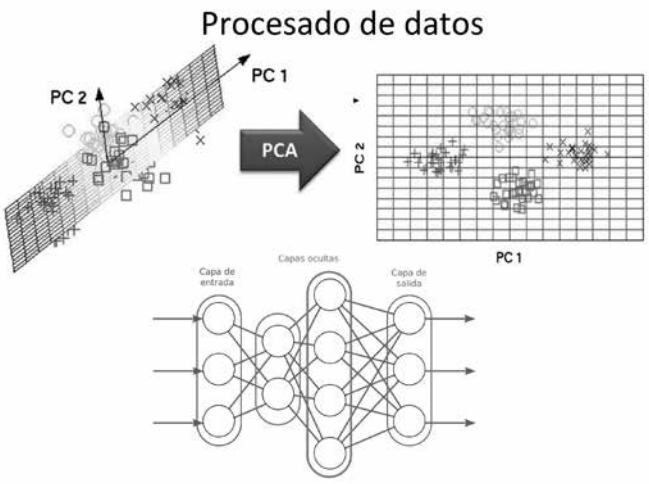


Imagen 9

puntos según estén agrupados de una forma u otra se corresponden con una sustancia en concreto; otro conjunto de puntos agrupados se corresponde con esta otra sustancia, que será distinta a la anterior y así sucesivamente. Y, ahora, le digo a la nariz electrónica cuando te dé por esa zona será cloro, cuando te dé por esa otra zona será acetona…

Este paso es lo que representa la Imagen 9 en la zona inferior, que son redes neuronales artificiales. Esto tiene una arquitectura con una capa de entrada que suelen ser señales de entrada y una capa de salida que son las señales de salida ¿Qué es lo que es la entrada? La señal que nos viene de los sensores de gases ¿Qué es lo que representa la salida? La categorización que yo le hago, podemos decir, voy a ponerle tres salidas de forma que una

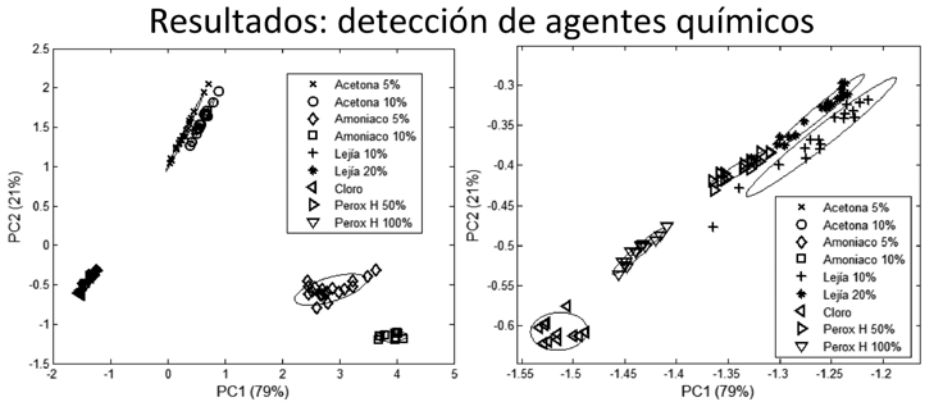


Imagen 10

salida me diga que es riesgo alto, otro medio y otro bajo. O digo, no, quiero que en vez de decirme riesgo alto, medio o bajo, me diga que es dinamita, pentrita o amoniaco, es decir puedo definir las salidas como yo quiera. Por tanto la arquitectura de la red que yo maneje es según lo que yo busque ¿A mí me interesa que identifique cinco sustancias, las más normales y cinco explosivos? Pues pongo diez salidas.

Resultados obtenidos (Imagen 10) con agentes químicos, estos son resultados reales obtenidos con la nariz electrónica inalámbrica WiNose que antes presentamos. ¿Qué es lo que vemos en la diapositiva? Acetona al cinco por ciento, acetona al diez por ciento,... Incluso dentro de una misma sustancia me puede identificar y diferenciar la concentración que tiene esa sustancia. Pero también me diferencia la acetona de lo que es el amoniaco. Incluso en zonas que parece que hay solapamiento lo que podemos hacer es ampliar la señal y se puede ver que incluso dentro de ese solapamiento cada cosa está por un lado; si todo lo juntáramos, diríamos que esta técnica no discrimina, igual que cuando nos viene el olor a la nariz nosotros tenemos una señal distinta cuando es amoniaco que cuando es acetona, con esta nariz electrónica nos está diciendo que la señal que obtiene es distinta cuando es una sustancia que cuando es otra y tiene, por lo tanto, poder discriminante, con lo cual, la técnica a priori es buena para diferenciar sustancias químicas.

Resultados obtenidos con explosivos y que tenemos en dotación (Imagen 11), dinamita, PG2, pentrita y pólvora, como se puede ver en la diapositiva, también me ha distinguido los diferentes explosivos. Si añadimos un poco más de dificultad, vamos a probar con los explosivos que se están utilizando actualmente por los terroristas yihadistas TATP, HMTD, que es lo que está de moda (Imagen 12). Pues incluso los diferenciaba mejor, pues estos explosivos improvisados desprendían incluso más olor que los industriales. Y efectivamente, es lo que nos confirmó la técnica. En la imagen 12

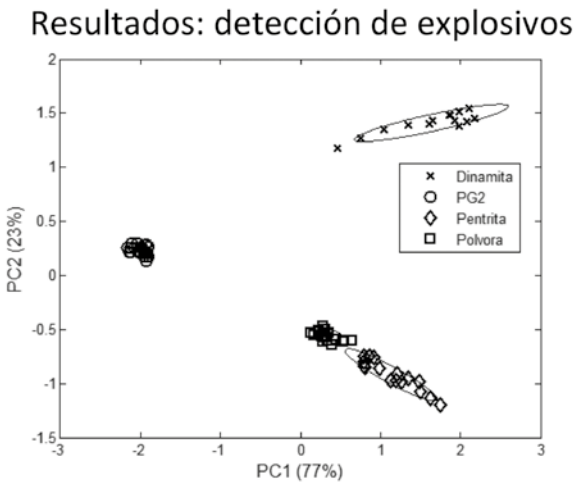


Imagen 11

tenemos lo que es el TATP y el HMTD. Se puede observar en la imagen que distingue mejor estas sustancias que el resto de explosivos vistos, con lo cual, la técnica también vale para identificar explosivos. Se trata de hacer muchas medidas y decirle a la nariz esta señal se corresponde con esta sustancia, esta otra señal con esta otra,…De modo que la idea es que una vez se obtiene una señal de salida mediante las redes neuronales artificiales, una programación y unos algoritmos adecuados se pueda obtener en la pantalla de un móvil, tableta u ordenador de mi casa, información acerca de la sustancia que pudiera haber sido identificada en un control en un aeropuerto donde se haya implantado este dispositivo o nariz electrónica.

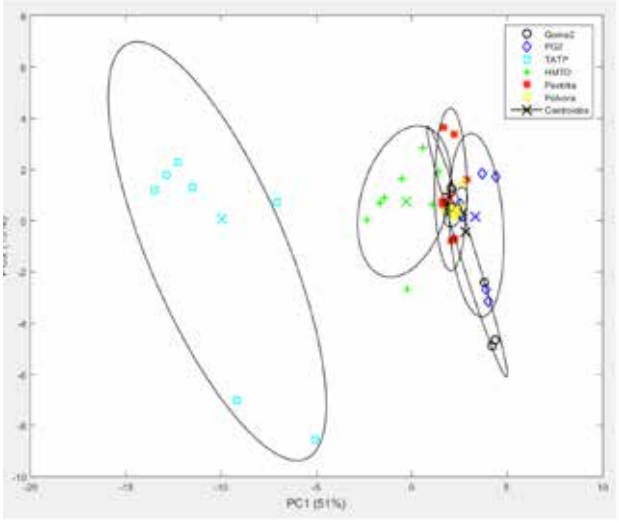


Imagen 12

CONCLUSIONES

Surge la necesidad de que haya un dispositivo que detecte agentes químicos y explosivos, que sean de bajo precio y pequeño tamaño, para que pueda ser acoplado a un dron o a un robot, que no pese mucho y que tenga una precisión aceptable. También hemos visto la posibilidad que se nos ofrece con este prototipo de trabajar a distancia mediante transmisión de datos vía inalámbrica. Este dispositivo permite detectar la sustancia en concreto y yo puedo estar en mi casa y mi móvil me muestra que se acaba de detectar acetona. Pensemos en la aplicación que podría tener en un control de pasajeros en aeropuerto. Hace unos días, cuando fui al extranjero, me pasaron unos papelitos en las manos y en el cinturón que luego pasaron a una máquina (máquina que cuesta más de cien mil euros). Una técnica de análisis químico que se denomina espectrometría de movilidad iónica y que, cuando se estropea hay que cambiarlo, hay que llamar a un técnico… Nuestro prototipo es más sencillo y más barato. Si se estropea no es lo mismo que se estropee un aparato que cuesta quinientos euros u otro que te cuesta treinta mil euros; o uno del aeropuerto que te cueste más de cincuenta mil euros.

¿Qué vamos a iniciar este año? Debería de haber comenzado mi exposición dando las gracias a la Fundación Policía Española por permitirnos estar aquí, hoy, y por habernos dado el primer premio el año 2017. Y también, darles las gracias por incentivar la investigación dentro de la Policía con becas, con conferencias como esta,… Acabamos de solicitar una beca y la idea es que este año 2018 podamos hacer pruebas con este sistema pero, en vez de realizarla con explosivos y agentes químicos, nos gustaría hacerlas con cocaína, heroína, es decir con droga. Sobre todo, por los resultados que puedan obtenerse en la aplicación en las unidades caninas, sobre todo, cuando pasan sus perros por un coche, por una persona que ha estado en contacto con hachís, en el caleteo de coches que ocultan droga e incluso en barcos, camiones, contenedores…

TURNO DE PREGUNTAS

Pregunta en sala: José María Cervera. Comisario provincial de Badajoz

Veo que las ayudas son muy poquitas y con bajo presupuesto, si el foro es ideal para que nos acerquemos a este baile de miles de millones que llevo toda la semana escuchando de los fondos europeos que son como setas que han crecido y están pidiendo que nos acerquemos a recogerlas, por lo tanto, vamos a buscar los sitios apropiados para podernos acercar.

Me interesa que me digas que esto no le pasa como al perro que a lo mejor tiene un día malo, pocas ganas de trabajar… Esto lo podemos aplicar constantemente, me imagino.

Responde: José Miguel Sánchez

Efectivamente, se han destinado dos millones de euros en el séptimo programa marco, antiguo, reciente Horizonte 2020, para técnicas de detección e identificación en el ámbito de NRBQ como de explosivos a nivel de la Unión Europea. Me consta también de que en este nuevo Horizonte 2020 hay uno de los puntos que destina unos catorce millones de euros para el campo y detección de identificación de explosivos en el tema de posibles atentados terroristas que recurran al uso de estas sustancias a nivel europeo. Estaremos pendientes, ya nos estamos informando a través de la universidad y veremos cómo se puede conseguir algo de eso.

En relación al asunto de los perros, efectivamente la nariz de los perros se satura y no solo eso, puede que tenga un mal día y no detecte o no identifique o incluso que no tenga ganas de sentarse o que se distraiga porque huele otra cosa que le llama la atención; incluso los errores que puedan tener. Yo antes estaba en la unidad de drogas y sí que se va algo cuando algún perro ese día no está bien y a lo mejor hay drogas y el perro no tiene ganas de sentarse. Se distrae porque ha olido algo por ahí o una perrilla que este cerca y al final se distrae.

En cuanto a la nariz electrónica, esta no se distrae, no se satura, sí que es cierto que lo que tienen bueno los perros es que la sensibilidad que tienen es que llega hasta partes por trillón, digamos que hay partes por millón, billón y por trillón que es lo más sensible. Con la nariz electrónica se ha llegado también a detectar partes por billón y trillón, depende lógicamente de lo que emane la sustancia en cuestión. La nariz electrónica no se plantea como un sustituto del perro sino como algo complementario. Todo lo que sea sumar es mejor, es garantía e incluso dentro de lo que es el campo de las narices electrónicas, hablamos de detección y hablamos de identificación pero hay que tener el respaldo de un laboratorio que es el que diga que efectivamente

qué sustancia es de la que se trata. Yo puedo tener una primera detección provisional, llamémosla como queramos, una vez que la detección es confirmada utilizamos una o dos tecnologías pero, tiene que ser un laboratorio acreditado el que diga que esa sustancia efectivamente es lo que es. A la hora de usar perros la seguridad del mismo puede estar en entredicho si lo que pretendemos es que nos detecte una sustancia tóxica, ya sea amoniaco o cloro, cosa que no sucede si usamos la nariz electrónica. El hecho de pensar en el uso del perro como algo complementario sería si hablamos de detección de drogas y de explosivos pero no así en aquellos casos en los que se comprometa la seguridad del perro, lo cual es una ventaja de la nariz frente a los canes pues no estamos limitados en cuanto a la sustancia a detectar. Pero en cualquier caso tiene que haber un laboratorio acreditado que sea el que me diga que lo que me ha detectado en un primer lugar la nariz electrónica es amoniaco, y eso es lo que va a valer de prueba de cargo, judicial. La detección/identificación que me hace la nariz in situ no la podré utilizar como prueba ante un juzgado sino que me valdrá operativamente para saber a qué sustancia es a la que nos estamos enfrentando.

Pregunta en sala: Juan Carlos Castro, Comisario General de Seguridad Ciudadana ¿Por qué esto no suple al perro? ¿Por qué, en lugar de ser complementario no podemos quedarnos con esto que con un perro?

Responde: José Miguel Sánchez

El prototipo está en fase de desarrollo, si en un futuro una vez terminado, se ve que funciona perfectamente, de momento con todo lo que lo estamos probando funciona, pero por otro lado aunque esté en fase de desarrollo lo que se trata es de sumar. Si tengo un perro que lo puedo usar en el ámbito de drogas o de explosivos, no así en el caso de que lo que tenga sea un agente químico, porque con un agente químico tipo sarín o amoniaco o cloro, no voy a mandar al perro, aquí la idea del perro no tiene ningún sentido, pero en los casos como en el tema de drogas o explosivos, si el perro se sienta y encima la nariz electrónica me dice qué es lo que es, tengo doble confirmación. Por tanto con la doble confirmación tendríamos una mayor seguridad a la hora de intervenir llegado el caso. Digamos que no se trata tampoco de eliminar la especialidad de caninos, porque la especialidad de caninos tiene su significado y su sentido, por lo tanto se trata de sumar.

Interviene: Juan Carlos Castro

Yo tampoco tengo ningún interés en eliminar las Unidades de Guías Caninos, pero a la hora de sumar, en el ámbito policial, entiendo que si tenemos un instrumento con el cual podemos llegar a la misma conclusión que con el perro, y además es seguramente más barato, podríamos plantearnos la sustitución. Porque tampoco hablamos con el perro para ver si tiene un

buen día, normalmente, sí que es cierto que en temas de explosivos actuamos con dos perros para contar con una segunda opinión.

Yo creo que es perfectamente válido en el caso del TATP, que nos cuesta un dineral, y que es un explosivo muy inestable que nos crea muchas complicaciones para el entrenamiento de los canes. Hay otras muchas más especialidades, como la detección de billetes de curso legal o la localización de personas ocultas, en las que me da la impresión que eso siempre debe oler a lo mismo. Si calculáramos lo que cuesta el desarrollo de la nariz artificial y que desconozco, y lo comparamos con lo que nos cuesta la especialidad de guías caninos para según qué cosas, porque también necesitamos un perro que meta miedo y que muerda y esto no lo suple este prototipo, quizás llegáramos a la conclusión de que podríamos reducir este tipo de Unidades o cambiar la orientación de algunos servicios.

Responde: José Miguel Sánchez

Simplemente añadir que sí, efectivamente, le tengo que dar la razón que la tecnología es barata, de hecho he comentado antes que lo que es la placa electrónica vale veinte euros y los sensores valen diez o quince euros. Lo que aquí realmente tiene el peso es el software de programación, lo que es la parte electrónica. Pero hablando con los ingenieros han comentado que lo que es el precio de la parte del aparato una vez montado no superan los setecientos euros. Los detectores en el mercado que tenemos actualmente que equivaldrían también a medidas de narcóticos, explosivos y agentes químicos, hablamos de más de treinta mil euros. Y en relación a lo que me ha comentado de los perros, es verdad que la nariz electrónica se puede entrenar para lo que sea, han catado cerveza, han catado vino; sanitariamente se utiliza para detección de la colitis ulcerosa y de la enfermedad de Crohn a través del análisis de heces, se ve si esa persona sufre o padece esa enfermedad porque por lo visto en las heces detecta una sustancia que es indicativo de este tipo de enfermedades. Incluso en los frigoríficos, en las neveras, te puede advertir mediante un mensaje a tu móvil si existe algo que está malo porque ha detectado que se está descomponiendo algo en el frigorífico y estamos de vacaciones y sabemos que la nevera nos ha dejado de funcionar, o sea, aplicaciones tiene muchas; lo que hay que hacer es encontrar tiempo y gente que pueda hacer medidas, que tenga ganas y con un equipo en condiciones. El proyecto horizonte 2020 plantea cosas a nivel más grande que supone ya la intervención de algún que otro país, que haya equipos multidisciplinarios, más gente dedicada íntegramente a esto, ahora mismo lo que nos estamos dedicando a esto somos dos ingenieros y yo, en nuestro tiempo libre y lo que estaría bien sería el tener a alguien que pudiera hacer muchas medidas.

Interviene: Juan Carlos Castro

No sé cuantos perros tenemos, pero un montón, pero claro es que el perro tiene un guía, el guía vale, termino medio, cuarenta mil euros al año, se puede poner malo, tiene vacaciones … y, luego el perro que puede tener un mal día; es decir, solamente por eso, merece la pena intentarlo.

INNOVACIONES TECNOLÓGICAS EN VIGILANCIAS Y SEGUIMIENTOS

JOSÉ ANTONIO CEBRIÁN DE BARRIO
Inspector Jefe del Cuerpo Navional de Policía

Me gustaría tratar de definir qué es el I+D+i, porque la verdad no tengo ni idea qué es la I+D+i. Ya en los años sesenta un ingeniero dijo que los transistores crecerían exponencialmente cada dos años. En esos años un transistor costaba cientos de dólares, actualmente ha salido un microchip que lleva integrados treinta mil millones de transistores y cuesta apenas nada ¿Qué significa esto? La innovación es algo que crece exponencialmente y desde el punto de vista del Cuerpo Nacional de Policía tenemos que continuar apoyándola y estar constantemente al tanto de las nuevas tecnologías.

¿Qué es la jefatura de sistemas especiales? Es una unidad que está formada por dos servicios, el de seguimientos electrónicos y el de sistemas electrónicos. Posteriormente se decidió crear una sección que se dedicara a buscar dentro del mercado primeramente relaciones y después el material que iba a necesitar la Policía Nacional para apoyar las investigaciones. Pero, no solamente dentro de las jefatura de sistemas especiales, como veremos más adelante, es una labor que trata de buscar nuevas tecnologías para cualquier unidad policial.

Las funciones de sistemas especiales son funciones de desarrollo y de aplicación de equipos técnicos ¿Por qué tengo que hacer mención a la Jefatura central de logística e innovación? Me parece un acierto que hace unos años decidieron crear el servicio de innovación y desarrollo ¿Qué problema le veo? que están profundamente centrados en proyectos europeos H2020 y hay una gran dispersión, vamos a llamarles "frikis" dentro de la Policía, que se están dedicando a hacer una labor de investigación y desarrollo pero que no tienen conexión entre ellos. De alguna forma, este departamento, el ser-

vicio de innovación y desarrollo debería integrar también o tratar de unir a todas esas personas que están dispersas.

¿Es le I+D en términos económicos una inversión segura a largo plazo? ¿Qué problema tiene España? España es el décimo país en publicaciones científicas, pero a nivel de desarrollo de I+D ocupa el puesto treinta y cuatro, treinta y cinco, o treinta y seis. Esto significa que muchos de los desarrollos científicos que se producen en nuestro país acaban en el archivo vertical ¿Por qué es una inversión segura? Los países más desarrollados son: Japón, Suecia, Finlandia, Suiza,Dinamarca, Estados Unidos … Y son los países que más dinero invierten en I+D pero, a la vez, son los países que más renta per cápita por habitante tienen ¿Dónde está España? Durante muchos años la inversión de I+D en España ha ido decreciendo y, por lo tanto, es muy difícil que un país avance si no hacemos inversión en I+D. Si lo ponemos en relación con que es el décimo país en publicaciones significa que en este país hay gente que vale muchísimo pero, por lo que sea, no se le deja trabajar; consecuencia: lo que todos conocemos como fuga de cerebros.

¿Cómo tenemos que ver el I+D dentro de la Policía? Esas dos palabras que hace poco me las inventé haciendo un trabajo y que se relaciona con la teoría del puzzle. El I+D hay que verlo desde un punto de vista global, tenemos que ser capaces de tener una visión desde arriba y ver todos los desarrollos que hay y ponerlos en común. Luego lo tenemos en el reconocimiento facial, y en el reconocimiento facial hay muchas unidades en la Policía que están interesadas en ello.

¿Qué es lo que han hecho estas unidades de Policía? Cada una de ellas ver los diferentes sistemas por separado y al final decir: a mí me gusta esta y a mí me gusta eso. Económicamente eso es inasumible. De alguna forma si cada uno de nosotros o cada uno de los departamentos o personas que nos dedicamos al desarrollo tecnológico, somos una ficha que solo nos permite ver nuestra pequeña ficha, si fuéramos capaces de unirlas todas, al final, veríamos una imagen, bonita, fea, la que sea; pero vamos a ser capaces de ver algo que es totalmente imposible de ver si cada uno de nosotros vamos por separado.

¿Cuál es la teoría de la biblioteca y aplicable a todos los rangos en esta vida? La información, la información dispersa no vale para nada, los desarrollos tecnológicos dispersos no valen nada. Imaginemos que cada desarrollo tecnológico es un libro y los vamos almacenando; si somos incapaces de hacer un índice o de poner en relación esos libros unos con otros, al cabo del año tenemos que quemar la biblioteca y empezar de cero porque seríamos incapaces de saber que es lo que hay almacenado, o si nos acordáramos de

algo seríamos incapaces de saber dónde lo hemos dejado; con lo cual, hay que tratar de tener una visión global, tenemos que ver a la Policía desde arriba y pensar en qué necesita tecnológicamente para poder apoyar a sus operativos.

Cuando afrontamos un proyecto en Policía Nacional, independientemente de que haya gente que individualmente tiene unos conocimientos espectaculares, no podemos tener, por ejemplo, un Policía programando porque todo su trabajo se va a basar en programación. ¿Qué es lo que tenemos que tratar de hacer para formar gente como directores de proyectos? Lo que tenemos que hacer es formar gente como directores de proyectos, que sean capaces de ver qué necesidades tiene la Policía Nacional y, a partir de esas necesidades, ser capaz de hacer *networking* con otras unidades policiales, con otras fuerzas y cuerpos de seguridad y con entidades externas, universidades, etc. Por ejemplo, hace unos días un inspector de la jefatura estuvo con un *spin-off* de la universidad de Vigo, ha vuelto alucinado ¿Qué se necesita para esto? Estar dispuesto a que la gente se dedique, en exclusiva, a estos temas.

¿Se requiere mucha gente? No, porque no hablamos de equipos que desarrollen un producto, estamos hablando de gente que sea capaz de dirigir un proyecto, de saber qué es lo que necesitamos y ponerse en contacto con los que realmente son capaces de desarrollarlo y, a partir de ahí, empezar a desarrollar proyectos. Y, sobre todo, saber muy bien si un proyecto puede implicar a otras unidades policiales, es fundamental ponerse en contacto con ellas, principalmente para ahorrar costes. Si este triángulo deja de ser equilátero y es una relación entre tres variables, tiempo, coste y alcance, el proyecto va a terminar fracasando sí o sí.

¿Qué se ha hecho en la jefatura de sistemas especiales durante los últimos años? Vamos a hablar de un proyecto de reconocimiento facial, un proyecto sobre drones en Policía Nacional, contra drones y otros. Todos estos proyectos no se los ha quedado la jefatura de sistemas especiales, la jefatura empezó a trabajar con ellos, reconocimiento facial se empezó a trabajar junto a la UPAC de comisaría general de información UAV se empezó en el año 2008 en la jefatura de sistema especiales, este año 2018 ha pasado a depender del servicio de medios aéreos. Se empezaron a estudiar sistemas contra drones en el año 2015 y el año 2017 pasaron a depender del área de telecomunicaciones. Se trabaja para toda la Policía Nacional, no solo para sistemas especiales.

En cuanto al sistema facial, lo primero que se hizo fue empezar a distinguir la detección facial. Generalmente, las imágenes se sacan de frente, con lo cual se tiene un software asociado que nos permite hacer artificialmente

una rotación de cara hasta treinta grados. Todas las caras se almacenan en base de datos con lo cual ya tenemos un *macht* para comparar y, a partir de ese momento, ya diferenciamos lo que es reconocimiento, identificación de una cara con lo que es el reconocimiento facial, comunicándonos que ha sido identificada esa persona con una de las personas que están en la base de datos y nos da una probabilidad de que sea esa persona. Hemos probado todo tipo de sistemas y, realmente, mientras seamos capaces de ver ojos y nariz, estos sistemas funcionan ¿Qué problema tienen estos sistemas? Necesitan mucha calidad de imagen, actualmente tiene que ser muy buena y, como toda nueva tecnología, el índice de falsas alarmas es todavía alto.

En cuanto a los drones, una de las cosas que quería resaltar de la Policía Nacional es que en determinados aspectos hemos sido pioneros y determinadas tecnologías con las que trabaja Policía Nacional aún habiendo sido pionera, no ha tenido la repercusión mediática que hubieran tenido en otras fuerzas y cuerpos de seguridad del Estado. Es hacer un llamamiento a nuestros jefes para que determinadas tecnologías, en las que hemos sido pioneros les saquemos el rédito necesario. Con los drones, la jefatura de sistemas especiales, en el año 2008, tuvo el primer dron en España de aplicación policial. Desde el punto de vista militar ya tenían unos anteriormente pero Policía Nacional en el año 2008 empieza a trabajar con drones. Desde entonces ha sido un campo que ha tenido un crecimiento tan exponencial y actualmente se hacen tal número de trabajos que las competencias las ha tenido que asumir el servicio de medios aéreos. Es imposible dar respuesta a todos los requerimientos que hay.

Desde el punto de vista policial tenemos que hacer uso de los drones desde dos puntos de vista. Como usuarios, es más fácil buscar qué unidad policial no los va a necesitar y, como Policía, llamémosle "administrativa", tratando de evitar el uso mal intencionado de los drones. El primer dron con el que se trabajó era un helicóptero, tenía una longitud de un metro y medio (1,5) y el rotor uno coma ocho (1,8) metros, en esos momentos era una auténtica maravilla, la calidad de la imagen era bastante regular y tenía una antena que iba persiguiendo permanentemente al helicóptero fuera donde fuera y con esto se empezaron a hacer las primeras misiones de reconocimiento.

En la actualidad debe de haber unas quince plataformas, se ha montado una furgoneta con diferentes antenas para poder hacer el seguimiento de las diferentes aeronaves y en el año 2017 se llegaron a hacer aproximadamente doscientos vuelos. En este sentido, desde la Secretaría de Estado de Seguridad, desde la subdirección se está con el proyecto Surveiron integrado por Guardia Civil y Policía Nacional el cual se va a basar en una plataforma inteligente de control de drones. Aquí, rompemos con el concepto que es el

operador con el mando, viendo el dron y manejándolo, algo que por la legislación actual va a tener que continuar siendo así, pero lo que se hace es un auténtico centro de control a nivel nacional donde se van a poder controlar todas las operaciones de drones que se produzcan en España y esto tiene su seguimiento en el sistema contra drones.

Medidas contra drones, fue el siguiente paso que se inició en el año 2014; desde la jefatura se mandó una noticia informativa a la antigua DAO comunicando de los peligros que podían tener estas nuevas tecnologías y su uso mal intencionado. A partir de ese momento se creó en Secretaría de Estado de Seguridad, una mesa de trabajo integrado por Casa Real, Presidencia del Gobierno, Cenepit, Guardia Civil y Policía Nacional, donde se empezaron a buscar medidas contra drones. Se definió que había que tener una detección, una identificación y una neutralización como pasos fundamentales; ser capaces de hacer un seguimiento y, sobre todo, una inteligencia que nos permitiera discriminar entre falsas alarmas y las no falsas alarmas. Dentro de esto hay cientos de tecnologías diferentes y ¿qué es lo que se hizo? ir probando todas estas tecnologías. Problema que tiene, por ejemplo, Indra por el sistema antidron pide más de medio millón de euros. Hay tantas infraestructuras que proteger que es inasumible gastar tanto dinero, con lo cual iniciamos unos test, hicimos las típicas combinaciones de sistema binario y, a partir de ahí, se estudiaron los diferentes comportamientos que tenían los drones cuando inhibíamos cualquiera de las señales. Desde entonces, podemos ver la señal de un dron y cuando encendemos, el inhibidor tapa totalmente la señal del dron y, en esos momentos, va a seguir el comportamiento predeterminado por fábrica que sería, o vuelta a casa, o se quedaría estático y terminaría aterrizando caóticamente.

Posteriormente, como sistema de detección se ha visto una maleta que ha sido desarrollada por la propia compañía de DJI; esta vende el 85% de los drones mundiales y detecta sus propios drones. Esto significa que tenemos ya un sistema relativamente barato que es capaz de detectar y de anular drones. Policía Nacional ha sido la primera fuerza de seguridad que ha tenido este sistema. Basado en el informe de Policía Nacional, Casa Real, Presidencia del Gobierno y Guardia Civil, han comprado exactamente el mismo.

Otra de las cosas que se han hecho ha sido el analizar drones que se han caído o que se han intervenido, a partir de esto se conecta la placa de memoria con diferentes software y somos capaces de sacar dónde ha estado volando, recorridos … Y que es competencia de Policía Científica.

Para finalizar, nuevos proyectos ¿Existe el gran hermano? Yo siempre digo lo mismo cuando me dicen que si la Policía es el gran hermano, y siempre

les contesto ¿tú quién te has creído que eres el Príncipe Carlos de Inglaterra para que nos preocupe tu vida? Pues no. ¿Se puede seguir a todo el mundo? Se le puede seguir.

Los teléfonos móviles envían unas cosas que se llaman *pruf request* que sirven para cuando nos conectamos a una red Wifi; la guarda como una red de confianza y está constantemente enviando esas cosas y, judicialmente no es intervención, o sea, se pueden captar esos *request* sin intervención judicial. Es, totalmente legal, estos *pruf request*, nos dan la *mac* del teléfono más los puntos donde se ha conectado. A parte de esto, lo ruters están constantemente enviando *bicons* que es: oye estoy aquí ¿te quieres conectar? Totalmente legal interceptarlos. Si todo esto lo ponemos en contacto y se hace con un ruter normal y corriente poniendo en el ordenador lo que se conoce como en forma promiscuo, somos capaces tras un escaneo de diez segundos de hallar todas estas relaciones entre teléfonos móviles y personas. ¿Qué significa esto? En el mundo hay siete mil millones (7.000M) de habitantes y cinco mil millones (5.000M) de teléfonos móviles.

Si tienen ustedes curiosidad, se van a ajustes Google y dentro de Google van a encontrar una pestaña que se llama anuncios, dentro de esas pestañas se van a encontrar un número que pone su identificación de anuncios es tal, ese es un número único para cada dispositivo que nos han puesto las compañías Google e Iphone y es con lo que consiguen saber dónde estamos en cada momento y mandarnos la publicidad… Y esto es lo que se denomina inteligencia del ambiente

LA POLICÍA CIENTÍFICA DEL CNP, EN LA VANGUARDIA DE LA INVESTIGACIÓN POLICIAL

Mª PILAR ALLUÉ BLASCO
Comisaria Principal del CNP,
Comisaria General de Policía Científica

La Comisaría General de Policía Científica es una de las cinco áreas operativas que integra la recientemente creada Jefatura Central de Investigación, Información y Ciberdelincuencia, definida en el mes de julio de 2017 por el Real Decreto 770. Aunque en el título de la Jefatura Central no se la mencione la Comisaría General de Policía Científica es una de las cinco áreas operativas que la integran, junto con las Comisarías Generales de Información, Policía Judicial, Extranjería y Fronteras y la División de Cooperación Internacional.

Se nos define por ese Real Decreto 770 de 28 de julio de 2017 como *prestadores de servicios de criminalística de identificación de analítica e investigación técnica, así como elaboradores de informes periciales y documentales* que nos sean encomendados, ello quiere decir que además de investigar en nuestro ámbito se hacen informes periciales que, como tales, luego se defienden en sede judicial.

A lo largo de esta intervención cuando hablamos de Comisaría General hay que entender que no nos referimos solo a los servicios centrales radicados en Madrid, sino también a todas las unidades territoriales que se encuentran desplegadas en todo el territorio nacional, estamos hablando de en torno a doscientas unidades del Cuerpo Nacional de Policía, lo que quiere decir que allí donde hay una Comisaría de Policía Nacional o un puesto fronterizo, por ejemplo, hay policías de Policía Científica prestando sus servicios, si bien con responsabilidades de mayor o menor calado en función de las capacidades de la plantilla, su volumen o el tamaño de la co-

misaría, pero en todos los sitios donde hay una Comisaría o un servicio de Policía Nacional, está la Comisaría General de Policía Científica a través de sus unidades territoriales. Estamos hablando de alrededor de unos dos mil ciento dieciséis funcionarios en estos momentos, lo que supone un 84% de la ocupación del catálogo de puestos de trabajo asignado o definido por la Dirección General de la Policía.

De esos dos mil ciento dieciséis funcionarios escasamente unos trescientos cincuenta son los que se encuentran destinados en los servicios centrales de la Comisaría General, situados en un edificio moderno, del año 2009, en el que disponemos de unos veintidós mil quinientos metros cuadrados, de los cuales unos trece mil quinientos aproximadamente están destinados a laboratorios.

La estructura desplegada por todo el territorio nacional alberga además seis laboratorios de ADN en las ciudades de Madrid, Barcelona, Valencia, Granada, Sevilla y A Coruña. Cada uno de esos laboratorios presta servicio a un territorio que va más allá de su provincia y/o región policial, por ejemplo: el de Barcelona despliega su actividad y presta apoyo en el análisis de ADN a la Comunidad de Aragón y a la de Navarra además de a nuestras unidades en Cataluña, o el de Valencia, que además de a las plantillas de la propia Comunidad Valenciana, presta apoyo a la de las Islas Baleares, esto es, cada laboratorio tiene un territorio propio al que responder para hacer los análisis de vestigios biológicos e identificar ADN. En este aspecto hay que destacar que somos el único operador de seguridad en España que tiene este número de laboratorios, lo que implica lógicamente un volumen mucho mayor de respuesta.

¿Cómo funciona la Comisaría General de Policía Científica? El núcleo central lo integran cinco unidades centrales, de las que hablaremos más tarde con un poco más de detalle, radicadas en Madrid en las instalaciones del complejo policial de Canillas, de ellas dependen funcionalmente las unidades territoriales de Policía Científica que, no obstante, dependen orgánicamente de sus respectivos responsables territoriales. La Comisaría General de Policía Científica asume la dirección, el control y la gestión técnica de las unidades territoriales de Policía Científica, y también la responsabilidad de suministrar materiales específicos y el apoyo tecnológico y personal necesario, pero también asume la responsabilidad de la formación, además de impartir doctrina y unificar criterios y procedimientos de actuación, desde las cinco unidades centrales.

¿Cómo se articula esa dependencia funcional con la dependencia orgánica y esa relación que hay entre los servicios centrales y las unidades terri-

toriales? Bajo un principio sencillo y a la vez algo complejo que no es otro que el de la subsidiariedad, que no quiere decir otra cosa que lo que puede hacer el escalón inferior no debe hacerlo el escalón superior. Ahora bien, ese complejo sistema en realidad pivota en torno a un Policía, al que se forma y dota de técnicas y materiales adecuados, el Policía especialista en Policía Científica, que es el que hace las inspecciones oculares en el lugar de los hechos, en el lugar del crimen, aunque lógicamente este Policía no actúa solo, se integra dentro del grupo local en el que también se realizan las tareas de reseña dactilar, se gestiona el Sistema Automático de Identificación Dactilar, así como otras de análisis técnico-científico, en función de las capacidades y del tamaño de la plantilla.

Si como decimos todo el sistema de Policía Científica gira alrededor de un Policía, el especialista, su formación es esencial, de ahí que la preocupación por la misma, y por su actualización constante, quede reflejada en el hecho de que en torno a un 75% de personas (a veces incluso bastantes más) de esas dos mil ciento dieciséis que hemos dicho que integran el área, a lo largo del año pasan por un curso de formación, especialización o perfeccionamiento, en el ámbito de Policía Científica. Hacemos un tremendo esfuerzo de formación en el ámbito de Policía Científica, creo que pocas organizaciones pueden soportar un sistema de formación continua tan potente como el que hemos establecido en Policía Científica junto con el apoyo de la División de Formación.

Sin embargo la fortaleza que nos da el esfuerzo en formación y actualización de nuestro personal, necesario para estar al cabo de la calle de lo que está ocurriendo en el mundo, de las novedades que están aportando la ciencia y la tecnología, para poder elaborar los informes que se nos solicitan con las mayores garantías, ese esfuerzo que supone una gran inversión, no sólo económica sino también en tiempo y recursos humanos, también nos debilita en cierta medida pues no podemos obviar que mientras estamos formando al personal nos siguen solicitando informes periciales, que hay que elaborar siempre sin merma de garantías y además en el menor tiempo posible, por lo que para esto último habría que incrementar sustancialmente el número de personas que se dedican a Policía Científica.

Los servicios centrales que prestan el apoyo a las unidades territoriales además de hacerlo tienen sus competencias propias y también elaboran los informes más complejos, haciendo valer el principio de subsidiariedad del que hablábamos antes, así, por ejemplo:

La Unidad Central de Identificación además de controlar, dirigir y establecer todo lo relacionado con el apoyo y el desarrollo de la reseña dactilar,

de la identificación lofoscópica y el servicio automático de identificación dactilar también asume la competencia de todo lo relacionado con las técnicas de identificación personal especialmente la identificación fisonómica.

En el ámbito de la identificación personal, en un momento en el que los sistemas automáticos de reconocimiento son cada vez más precisos a la hora de identificar entre miles a individuos concretos nadie habla de la persona que hay detrás de la identificación más allá de la máquina, como decía uno de los ponentes anteriores en el caso de las granjas de bots, pero en este caso en sentido contrario ¿Quién hay detrás de esa identificación? Por ejemplo: ¿Quién valida la identificación que ha hecho la máquina? Esto es: ¿Quien es la persona que, en un juzgado, ante un juez, certifica que una persona que aparece en una imagen o en una secuencia de ellas es la misma que la que está frente al estrado judicial? Es importante, por tanto, recordar la condición forense que tienen los trabajos de Policía Científica, una condición que supone su presentación a la luz pública en el foro judicial y su sometimiento, entre otras cosas, a los principios de contradicción, en contraste con los peritos de parte, que tienen que soportar los funcionarios que van como peritos a los juicios. Es cierto pues que las máquinas cada vez hacen más cosas, pero hay que recordar que en el ámbito forense son los peritos de Policía Científica.

En este sentido, especialmente hablando de innovación y desarrollo, hay que recordar que somos la única policía europea que se ha acreditado en el examen y comparación de morfologías faciales visionadas en fotografías y fotogramas. Se puede consultar en la página oficial de ENAC (Entidad Nacional de Acreditación) donde figura que el Servicio Central de Identificación de la Unidad Central de Identificación de la Comisaría General de Policía Científica está acreditado bajo la norma internacional UNE-EN-ISO-IEC 17025 para hacer ese tipo de exámenes, ya que ha demostrado cumplir sus requisitos y exigencias y como tal lleva aparejado que los informes periciales que en esa materia elabora esa unidad central lleven impreso el sello de ENAC certificándolo.

También hay que reseñar que la Unidad Central de Identificación de la Comisaría General de Policía Científica gestiona todo lo relacionado con el Sistema Automático de Identificación dactilar (SAID) materia en la que fuimos pioneros en el mundo al ser la cuarta institución que puso en funcionamiento este sistema, allá por el año 1984, y los primeros en Europa en hacerlo. Destaca también el hecho de que haya sido el Cuerpo Nacional de Policía el que haya aportado aproximadamente el 64% de los datos que contiene la base de datos nacional de huellas dactilares, ahora radicada en la Secretaría de Estado de Seguridad y compartida con la Guardia Civil y las

Policías Autonómicas, a la que la Policía Nacional sigue contribuyendo con más de la mitad de la información que va incorporándose cada año.

Por otro lado, también para hacerse una idea aproximada del trabajo que se desarrolla y gestiona por la Unidad Central de Identificación, podemos poner como ejemplo el hecho de que al cabo del año (en cifras de 2017) en torno a siete mil doscientas personas fueron identificadas como posibles autores de hechos delictivos, gracias a las huellas dactilares o a los estudios fisionómicos.

La Unidad Central de Coordinación Operativa, es la que asume todas las actividades relacionadas con la realización de las inspecciones oculares técnico-policiales y su coordinación nacional, también sobre la reseña fotográfica, la tecnología de la imagen y la elaboración de los informes periciales correspondientes en estas materias. Apoya todos los aspectos técnicos de las unidades territoriales en las materias de su competencia, pero además desarrolla también inspecciones oculares complejas y otras específicas como las relacionadas con materia terrorista. Estamos hablando de un volumen de alrededor de ochenta y ocho mil inspecciones oculares a lo largo del año pasado.

La Unidad Central de Criminalística, es la que gestiona todo lo relacionado con el estudio y la realización de informes periciales en materia de falsificación documental, grafoscopia, balística forense identificativa y operativa, trazas instrumentales, acústica forense, informática forense y de ingeniería forense (éstos últimos son los que hacen los informes periciales en materia de drones). Esta unidad gestiona la realización de unos once mil informes a lo largo del año.

La Unidad Central de Análisis Científicos, es la que gestiona los seis laboratorios de ADN así como los laboratorios químico-toxicológicos de los que disponemos, y gestiona ya solo en el caso de ADN la realización de unos veintitrés mil informes a lo largo del año.

La Unidad Central de Investigación Científica y Técnica, es la que gestiona todo lo relacionado con la materia de calidad, las relaciones internacionales, así como la investigación, la innovación y el desarrollo en las demás unidades, añade un plus a todos los trabajos que hacen el resto de unidades en la medida que gestiona el control de una calidad entendida como el sometimiento a las normas internacionales y a los estándares de calidad que son las que guían el desarrollo del trabajo de policía científica, garantizando la fiabilidad y la transparencia de los resultados que se obtienen.

La implantación de las normas internacionales de calidad como tales, en el ámbito de policía científica, tiene su origen en un imperativo normativo que no es otro que la Decisión Marco 2009/905/JAI del Consejo de la UE de 30 de noviembre de 2009 sobre acreditación de prestadores de servicios forenses que llevan a cabo actividades de laboratorio, la cual obliga a todos los Estados miembros a acreditarse conforme a la Norma UNE-EN-ISO-IEC 17025, lo que debería llevarse a cabo antes del 30 de noviembre de 2013 en el caso de los análisis de perfiles de ADN y antes del 30 de noviembre de 2015 en el ámbito del revelado y cotejo dactiloscópico. La Policía Nacional española, su Policía Científica, ha cumplido en tiempo y forma esas obligaciones y en estos momentos hay treinta y nueve plantillas acreditadas en revelado de huellas, veintidós en cotejo lofoscópico y los seis laboratorios de ADN, además de otras actividades que también se han acreditado como los estudios fisonómicos o de morfologías faciales visionadas en fotografías y fotogramas comentados anteriormente, o como el examen y comparación de huellas palmares, aunque también el estudio y comparación de impresiones de huellas de calzado, y el de elementos balísticos por microscopía óptica, y también la identificación de autores de escritura manuscrita latina y el examen y comparación de firmas manuscritas. Todo ello se ha llevado a cabo no sin notable esfuerzo y además en escaso tiempo, nótese que en el año 2012 ni tan siquiera estaban todos los laboratorios de ADN acreditados como iba a ser obligatorio en noviembre de 2013.

Toda la información relativa a las diferentes acreditaciones de las diferentes organizaciones nacionales y extranjeras se puede consultar en la página web de ENAC, la Entidad Nacional de Acreditación declarada, según el Real Decreto 1715 del año 2010 del Estado español, como el único organismo dotado de potestad pública para otorgar acreditaciones de acuerdo con lo establecido en el Reglamento Europeo (CE) nº 765/2008. En el caso concreto de la Policía Científica del CNP se puede consultar la acreditación Nº 816/LE1757 en cuyo anexo técnico constan los estudios técnicos acreditados y todos los trabajos que se hacen con arreglo a la norma de calidad 17025.

La Unidad Central de Investigación Científica y Técnica también es la que gestiona todo lo referido a las relaciones internacionales, aspecto tremendamente importante de nuestro trabajo pues somos muy conscientes de que estamos en un mundo globalizado y de la necesidad de conocer lo que se investiga y/o se pone en practica en cualquier parte del mundo para poder prestar el servicio adecuado. Por ello, entre otras cuestiones, estamos integrados como uno de los miembros fundadores de la Red Europea de Institutos de Ciencias Forenses (ENFSI por sus siglas en inglés) desde el año 1992, que fue cuando se creó, siendo en estos momentos el organismo

de referencia en materia de ciencias forenses para la Unión Europea. También estamos integrados en los grupos de trabajo de carácter forense de la Organización Internacional de Policía Criminal-INTERPOL, y también formamos parte del Comité Permanente de Identificación de Víctimas de Catástrofes, gracias a que hemos demostrado nuestra capacidad técnica y de respuesta, adquiriendo por ello la confianza del Comité, por ello somos partícipes e integrantes del grupo que gesta las primeras actuaciones, en cualquier parte del mundo, en materia de identificación de cadáveres en sucesos de víctimas múltiples. También somos integrantes y socios fundadores de la Academia Iberoamericana de Criminalística y Ciencias Forenses (AICEF) desde al año 2004, que es la organización de referencia en materia de ciencias forenses en América latina. Y por último ni que decir tiene que también participamos en las correspondientes actividades de EUROPOL relacionadas con el mundo de las ciencias forenses.

Para continuar no estaría de más hacer un alto en el camino y recordar de donde venimos: si bien es verdad que todos convenimos que el primer antecedente de la Policía Nacional se sitúa en el año 1824, con la creación de la Policía General del Reino mediante la Real Cédula de Fernando VII de 13 de enero de ese año, no es menos cierto que no es hasta el año 1911 cuando se crea el Servicio de Identificación dactiloscópica para la identificación y reseña de detenidos, puesto que solo escasos años antes (en 1903 para ser más exactos) fue cuando se presentó el proyecto de clasificación dactiloscópica para estudiar las impresiones digitales como medio de identificación por el Doctor Olóriz, desde entonces hasta hoy, y siempre dentro de los servicios de policía judicial o de investigación criminal, pasando a su vez por diferentes denominaciones, no fue hasta 1994 cuando se crea de manera independiente lo que hoy conocemos como Comisaría General de Policía Científica.

Pero lo que realmente nos ha de importar es ¿hacia donde vamos? Hacia dónde se dirige la investigación en ciencias forenses y la actividad policial en ese ámbito.

En el año 2012 el Instituto Forense de los Países Bajos (NFI por sus siglas en inglés) en un vídeo que todavía se puede visualizar en su página oficial, e incluso en YouTube, explicaba desde su experiencia su visión del futuro de las ciencias forenses, contraponiéndolo a la realidad actual, ejemplificándolo con una tradicional inspección ocular técnico policial tras un crimen, en la que se recogen los vestigios y se protegen para su traslado a los laboratorios correspondiente en los que luego se han de analizar, contraponiéndola a una inspección ocular del futuro en la que los vestigios que se descubren se analizan in situ mediante sistemas que permiten no solo el análisis forense

en el lugar de los hechos, ya sea químico o biológico o de cualquier otro tipo, sino que permiten también el traslado inmediato de la información resultante a la unidad investigadora y su contraste directo con las bases de datos de referencia necesarias.

Esa idea, del año 2012, que en principio era un concepto que vendía el instituto forense holandés como espejo de las empresas de tecnología de su país también la compartíamos en la Policía española y ya la llevábamos a cabo con algunas empresas, pero en nuestro caso españolas. Tal es el caso del proyecto FORLAB iniciado en marzo de 2012 y finalizado en el año 2015, precisamente un proyecto que pretendía por un lado el análisis in situ de los vestigios que se hallaban en un lugar tras una explosión y no solo eso sino que también permitía interactuar e incluso recrear el escenario en tres dimensiones en un centro integrador de datos y de mando al que llegaban las imágenes y la información del lugar en el que se había producido la explosión, de manera que los responsables de los dispositivos podían tomar decisiones incluso sobre el tipo de vestigios que debían ser recogidos y cuáles no era necesario.

El proyecto FORLAB derivó en otro (denominado FORENLIBS) pues como se ha dicho el inicial terminó en el año 2015, que se materializó en la construcción de un prototipo en el que seguimos trabajando que permite analizar in situ vestigios químicos, una herramienta que ha pasado de pesar doscientos kilos a unos veinte. El actual prototipo consta de una mochila en la que se instala la base lógica del sistema y una pistola con un láser LIBS (Laser Induced Break-Down Spectroscopy) lógicamente con las garantías debidas para el policía que la utiliza y transporta, de manera que en el lugar de la inspección ocular se pueden analizar puntualmente todos y cada uno de los vestigios que se considere necesario, aunque en estos momentos la estamos desarrollando y circunscribiendo a los elementos químicos presentes en los residuos de disparo.

Como quiera que la Comisaría General de Policía Científica también publicita sus logros en el entorno forense precisamente la Policía Técnica y Científica francesa (a través de su Director General) se ha mostrado interesada en el prototipo anteriormente mencionado gracias, entre otras cosas a la presentación que sobre nuestras capacidades hicimos en el foro de la reunión anual de directores de laboratorios forenses de ENFSI que se celebró en mayo de 2018 en Budapest, en la que se consiguió, además, gracias también a nuestro prestigio y consideración en Europa, que la reunión anual de directores de laboratorios de ciencias forenses que se ha de celebrar en el año 2020 se desarrolle en la ciudad de Madrid organizada por el Cuerpo Nacional de Policía y bajo los auspicios de la Fundación Policía Española. He de reconocer que la presentación que hicimos en Budapest no

solo trasladó la calidad de nuestro trabajo, nuestras capacidades y el esfuerzo modernizador continuo, sino que también evidenció el volumen de nuestro trabajo, pues no en vano la Policía Nacional es la que más volumen de trabajo desarrolla en el ámbito de las ciencias forenses en España, valga como ejemplo de ello el aporte a las bases de datos nacionales, tanto de huellas dactilares como de identificadores de ADN, un aporte cercano a las tres cuartas partes del contenido de las mismas.

En cuanto a los proyectos más recientes cabe destacar precisamente el denominado ICRIME que contribuirá a la lucha contra el crimen organizado; un programa financiado por la Unión Europea y destinado a los países del sistema de integración centroamericana: Belice, Costa Rica, Guatemala, Salvador, Honduras, Nicaragua, Panamá y República Dominicana; cuya finalidad esencial es la mejora de la investigación criminal y el enjuiciamiento del crimen organizado y el tráfico de drogas. Es un proyecto para cuatro años que será liderado por un comisario del Cuerpo Nacional de Policía y en el que la Policía Científica aportará técnicos sobre materias concretas.

Lamentablemente el tiempo de mi intervención no me permite ser más exhaustiva por lo que solo apuntaré algunos de los proyectos de investigación en los que participamos junto con universidades españolas y extranjeras, el CESIC, grupos de trabajo de ENFSI e INTERPOL y EUROPOL, por ejemplo:

- Evaluación de la calidad y seguridad de complementos alimenticios derivados de las plantas consumidas por la población española para el control de sobrepeso.

- Proyecto COSMO (Corrientes Oceánicas y Seguridad en el Medio Marino) en relación con la aparición de cadáveres en las costas e intentar determinar dónde pudieron ser arrojados.

- Análisis comparativo de registros de habla en el entorno forense: Una revisión del marco conceptual.

- Estudio fisicoquímico sobre cruce de trazos, dentro de un grupo de trabajo de INTERPOL en el que concretamente hemos trabajado sobre una de las cuatro líneas de investigación, la de la intensidad de luminiscencia cromática en la zona de cruzamiento en función del tiempo.

- Estudio forense sobre clientes P2P (Emule, EmuleTorrent y GigaTribe) centrado en el rastro de Información que dejan estas aplicaciones en una máquina tras un periodo de uso.

- Proyecto ENTIRE dentro del programa europeo de I+D H2020 para la construcción de una red europea de usuarios finales relacionados con las aplicaciones biométricas, con el propósito de establecer requisitos operacionales comunes y un entorno dinámico donde los mismos puedan interrelacionarse con la investigación de la situación actual en esa materia y con la industria.

He de reconocer que también hay algunos proyectos de interés en los que no participamos, por el momento claro; nos resistimos a participar por más que desearíamos pues los recursos son escasos y el personal también lo que nos obliga a priorizar, no hay que olvidar que mientras estamos investigando o estudiando siguen entrando solicitudes de informes a las que hay que responder y, no nos engañemos, esto es en realidad por lo que al final se nos mide, por el volumen de informes que hacemos, o diría que más bien se nos mide por los que tardamos más en hacer, que es por lo que realmente se nos piden explicaciones.

Por último solo me queda reconocer públicamente que podemos enorgullecernos de que si las organizaciones internacionales, las universidades y las empresas desean que colaboremos con ellos y nos ofrecen participar en sus proyectos de I+D+i es gracias al trabajo y el prestigio de nuestros profesionales, pues incorporando la marca CNP a sus proyectos añaden garantías de solidez y credibilidad a los mismos.

I+D+I EN LA SEGURIDAD CIUDADANA

JUAN CARLOS CASTRO ESTEVEZ
Comisario Principal del CNP,
Comisario General de Seguridad Ciudadana

En la introducción, me uno prácticamente a todas las premisas de Pilar Allúe, yo también he pretendido mostrar de forma genérica qué es la Comisaría General de Seguridad Ciudadana que, si se caracteriza por algo, es porque somos la parte doméstica de la Policía. Actuamos con la misma rigurosidad que la Comisaría General de Policía Científica, pero nuestro laboratorio está en la calle, esa es la gran diferencia. También he intentado que la presentación pueda aportar algo a todos los que componen este heterogéneo auditorio, en el que se encuentran desde profesionales de la Policía con muchos años de experiencia, a los que sobraría parte de la presentación, hasta personas que no la conocen en absoluto.

El artículo 104 de la Constitución Española establece que es misión de las Fuerzas y Cuerpos de Seguridad del Estado proteger el libre ejercicio de los derechos y garantizar la seguridad ciudadana. Esa seguridad ciudadana la entendemos en sentido amplio, una misión de todas las Fuerzas y Cuerpos, de toda la Policía. Yo, no voy a hablar de toda la Policía, voy a hablar de la seguridad ciudadana en sentido estricto, es decir, de aquello que acomete funcionalmente la Comisaría General de Seguridad Ciudadana con la consiguiente extensión a las Brigadas de Seguridad Ciudadana, que se desenvuelven en el ámbito territorial. Este matiz es fundamental, no tanto para los profesionales de la Policía, que lo saben, sino para el resto de las personas que se encuentran en esta aula.

Antes de entrar en materia, me gustaría decir que todo esto de la investigación y del desarrollo es muy importante, y yo soy el primero que lo creo, pero hago una diferenciación, una cosa es la creatividad y otra cosa es

la innovación; una cosa es el concepto y otra cosa es el proceso. Yo creo que para innovar es preciso invertir y eso es lo que nos falta; quizás porque estamos viviendo un periodo de vacas flacas que ya se está alargando demasiado, aunque no se si es verdad que ya estamos empezando a remontar.

Durante el trascurso de mi exposición pretendo resolver los siguientes interrogantes:

¿Qué pretendemos?

En la Comisaría General de Seguridad Ciudadana y en todo el ámbito de seguridad disponemos afortunadamente de muchos creativos, no tanto de herramientas o de medidas físicas, electrónicas y todo esto que generalmente se pone más en énfasis, sino de procedimientos y procesos. Para mí la investigación, el desarrollo, la creatividad, es fundamental en el ámbito de los procedimientos, en el análisis para determinar cómo luchamos contra las amenazas y los riesgos aparejados a esas amenazas, poniendo al ciudadano en el centro de la cuestión. En este sentido, habría que implementar los procedimientos de los que somos referentes a nivel mundial, complementándolos con los medios técnicos y el uso de las últimas tecnologías, con la finalidad de que las unidades de seguridad ciudadana dispongan de los recursos necesarios y suficientes para prestar un servicio eficaz, eficiente y de calidad. Para ello es preciso realizar un diagnóstico ajustado de nuestro entorno de seguridad y, sobre esto, voy a hablar durante aproximadamente la mitad de mi exposición. Después, entraremos a ver qué es lo que hacemos en materia de I+D+i y cómo aportamos a nuestros procedimientos el valor añadido que implican las herramientas y avances tecnológicos creados o diseñados por empresas y por compañeros de otros ámbitos de la Policía.

Dos matices, para innovar no siempre es necesaria la tecnología, al menos esa es mi opinión, por eso pongo el énfasis en los procesos. Y en muchas ocasiones bastaría con romper los esquemas tradicionales, apostar por potenciar sinergias, no solamente entre las unidades sino entre diferentes Cuerpos y Fuerzas de Seguridad; y alinear los recursos del Estado e invertir adecuadamente. Invertir adecuadamente no es otra cosa que ser conscientes de qué tenemos que priorizar, identificar qué es lo que más afecta a la ciudadanía en materia de seguridad en un momento dado. Para mí esto es lo difícil, porque lo otro, muchas de las otras cosas, están creadas; no habría más que comprárselas a una empresa o quizás adaptarlas, adaptar esa tecnología a la función policial y, además, como aquí tenemos grandes creativos, propiciar la participación de estos con el mundo empresarial para innovar y poner en valor determinadas herramientas dentro de la organización policial.

¿Quiénes somos en la CGSC?

Como organismo central, la Comisaría General de Seguridad Ciudadana está integrada por las siguientes Unidades (Imagen 1): Secretaría General, Jefatura de Unidades de Intervención Policial, Unidad Central de Protección, Jefatura de Unidades Especiales, Unidad Central de Seguridad Privada y Unidad Central de Participación Ciudadana.

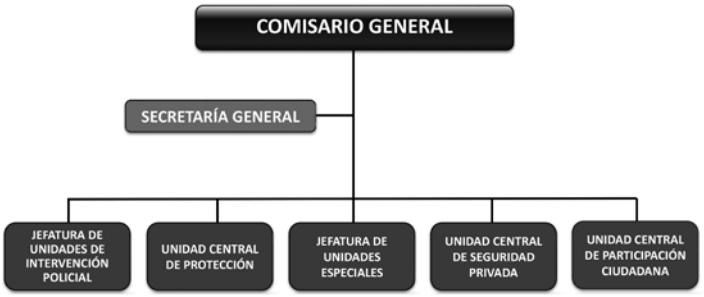


Imagen 1

Al igual que todos ustedes, son unidades tremendamente heterogéneas, con pocas afinidades entre sí, por lo menos a priori, pero lo cierto es que, dependiendo de sus funciones y/o capacidades operativas, todas ellas complementan los servicios que a diario se desarrollan en las distintas plantillas que componen el territorio nacional, apoyando a otros ámbitos policiales o estableciendo grandes dispositivos de seguridad como consecuencia de cualquier tipo de evento.

En el ámbito territorial, las Brigadas de Seguridad Ciudadana disponen de unidades similares a las contempladas en el contexto central, que se concentran en tres grandes grupos (Imagen 2).

En primer lugar, Prevención de la Delincuencia: básicamente compuesto por la Sala del 091 y los radio patrullas que conoce todo el mundo, dedicados a la prevención de la delincuencia en nuestras calles, en su más amplio sentido; nosotros no prevenimos realmente ni el terrorismo yihadista en su origen, que le corresponde a la Comisaría General de Información, ni el crimen organizado en su origen, que le corresponde a la Comisaría General de Policía Judicial, pero contribuimos a combatirlo a través de nuestros despliegues en las calles, dificultando o impidiendo la actuación de terroristas y todo tipo de delincuentes. A esto es a lo que se dedican estas Unidades fundamentalmente.

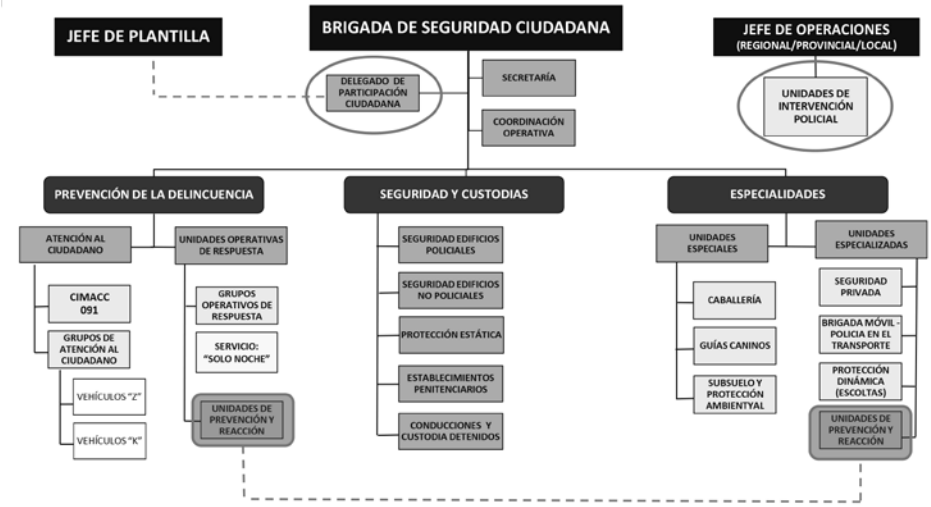


Imagen 2

En segundo lugar, Seguridad y Custodia, dedicado a proteger tanto los edificios policiales como los no policiales y los establecimientos penitenciarios; también realizan protecciones estáticas de personalidades y conducciones y custodias de detenidos.

Y en tercer lugar, las Especialidades, integradas por las unidades especiales de Caballería, Guías Caninos, y Subsuelo y Protección Ambiental, cuyos componentes han de superar un proceso de selección y un curso previo para poder pertenecer a ellas; y las unidades especializadas, para las que no se requiere dicho proceso de selección: Seguridad Privada, Brigada Móvil-Policía en el Transporte, Protecciones Dinámicas y Unidades de Prevención y Reacción (UPR).

¿Qué servicio prestamos?, ¿qué es lo que hacemos?

La Secretaría General es la encargada de la planificación, y de la coordinación, seguimiento y control de todas las unidades que componen la Comisaría General. De ella dependen, a su vez, distintas Unidades: la Unidad de Inteligencia de Seguridad Ciudadana (ISECI), la Unidad que coordina los Centros Inteligentes de Mando, Comunicación y Control (CIMACC 091), y la Oficina Nacional de Deportes (OND) que es el Punto Nacional de Información sobre Fútbol en España (PNIF) y un referente mundial en su materia.

Además, la Secretaría General es la que se responsabiliza de las actividades de investigación y desarrollo en la Comisaría General de Seguridad Ciudadana, ahora que estamos hablando de I+D+i.

También coordina y controla las Unidades Básicas de Seguridad Ciudadana que integran las Salas del 091, que en estos momentos están mutando hacia los denominados CIMACC, los Grupos de Atención al Ciudadano y los Grupos Operativos de Respuesta. Y esto es lo que garantiza la seguridad de nuestras calles.

Con las unidades especiales, lo que se hace es reforzar todo este despliegue cuando nos interesa, cuando necesitamos mayores capacidades operativas, fundamentalmente en grandes dispositivos de seguridad.

En este sentido, hemos de tener en cuenta que el ámbito de demarcación territorial asignado a la Policía Nacional son las ciento setenta y siete ciudades más pobladas y, por tanto, las más importantes de España, donde los eventos sociales, políticos, económicos, deportivos, etc., tienen lugar con especial incidencia; y todos ellos llevan aparejado un componente de seguridad que conlleva establecer los correspondientes servicios, que hay que complementar con las medidas que requiere el actual nivel cuatro de prevención y protección antiterrorista.

¿De qué otras unidades disponemos?

Las Unidades de Intervención Policial, que constituyen la reserva del mando, por antonomasia, y son las que nos sirven para reforzar todos estos servicios. No se dedican solo al orden público, que es lo que sale en los medios de comunicación porque es lo que suele ser noticia, también realizan otras muchas funciones que, básicamente, consisten en reforzar grandes dispositivos donde nos interesa poner más personal, es decir, más unidades para garantizar una mayor capacidad operativa y de respuesta.

La Unidad Central de Protección, que es la que garantiza la seguridad a todas las personalidades que requieren una protección especial: jefes de Estado, presidentes de gobierno u otras personalidades extranjeras cuando visitan España; o los ministros españoles y otras autoridades del Estado. Y también se encarga de la protección de edificios policiales y no policiales.

La Jefatura de Unidades Especiales, compuesta por Caballería, Guías Caninos, Subsuelo y Protección Ambiental, además de la Brigada Móvil-Policía en el Transporte y las Unidades de Prevención y Reacción (UPR). En casi todas las ciudades de España hay subsuelo para canalización, en sus tiempos de agua y ahora de la mayor parte de los servicios esenciales para la comunidad; además, hay un tipo de delincuencia que utiliza el subsuelo para cometer sus fechorías. Las Unidades de Prevención y Reacción (UPR) constituyen un segundo escalón como reserva del mando, con funciones si-

milares a las de las UIP, aunque más implicadas en el día a día de las plantillas donde tienen su base operativa.

La Unidad Central de Seguridad Privada, que es un referente a nivel mundial no solo en cuanto a sus funciones y procedimientos de actuación sino como consecuencia de toda la normativa que ha desarrollado. La ley de Seguridad Privada ha sido engendrada en la Unidad Central de Seguridad Privada y el reglamento que ahora está en su fase de visibilidad, igualmente, sirviendo de ejemplo a numerosos países.

Respecto a la Unidad Central de Participación Ciudadana, la mayor parte de los programas que la Secretaría de Estado de Seguridad ha implementado fueron ideados y creados en esta Unidad de la Comisaría General de Seguridad Ciudadana, evidentemente con menos medios técnicos y de soporte. Por poner un ejemplo, las Unidades de prevención, asistencia y protección a mujeres víctimas de violencia de género (UPAP) se crearon en esta Unidad, así como el Plan Mayor, el Plan Director para la convivencia y mejora de la seguridad en los centros educativos y sus entornos y el Plan Comercio Seguro, etc. Somos un referente mundial y nos visitan numerosas policías de diferentes países para ver qué hacemos en estas materias y cómo lo hacemos.

¿Dónde prestamos nuestros servicios?

Este es el eslogan que venimos utilizando desde hace ya algún tiempo: "Seguridad ciudadana, cerca de ti y siempre a tu servicio", esta es la realidad, siempre al servicio de los ciudadanos que viven o desarrollan su trabajo en las cincuenta capitales de provincia que componen el territorio nacional, en las ciudades autónomas de Ceuta y Melilla y en las ciento veinticinco localidades, que salvo excepciones, son las más pobladas e importantes de España. Es decir, en el territorio donde la incidencia delictiva es mayor y en el que se dan los principales problemas de seguridad. ¿Qué se quiere decir con esto? Como se ha comentado antes, se pone al ciudadano en el centro de todo, las actividades sociales de mayor envergadura que se desarrollan en la calle tienen lugar en las grandes ciudades, todos los eventos y no solamente los deportivos, porque a veces nos pierde el futbol -tenemos veintiún partidos de liga de futbol profesional todas las semanas, primera y segunda división A, con todo lo que eso conlleva en seguridad- pero igualmente los conciertos de cualquier género musical o las reuniones empresariales de cualquier índole, las reuniones de la propia administración de cualquier ministerio, las visitas de los jefes de Estado o presidentes de gobierno que se dan en las ciudades, fundamentalmente en Madrid, pero también en otras ciudades. Y todo esto es lo que tenemos que proteger. Además, ochenta millones de tu-

ristas en el año 2017, que se integran en todo el espectro de actividades que acabamos de comentar, fundamentalmente en las ciudades. (Imágenes 3-4).

Imagen 3

Imagen 4

De las cien ciudades más importantes de España, la Policía Nacional está en setenta y tres ciudades, son datos del Instituto Nacional de Estadística, la Guardia Civil en seis, los Mossos de Esquadra en dieciséis y la Ertzaintza en cinco, en un país de cuarenta y seis mil habitantes; hablo solo de las cien más pobladas, nos quedan otras setenta y siete que van a continuación.

¿Con qué condicionantes?

La Comisaría General de Seguridad Ciudadana se dedica a la prevención, a la reacción y la respuesta, fundamentalmente a asegurar la convivencia pacífica, el uso ordenado de los espacios públicos y la protección de personas y bienes ¿Y con qué condicionantes? El primero de ellos es la amenaza actual, fundamentalmente la amenaza terrorista yihadista, que no es ETA, ya afortunadamente extinguida, según reconoce incluso la Estrategia de Seguridad Nacional de 2017.

Respecto a la amenaza actual, hemos pasado de ETA, que intentaba actuar sobre una persona o una institución concreta, al terrorismo yihadista, que busca matar a cuantos más mejor en el mínimo tiempo posible, es decir, un ministro, que es una de esas autoridades a las que se protege, tiene muchas más posibilidades de ser objeto de un atentado en una calle comprando un libro, como otros tantos ciudadanos, que por el hecho de ser ministro.

Como consecuencia de este cambio de paradigma terrorista, para innovar no habría que ir solamente a las medidas técnicas sino a remover conciencias, a que el tramo político de la Policía donde se toman ese tipo de decisiones, sea consciente de que ETA ya no existe, que, por tanto, esa amenaza tampoco existe y, por tanto, los riesgos aparejados han desaparecido. Nos tenemos que defender de otras cosas y de otra manera, porque el modus operandi también ha cambiado. No tiene sentido el Policía de la puerta del segundo paquete de Unidades que citábamos anteriormente (seguridad y custodia) o al menos no en todos los sitios y, por el contrario, tienen sentido otras cosas como implementar medidas físicas y electrónicas, sobre todo, en un momento donde una cámara DOMO de 360º es muy asequible. Hace unos años una cámara y su mantenimiento tenía un precio muy abultado; ahora, sin embargo, su precio es mucho más asequible.

Hemos de ser conscientes de que tenemos un nuevo escenario, que la amenaza se ha transformado, hay un nuevo marco de actuación que requiere nuevos métodos de prevención, protección y reacción y, además, sabemos cuáles son; no nos hace falta ningún creativo que nos lo cuente. Tenemos que ser conscientes del cambio de paradigma, de la importancia de la implementación del procedimiento AMOK y de la formación de los policías. Ya se ha formado a más de quince mil policías de las unidades básicas de seguridad ciudadana que son las que están en la calle y las que se pueden encontrar con uno o varios individuos de esas características. El GEO no se va a encontrar nunca con un terrorista yihadista dispuesto a atentar en la calle, se lo va a encontrar un radiopatrulla o una patrulla de la Policía Local. Y, cuando en poco más de cinco minutos los terroristas hubieran hecho lo que vinieran a hacer, llegarán las unidades tácticas especiales, aun cuando probablemente ya se haya resuelto el incidente, el acto terrorista. Solamente en caso de que se hagan rehenes o que consigamos aislar a los terroristas en una zona determinada serán necesarias esas unidades tácticas especiales. Por eso es imprescindible alertarlas desde el primer momento, para que lleguen lo antes posible a resolver otro tipo de incidente porque, salvo en los supuestos citados, es muy probable que el acto principal del atentado haya concluido y esté resuelto.

AMOK significa atacar y matar con ira ciega en malayo, y esta palabra es la que ha dado nombre al procedimiento antiterrorista para combatir esa

intención, la de causar cuantos más muertos mejor y en el mínimo tiempo posible. A esto hay que unir que llevamos tres años, que se cumplieron el 26 de junio de 2018, con el nivel cuatro de prevención y protección antiterrorista y que esto implica tomar una serie de medidas de seguridad complementaria en numerosos lugares, especialmente en todos aquellos en los que se concentra una gran cantidad de personas, lo que afecta esencialmente al ámbito de seguridad ciudadana.

El segundo condicionante sería el déficit de efectivos. En el ámbito de seguridad ciudadana somos alrededor del 40% de la Policía Nacional y, por los motivos especificados anteriormente, nos afecta especialmente el déficit de efectivos producto de la crisis económica. (Imagen 5)

Imagen 5

En tercer término, hay que considerar el efecto complementario que, respecto a los efectivos, ha supuesto la nueva Circular de jornada laboral. Un año para cualquier ciudadano tiene ocho mil setecientas sesenta horas reales (8.760), antes de la última circular sobre esta materia, para la Policía un año tenía diez mil trescientas cincuenta y nueve horas (10.359) como consecuencia de los coeficientes correctores aplicados a los horarios de noche y fin de semana. Con la actual circular en lugar de estas diez mil trescientos cincuenta y nueve, tenemos once mil ciento una horas (11.101), esta es la realidad.

Y una vez visto cuál es nuestro entorno de seguridad, pasaré a exponer qué es lo que hacemos en materia de I+D+i, qué innovaciones hemos realizado y como incorporamos a nuestros procedimientos el valor añadido que implican las herramientas y avances tecnológicos.

Unidad de inteligencia de Seguridad Ciudadana (ISECI)

De reciente creación formal. Me pregunto ¿antes no se hacía inteligencia? Desde tiempo inmemorial. Hace años, cuando se iba a una Comisaría de Policía o por lo menos a la Brigada de Seguridad Ciudadana, encontrabas un panel de corcho con un plano con chinchetas de colores donde se marcaban las diferentes zonas de patrullaje y dónde se producían los diferentes delitos. Este corcho evolucionó en el Programa Policía 2000 con el SIG, Sistema de Información Geográfica, que nos iba a decir lo mismo que el corcho pero en una aplicación informática que no terminó de funcionar del todo. Ahora estamos en las mismas, estamos hablando de patrullaje inteligente, que es lo que hacemos desde hace tiempo aunque no disponemos aun de una aplicación informática que nos permita una verdadera adaptación y evolución de la herramienta a la modernidad.

Con este ejemplo quiero decir que inteligencia se ha hecho siempre, aunque quizás no se plasmaba documentalmente; ahora pretendemos formalizar este aspecto. Como hemos dicho, somos casi el 40% de la Policía y estamos permanentemente en la calle, además conseguimos sinergias fundamentales para toda la Policía a través de las Unidades de Seguridad Privada, en intima colaboración con el sector a través de la Plataforma Red Azul, que tiene un espléndido desarrollo.

Esa captación y evaluación de la información se hace fundamentalmente a través de las Unidades de Participación Ciudadana, relacionadas con ONGs y asociaciones de toda índole, y se pone a disposición no solo en el ámbito de Seguridad Ciudadana, sino de unidades de Información, Policía Judicial y Extranjería; no tanto de Policía Científica, que es nuestro laboratorio de referencia para todo. Se pone en conocimiento de estas unidades para su explotación y lo único que se solicita a cambio es que nos comuniquen qué es lo que han hecho con esa información, para que se pueda ir al ciudadano que confió en nosotros y decirle: hemos solucionado su problema de seguridad o al menos hemos intentado solucionarlo. En fin, una respuesta para alimentar ese feedback absolutamente necesario en todos estos procesos. Lo mismo que con Seguridad Privada.

Los Centros Inteligentes de Mando, Comunicación y Control (CIMACC 091)

Se ha mantenido 091 porque no se quiere perder la denominación de aquel teléfono que dio inicio a estos centros de intercomunicación con la ciudadanía, con ese aparataje tremendo, fundamental, que en estos momentos estamos desarrollando en el ámbito de seguridad ciudadana, los CI-

MACC 091 deben ser la herramienta fundamental de los jefes de operaciones regionales y locales.

Es imposible extraer inteligencia si no tenemos este tipo de herramientas, tendremos la información pero, como ocurre ahora, mucha de esa información no la podemos ni siquiera leer y, mucho menos, considerar. Para esto, nos hacen falta estas herramientas tecnológicas que sean capaces de llevarnos a cosas concretas que nos permitan analizar y valorar datos sobre determinadas cuestiones. Aquí también se está integrando Alertcops, el 112 y las Centrales Receptoras de Alarmas (CRA) de las empresas de seguridad. Ya se tenía que haber desarrollado esta última herramienta pero hubo una marcha atrás por parte de las empresas. Ahora, cualquier empresa de seguridad que dispone de una central receptora de alarmas, debe comprobar la alarma y una vez que esto ha sido realizado es cuando llama a la Policía, eso se hace por teléfono ¿Qué se pretendía? Que cuando la Policía alerta al radio patrulla sobre una amenaza cierta y el radio patrulla se dirige al lugar del hecho, la Sala, el CIMACC, tuviera la oportunidad de pasar las imágenes interiores y exteriores procedentes de las cámaras de seguridad para que la patrulla policial que va a actuar tuviera conocimiento, en tiempo real, de lo que está ocurriendo allí.

Lo ideal es que el radio patrulla lleve una tablet donde se puedan ver esas imágenes, una tecnología perfectamente factible y disponible, a falta de inversión.

Los CIMACC están desarrollados en la mayoría de las plantillas previstas (Imagen 6).

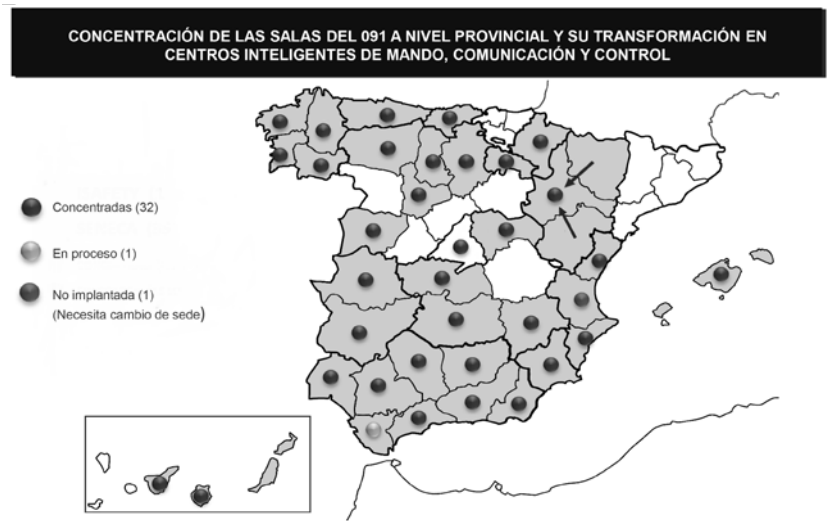


Imagen 6

Vehículo policial inteligente

Que debería incorporar el siguiente equipamiento:

- Tablet portátil con conexión a intranet policial para acceder a los datos relevantes relacionados con el servicio que presta y las comprobaciones de identidad oportunas, tanto de personas como de objetos. Y ha de ser portátil porque la patrulla policial no siempre va en el coche, es más, lo que se pretende es que se baje del mismo. Por eso, no parece adecuado que la tablet forme parte del módulo central del vehículo, se pretende que sea móvil para que el copiloto, generalmente diestro, pueda quitarla de la estructura central y utilizarla de una forma más eficiente, además de utilizarla fuera del vehículo.

- Tiene que tener un Geoposicionamiento del vehículo (AVL).

- Dispositivo de lectura de huella digital.

- Grabación del exterior del vehículo (pre-grabación).

- Posibilidad de que el puente de luces se pueda usar con pantalla para visualización de mensajes preestablecidos.

Cámaras personales de videograbación (Imagen 7).

Los Mossos de Esquadra ya dijeron hace unos días, en todos los medios de comunicación, que disponen de pistolas Taser y las correspondientes cámaras aparejadas; La Policía Nacional está probando las Pinnacle desde hace muchos años, cuando se liciten y nos las proporcionen, habrán salido nuevos modelos que dejarán anticuados a los actuales.

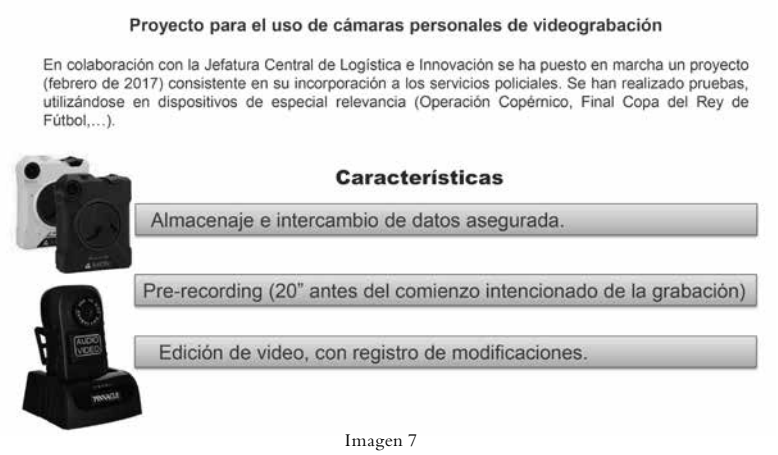


Imagen 7

Proyecto "Identificación en movilidad"

En colaboración con la Jefatura Central de Logística e Innovación, se pretende dotar a los agentes de la Policía Nacional de dispositivos móviles portátiles para acceder a servicios de información y bases de datos para la identificación de personas y vehículos.

Oficina Nacional de Deportes (OND)

Es un referente mundial por las iniciativas adoptadas para erradicar la violencia en el deporte, singularmente en el futbol; acaban de llegar del mundial de Rusia 2018. La Policía Española fue la propulsora de aquel libro verde del Senado en materia de seguridad en el futbol que dio lugar a la Ley del deporte del año 1990. La Policía Nacional fue pionera para que los aspectos relacionados con la seguridad en los estadios y la no violencia se regularan normativamente.

La unidad de control organizativo (UCO) es el lugar donde se ubica el día del partido el coordinador de seguridad, que es un miembro de la Policía responsable del dispositivo de seguridad establecido al efecto. Dispone de numerosas herramientas que le facilitan su trabajo y le permiten el seguimiento del evento: entre otras, cámaras, aforadores sectoriales y megafonía de la que puede hacer uso, anulando la del propio estadio, para dar mensajes de seguridad.

Equipamiento para las Unidades de Intervención Policial

La Jefatura de Unidades de Intervención Policial (JUIP) ha mantenido una permanente preocupación para que se dispusiera de lo necesario respecto al vestuario, armamento, equipo y vehículos, haciendo propuestas que dotan a estas Unidades de una gran capacidad operativa.

En cuanto a drones y antidrones, somos los que los implementamos. Se están estableciendo y desarrollando los protocolos de actuación.

Respecto al entrenamiento tecnológico en tiro Victrix, no dejan de ser galerías de tiro de arma corta y arma larga, de momento se está entrenando en las galerías de tiro militar de Pamplona y Oviedo, haciendo prácticas con las Unidades de Intervención.

Unidad Central de Protección

Desde el punto de vista de la Unidad Central de Protección, se elaboran informes para adaptar los riesgos propios de la amenaza terrorista a la

realidad actual, realizando propuestas para implementar el uso de vigilantes de seguridad y/o medios técnicos de vigilancia, detección y alarma en los servicios de protección de personas, edificios e instalaciones, con la consiguiente reducción del personal destinado a dichas funciones.

Unidad de Guías Caninos de la Jefatura de Unidades Especiales

La Unidad de Guías Caninos de la Jefatura de Unidades Especiales desarrolla las actuales especialidades de Guías Caninos e impulsa novedades, como por ejemplo la detección de armas. Entre dichas especialidades, figuran:

- Detección de explosivos (TATP).

- Detección de drogas.

- Detección de Acelerantes de Fuego (DAF).

- Búsqueda y Localización de Restos Humanos (REHU).

- La Detección Billetes de Curso Legal (BCL).

- Localización de Personas Ocultas (LOPO).

En cuanto al TATP, decir que es un explosivo tremendamente inestable con el que no se puede entrenar a los perros en cualquier sitio y, para ello, vamos al Instituto Nacional de Técnica Aeroespacial (INTA) que nos pone ese explosivo en unas condiciones en las que no es inestable y de esta forma podemos entrenar a los perros.

Si tuviéramos el aparato de José Miguel figúrense el dineral que se ahorraría y, también, nos ahorraríamos el brifing con el perro para ver si ese día está en condiciones de oler y si es absolutamente cierto lo que nos está marcando, si hay TATP o no. Fíjense lo que sería poner un detector de TATP en un estadio de futbol donde hay que tener la garantía de que antes de abrir las puertas no hay ningún explosivo. Y, eso no lo hace el Tedax, porque hay mucha gente, incluso en la Policía, que piensa que esto lo hace el Tedax. Para hacer las requisas se necesita mano de obra, evidentemente tienen que saber qué buscan, cómo y de qué manera; y solo en el caso de que se encuentre algo que pudiera ser un explosivo, se llama al Tedax para que tome las medidas correspondientes.

Respecto a la Detección de Acelerantes de Fuego (DAF), se colabora con Policía Judicial, con unos extraordinarios resultados, el perro detecta dónde

se inició el fuego y, una vez conocido esto, Policía Científica hace los análisis correspondientes para ver con qué.

Restos Humanos (REHU), con la nariz de José Miguel dejaríamos de utilizar carne de cerdo, que es lo más parecido al olor de un humano.

Detección de Billetes de Curso Legal (BCL), antes Policía Judicial iba a buscar armas, drogas…, iba a un domicilio con un mandamiento y había un montón de dinero de curso legal que no se detectaba. Y, esto huele siempre a lo mismo, a los componentes de los billetes que nos pasa la Fábrica Nacional de Moneda y Timbre para entrenar al perro.

Localización de personas Ocultas (LOPO), un ser humano no huele igual cuando es cadáver que cuando está vivo, no es lo mismo buscar un cadáver que una persona viva.

Unidad Central de Participación Ciudadana

Tiene como fin potenciar los servicios y mejorar la calidad en la prestación de los mismos a través de las siguientes herramientas:

Servicio de Atención al Turista Extranjero (SATE). La unidad fue pionera en la creación de este servicio, en colaboración con determinados ayuntamientos, para dar un mejor servicio al ciudadano aunque este no sea español y en la actualidad existen trece SATE: Madrid, Málaga, Marbella, Benidorm, Gandía, Manacor, Benalmádena, Playa de palma, Ibiza, Estepona, Sevilla, Granada y Mahón; como se puede comprobar, fundamentalmente en la zona sur y el Levante.

Como se dispone de pocos funcionarios y no demasiados medios, se busca la colaboración de ayuntamientos y empresas que se hagan cargo y financien la participación de los intérpretes.

Servicio de Atención y Traducción al Idioma Chino (SATIC). En Madrid, en los distritos de Usera-Villaverde, Carabanchel, Centro Puente de Vallecas, Fuenlabrada y Parla hay un importante grupo de personas de nacionalidad china; y, a través de Participación Ciudadana se activó este sistema, que se ha extendido a toda España, ya que en realidad consiste en una llamada a tres: ciudadano chino, traductor de la Fundación Orient y Oficina de Denuncias.

S Visual, funciona de la misma forma pero con los sordomudos. Determinados conciertos con grupos vulnerables propician el establecimiento

de este mecanismo, esta vez a través de una APP. El sordomudo llama a un centro de interpretación de sordomudos que hace de intérprete y desde este se establece una vídeo conferencia entre dicho centro, el ciudadano sordomudo y la Policía: Oficina de Denuncias, Unidad de Documentación o Sala del 091.

Bucles magnéticos, se utiliza con sordos o personas con un porcentaje de sordera alto. Actúa como un micrófono direccional de tal manera que la persona con ese micrófono direccional habla con quien tiene que hablar que es el que le está atendiendo y no escucha todos los ruidos de alrededor, que a ellos les dificulta tremendamente la audición.

Alertcorps, está integrado en los CIMACC 091 y a través de una app envía el tipo de incidencia, el posicionamiento y los datos del registro de la persona que lo utiliza.

Las Redes Sociales, a través de Participación Ciudadana y de todos los programas que se han ido comentando, se trata de llegar con todos nuestros mensajes a la sociedad. Por ejemplo, ha llegado el verano, tenga en cuenta que no debe dejar su casa con … Los folletos informativos están colgados en la web de la Comisaría General de Seguridad Ciudadana, Twiter, Facebook, Instagram...

Plan Comercio Seguro. Considerando la importancia que tiene la actividad comercial en el sector económico, teniendo en cuenta que la protección de la economía es uno de los objetivos estratégicos de la Policía Nacional y con la finalidad de garantizar la seguridad en el comercio frente a cualquier actividad delictiva, el Plan Comercio Seguro se ha prorrogado con carácter permanente.

El Protocolo de actuación de las Fuerzas y Cuerpos de Seguridad para los delitos de odio y conductas que vulneran las normas legales sobre discriminación, determina que la Unidad de Participación Ciudadana es el interlocutor social en la Policía Nacional en esta materia, para lo que desarrolla las siguientes funciones:

- Es contacto permanente con asociaciones y ONG.

- Facilita asesoría técnica y apoyo policial.

- Es el cauce de comunicación de inquietudes y requerimientos.

- Mantiene reuniones periódicas con las diferentes asociaciones representativas de derechos de los diferentes colectivos.

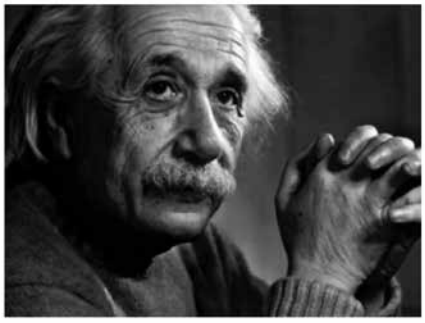
Es la primera línea de contacto con la ciudadanía y a la que verdaderamente le van a contar los problemas de seguridad.

En cuanto a la campaña "Somos más", pivota sobre una aplicación de Google, y su inventor fue el CICO, pero las Unidades de Participación Ciudadana de la Comisaría de Seguridad Ciudadana, designadas como interlocutores sociales, también participan en esta campaña.

Ciber Experto. Programa formativo en el uso de las TIC para niñ@s de primaria, impartido dentro del Plan Director. En este año se han hecho setecientos ochenta y cuatro (784) contactos en seiscientos treinta y dos (632) centros y se han otorgado carnet de ciberexperto a veintinueve mil ciento sesenta (29.160) niños de primaria, donde se les advierte sobre la problemática del uso del teléfono que le han regalado, por ejemplo, en su primera comunión.

Respecto al intercambio de información con Policías Locales hemos de tener en cuenta que el complemento de la Policía Nacional en las ciudades objeto de nuestro ámbito de responsabilidad territorial son los ciento setenta y siete (177) Cuerpos de Policía Local más importantes de España. Es preciso potenciar la actividad de las Juntas Locales de Seguridad que compartimos con ellos y los Consejos Locales de Seguridad, donde están llamados a intervenir todos los grupos sociales, para lograr la máxima participación ciudadana.

Como corolario de mi intervención, creo que deberíamos promover el cambio y hacer caso del contundente mensaje atribuido a Einstein.



*"**Locura** es hacer la misma cosa una y otra vez esperando obtener diferentes resultados".*

PREVENCIÓN E INVESTIGACIÓN POLICIAL EN DIFERENTES ESCENARIOS POSIBLES DE CIBERSEGURIDAD

ANTONIO LÓPEZ MELGAREJO
Inspector del CNP, Unidad Central de Investigación Tecnológica (UIT) de la Comisaría General de Policía Judicial

Viene al caso referirse al "Centro para la Ciberseguridad a Largo Plazo" (CLTC, en inglés), un organismo creado en el seno de la Universidad de Berkeley, y en concreto al trabajo que realizó en el año 2016 -futures 2020- con el propósito de pronosticar los posibles escenarios de ciberseguridad en el año 2020. Tal es el ritmo del cambio, que no se nos antoja descabellado que en 2016 el "largo plazo" se ubicara en el 2020.

https://cltc.berkeley.edu/scenarios/

Se trata de un estudio basado en la identificación de "tendencias emergentes", y en la aplicación de metodologías que, a partir de las posibles formas de cristalización de estas tendencias, desarrollan y describen hasta un total de cinco posibles escenarios. El estudio previene, sin embargo, de que la realidad más probable en 2020 se establezca a partir de elementos de cada uno de ellos, tal vez añadiendo alguno más. Los escenarios así recreados se denominan: Nueva normalidad, Omega, Bubble 2.0, IIOT y Sensorium.

El llamado "Omega" seguramente esté basado en los acontecimientos de Cambridge Analytica, aquellos por los que algunos datos de carácter personal que tenían que haberse mantenido seguros y reservados, trascendieron a esta empresa orientada al marketing político, y sobre los que se aplicaron a novedosas técnicas de publicidad personalizada que -presuntamente- tuvieron como consecuencia "vuelcos electorales" en procesos plebiscitarios tan famosos y trascendentes como el "Brexit" o las presidenciales USA. Este escenario se resume como que en 2020 los estudiosos del Big Data habrán conseguido modelos tan finos que serán capaces de predecir y manipular el comportamiento de los individuos uno a uno con un alto grado de precisión.

El siguiente es el llamado "Bubble 2.0", y parte de la base de una supuesta similitud en las circunstancias socioeconómicas actuales con las que se dieron al inicio del siglo en relación con las así llamadas "punto com", que desembocaron en el crack de sus valores bursátiles. Probablemente este escenario esté inspirado en el "fraude del click", previsto contra los servicios publicitarios "on line" que facturan sobre la base del número de visitas. El fraude consiste en comprometer los navegadores de los usuarios de la red para que estos simulen "clicks"; simulen y contabilicen visitas que en realidad no se llevan a cabo; de modo que los grandes de internet (GAFA), cuyos negocios se basan en buena medida en esta publicidad, verían gravemente menoscabados sus negocios. En este escenario estos gigantes intentarían mitigar las pérdidas malvendiendo sus soberbios paquetes de datos de perfiles comerciales acumulados en sus largos años de intensa actividad interactuando a los usuarios y sus tendencias comerciales.

El escenario "IIOT" (intentional internet of things),tiene que ver con el "Internet de las cosas" y viene a decir que, a medida que las instituciones públicas vayan conectando los objetos a Internet, la seguridad informática irá mutando a seguridad a secas, a "seguridad ciudadana" si ustedes lo prefieren. Si las máquinas están controladas desde Internet (especialmente dispositivos orientados a la gestión de los suministros, sanidad, dependencia y asistencia...) las vulnerabilidades de Internet tienen impacto directo en el mismo mundo físico. Este escenario puede haberse inspirado en el ataque de denegación de servicio que tuvo lugar en el año 2016, por el que se tum-

baron las máquinas de la comercial DYN, pertenecientes al sistema DNS, esencial en Internet. Este ataque fue posible merced al compromiso de gran número de dispositivos digitales conectados a Internet como routers domésticos o cámaras de vigilancia, que mantenían las contraseñas de fábrica. Los atacantes tomaron el control de miles de estos dispositivos para formar una poderosísima botnet.

El escenario "Senrorium" describe un mundo de sensores ubicuos y poderosos sistemas de análisis de datos. Se está imaginando un mundo en el que se hace un uso cotidiano de dispositivos personales que detectan y registran constantes vitales humanas; sofisticadas, no ya las pulseras actuales que se limitan a registrar nuestra frecuencia cardíaca o el número de pasos dados en un paseo, sino otros parámetros como ciertos niveles hormonales, glucosa, temperatura, o el diámetro de la pupila. Estos datos no apuntan a nuestros actos o testimonios, sino a nuestras emociones, algo mucho menos falseable y que nos hace mucho más vulnerables... capturar estos datos y tratarlos debidamente puede ofrecer un muy profundo conocimiento de nosotros, es como si estuviéramos permanentemente conectados a un finísimo polígrafo... sin recurrir a futuribles ni ciencia ficción, ya existe una aplicación para pedir taxis por UBER desde nuestro móvil que es capaz de detectar una intoxicación etílica y comunicarlo al conductor del taxi, por si prefiriera denegar el servicio. La tal aplicación se basa en parámetros muy sencillos, como el número de errores al teclear, o lo errático de nuestra marcha según las inclinaciones del teléfono y la geolocalización... imagínense si esta práctica va un poco más lejos e incorpora y maneja datos hormonales.

Por fin el escenario número uno, la "nueva normalidad", estrictamente policial. Lo que vienen a decir es que las agencias de Policía encargadas de luchar contra el cibercrimen, además de investigar a las grandes botnets o desarrolladores punteros de malware, van a tener que luchar también con ciberdelincuentes más domésticos. Este escenario parece estar inspirado en el fenómeno pujante por que el que es fácil obtener kits con todo lo necesario para delinquir en la red sin la necesidad de profundos conocimientos. También relacionado con el "Crime as a Service", denominación genérica de servicios y paquetes de malware que se venden en los mercados clandestinos de la red "Tor" por algunos tokens de bitcoin u otro criptovalor más difícil de rastrear.

Ante este escenario, con una cibercriminaldad desbocada, la población va a reaccionar retirando los datos de Internet, haciéndolos públicos directamente, o abandonando el ciberespacio. Este es el escenario que más nos afecta a nosotros como policía.

Les recomiendo que no dejen de leer el trabajo "Futures 2020" de la Universidad de Berkeley.

Aparte de este ejercicio prospectivo, que me parece un excelente material como introducción, lo que debemos plantearnos para abordar el tema propiamente dicho es:

¿Cuáles son los elementos básicos de la ciberseguridad o, si lo prefieren, de la ciber-in-seguridad?

El primero de ellos es el producto "no acabado"; todo software de cierta complejidad procede de la compilación de millones y millones de líneas de programación en las que necesariamente se incluyen errores. Algunos de esos errores, críticos para la seguridad del sistema, son detectados y explotados por personas del mundo de la ciberdelincuencia, son lo que se llaman "bugs" (bichos), que sirven de base para la creación de herramientas para atacar a los sistemas vulnerables, los "exploits".

Eso en lo que toca a los programas; pero el segundo elemento básico se refiere a las personas, se trata de la ingenuidad o falta de conciencia de los usuarios. Cuando accedemos a Internet, por regla general, no vamos prevenidos, o no siempre; nos dirigimos a los servicios que consultamos habitualmente y no vamos con una prevención general. Esto lo saben los delincuentes, que utilizan tretas y formas de engaño, algunas especialmente ingeniosas o elaboradas.

Un tercer elemento tiene que ver con el "medio" en que aplicaciones y usuarios se relacionan, se trata de internet, desde luego, una red que se concibió para algo muy distinto de su muy variado uso actual. Internet se desarrolló como una respuesta de los Estados Unidos al liderazgo soviético en materia tecnológica. Los soviéticos colocaron el Sputnik en órbita y los americanos se vieron obligados a responder de algún modo, para eso crearon la red ARPA que, sin bien estaba residenciada en el Departamento de Defensa, su objeto era contratar y beneficiarse del trabajo de los más prestigiosos científicos para asegurar su competencia científica, tanto en el terreno militar como en el civil. Cada científico quería su propia computadora; pero era antieconómico adquirir un gran mainframe para cada uno de ellos, y las regulaciones administrativas impedían comprar todas la unidades a la misma compañía, por lo que se adquirieron solo unos pocos, de distintos fabricantes, y por tanto de distintos lenguajes. La solución fue el desarrollo de los protocolos TCP-IP, que funcionan "por encima" de los lenguajes de cada una de las computadoras. Ese invento, el embrión de internet, estaba concebido para dar el máximo servicio a todos lo miembros de la Red, unos

miembros perfectamente tasados y conocidos... no hubo en su diseño, por tanto, la menor consideración de seguridad que previniera, por ejemplo, el spam o los ataques de denegación de servicio.

Ese mismo diseño de base es el que mantiene una red que actualmente comunica a la mitad de la población mundial y que permite transferencias bancarias y soporta protocolos de comunicación para televisión privada, entre otras muchas cosas. Es un diseño inseguro, porque cuando se desarrolló no había ninguna necesidad de tener en cuenta la seguridad.

En este ecosistema inseguro, ¿Cuáles son los elementos que tenemos para luchar en favor de la ciberseguridad y contra la cibercriminalidad?

La ley, que a un ritmo mucho más lento que la evolución de la tecnología se va adaptando para poder perseguir nuevos delitos, nuevos modus operandi y nuevas pruebas; pero una de las características esenciales de la ley es su territorialidad. Está creada para tener efecto y vigor dentro de un determinado territorio. En Internet las fronteras políticas son infinitamente más permeables que en el mundo físico, de tal manera que en este aspecto encontramos un primer límite espacial que merma mucho la capacidades de investigación y persecución.

Otro límite también de carácter espacial lo constituyen los oasis al margen de a ley; estamos hablando de servidores radicados en países que no reconocen ninguna ley, estados fallidos o con poca vocación de cooperación internacional, que no colaboran con la Justicia, de tal modo que cuando un investigador se dirige a ese servidor solicitando información vital, sus administradores no responden o indican no disponer de ella.

También hay unas limitaciones temporales muy relevantes, la primera tal vez pudiera describirse como ritmo propio de la administración de justicia, una administración de justicia que tiene unos condicionantes garantistas y que suponen unos plazos y unas dilaciones en cualquier gestión que tengamos que hacer. Otra limitación temporal es la retención de datos, un tema prolijo y realmente complicado pero del que esencialmente deberíamos decir que la justicia, al menos la europea, parece inclinarse contra de la retención de datos masiva e indiscriminada. Esto hay que decirlo así de claro, si no tenemos datos retenidos no tenemos manera de investigar con las técnicas de las que hoy nos valemos, sin ningún tipo de paliativos, esto es así. Las últimas sentencias van en esta línea, en el sentido de que los proveedores de servicios no solo no tienen la obligación de retener datos de manera indiscriminada, sino que deben destruirlos una vez han satisfecho las necesidades propias del negocio: administración y facturación, si fuera el caso.

Con independencia del impacto que la ciberseguridad o ciberinseguridad en la vida cotidiana, lo que sí es mucho más común para cualquier investigador policial es la penetración cada vez mayor del ciberespacio y el mundo digital en la realidad cotidiana. La clasificación que hace Europol de los delitos desde el punto de vista cibernético distingue, por un lado, los delitos cibernéticos "puros", en los que están involucradas máquinas que atacan a máquinas, típicamente los clasificados como "hacking", como término genérico, y la denegación de servicio; y por otro lado, aquellos en los que internet y las redes participan de manera relevante, pero que son delitos y formas de delinquir que ya existían, tal vez con otra forma, antes del desarrollo de Internet. Los que mejor representan esta última modalidad serían la pornografía infantil, el fraude electrónico y, en España, un amplio elenco que se lleva a cabo a través de redes sociales.

Puede que las agresiones sexuales a menores, y con ellas sus representaciones gráficas, lo que comunmente conocemos como "pornografía infantil", sean los delitos que más repugnancia y reproche conciten. La pornografía infantil podía existir desde que se inició la fotografía; pero antes del desarrollo de internet aquel que quería obtener material pedófilo tenía que dar la cara, tenía que exponerse; hoy día, es absolutamente fácil obtener pornografía infantil a través de unos cuantos clicks.

Sobre las agresiones sexuales a menores en concurrencia con Internet podemos distinguir tres líneas de amenaza: en primer lugar, como se ha dicho, y por su abundancia, el acceso a la pornografía infantil es muy fácil, hay ya especialistas (Max Taylor) que explican que la capacidad erotógena de las imágenes caduca con el uso repetido, de tal manera que la comunidad pedófila instiga la creación de nuevo material pedófilo, es decir, el consumo de pornografía es, de alguna manera, un acicate para la producción de nuevo material, para la comisión de nuevas agresiones sexuales a menores.

Otra amenaza consiste en el refuerzo psicológico de los miembros de la comunidad pedófila cuando acuden a un foro secreto y blindado de pederastas. Mientras un pederasta aislado debe verse fuertemente controlado por su entorno, temeroso de ser descubierto, y tal vez proclive a recibir tratamiento, uno que se relacione en foros con homólogos intercambiará refuerzos en la condición que les distingue. He podido leer en alguno de esos foros "la sociedad también ha perseguido a veces a los homosexuales, actualmente se les protege y promociona, eso ocurrirá con nosotros algún día".

La última línea de amenaza se relaciona con el intercambio de información operativa, en esos mismos foros, para aprender a cifrar y esconder el

material; para saber responder ante una actuación policial, o para acertar a encontrar sexo real con menores.

El fraude electrónico es la otra gran modalidad de "cyber-enabled crime". La banca electrónica esta emigrando hacia Internet, todo aquello que era fraude bancario basado en falsificación de documentos en la actualidad se proyecta hacia el uso de tarjetas en Internet o la suplantación de identidad a la hora de firmar digitalmente transferencias bancarias.

Además, la Secretaría de Estado de Seguridad, en consideración del número de denuncias registradas, añade en un tercer bloque otras modalidades delictivas que no están contempladas en el Convenio de Budapest de cibercriminalidad, como amenazas y delitos contra el honor, con lo que quedarían representadas las tres grandes modalidades que ocupan el elenco de criminalidad que se ha visto reforzada con el concurso de Internet.

En definitiva, existe un nuevo espacio o dominio de investigación policial que es el mundo digital. Una idea que me gusta trasladar porque veo que los militares no han tenido ningún complejo en reconocer y dar carta de naturaleza a los nuevos dominios, y así, a los tradicionales "tierra, mar y aire", han añadido el "espacio y el ciberespacio". Creo que las agencias de Policía deberíamos considerar explícitamente también el mundo digital, aquel que comprende los dispositivos de almacenamiento masivo, incluyendo los teléfonos móviles, y el ciberespacio.

Los "tradicionales" en cuanto a investigación son bien conocidos. De una parte tenemos el mundo físico; es decir, todo lo que tiene que ver con Policía Científica: la medicina legal, lofoscopia, criminalística... ahora también, en ese mismo mundo, todo aquello que tenga que ver con discos duros físicos u otros soportes. Estos contienen ficheros que tienen vocación de permanencia, y son dispositivos que vamos a encontrar, normalmente, en el entorno de la inspección ocular, un espacio y un análisis que se conoce bien en la Policía.

La otra parte sería el mundo de las ideas, el psicológico; en el que la información se traslada en forma de lenguaje natural, es el mundo de las declaraciones, de los testimonios; de los registros oficiales, confidencias, documentoscopia... y esa parte, también la conocemos bastante bien.

Pero existe un tercer dominio, que es en el que se desarrolla la investigación del ciberespacio, los "logs" y los metadatos. Alguien me podría decir que la investigación en el ciberespacio, es, en realidad, lo mismo que lo que habíamos señalado como cosa nueva en el mundo físico, los discos duros o

dispositivos de almacenamiento de las máquinas servidoras, es verdad; pero téngase en cuenta que la investigación en el ciberespacio es la investigación de elementos que no están en la escena del crimen, ni mucho menos, que no es trivial averiguar dónde se encuentran efectivamente y que además son datos volátiles que tienen que ser cedidos por los administradores de los sistemas en los términos que establezca la ley. La investigación en el o del ciberespacio responde a técnicas muy especializadas.

Con estas clasificación de "dominios de investigación" no se pretende hacer una clasificación exhaustiva, ni seguramente lo suficientemente solvente. A bote pronto pueden identificarse elementos de valor investigativo que no han sido referidos en esta clasificación, sea por ejemplo la "comunicación no verbal", aquella que se invoca siquiera de modo indirecto en la diligencia de careo, o la que sobrevuela en las diferencias de consideración legal de la audio conferencia o vídeo conferencia; también aquellas pruebas contenidas en la memoria RAM entretanto el ordenador está encendido, que se encuentran en la escena del crimen pero en modo alguno tienen vocación de permanencia, más bien al contrario o, en fin, los registros videográficos de cámaras de vigilancia.

Pero aun con estas prevenciones, es preciso reivindicar un tercer dominio de investigación: el digital.

Y todo esto ha ocurrido, como aquel que dice, hace un cuarto de hora; en la actualidad hablamos mucho de ello, pero esto empezó a surgir de ma-

nera perceptible hace realmente poco, acaso un cuarto de siglo, por eso es muy difícil que nuestros modelos de trabajo se ajusten de manera eficaz y completa a esta nueva realidad.

Volviendo atrás, esa clasificación de delitos "cyber-enabled" y "cyber-based" en modo alguno agota el impacto del mundo digital en la investigación policial: hoy día es difícil encontrar un solo hecho delictivo en el que no correspondiera investigar un teléfono móvil, una cuenta de correo electrónico, o un perfil de facebook; por ejemplo, ante un homicidio o asesinato, que nada tiene de "cyber-enabled" o "cyber-based", tenemos todo aquello que nos dice la medicina legal; el análisis lofoscópico del arma homicida; el análisis caligráfico de alguna supuesta nota suicida, o el análisis biológico de alguna punta de cigarrillo, por citar algunos indicios o pruebas; pero si el finado portara consigo un teléfono móvil, pudiera ser esta una de las vías de investigación prioritarias... desde hace, como decimos, un cuarto de hora.

El otro gran aspecto que quería mencionar, como segunda gran idea importante de mi intervención, es lo que tiene que ver con la prevención.

Nuestros esquemas de prevención pasan necesariamente por la idea de "seguridad ciudadana" y con ella la del patrullaje, cuyo concepto se ha querido trasponer al ciberespacio. Si lo hay es un patrullaje fuertemente orientado a requerimiento de los usuarios, que observan circunstancias merecedoras de trasladar a su policía, y que los actuantes comprobamos suficientemente. Además disponemos de las propias herramientas que la Red nos ofrece para llevar a cabo una labor de prevención y concienciación que estamos haciendo muy bien: mencionemos primero a nuestro perfil en Twitter; recuerden que decíamos que uno de los elementos de la ciberinseguridad era el usuario ingenuo o poco concienciado; ciertamente lo que se puede contraponer en su favor es el conocimiento de las cosas: si somos capaces de alertar de una manera eficiente y puntual en qué consisten los engaños, estaremos conjurando el riesgo de fraude y acoso, estaremos previniendo a la población de las cosas de las que tienen que cuidarse.

No olvidemos las charlas en los colegios. Aparte de la magnífica imagen que damos como institución, el hecho de que seamos capaces de instruir a nuestros pequeños en los riesgos que pueden encontrar, es algo inestimable.

Y en tanto que somos depositarios de una gran confianza por parte de la sociedad y al mismo tiempo conocedores de los riesgos y amenazas que suponen las nuevas tecnologías, creo que en los foros en los que podamos hacerlo, deberíamos promover que en la enseñanza obligatoria se incluyeran contenidos sobre conocimiento del medio digital; instar a las autoridades educativas

para que, del mismo modo que tradicionalmente se enseñan ciencias sociales y ciencias naturales, se forme a nuestros jóvenes en el entorno digital.

Cuando tenemos buena información, también la tenemos que reportarla a la industria. Aquellos conocimientos que hayamos obtenido a través de nuestras investigaciones, siempre que no comprometa otras en marcha, pueden ser de gran importancia para la prevención.

Y por fin, para abordar lo tocante a la I+D+i, parece prudente hacer uso de esta clasificación de "mundo digital en relación con todos los delitos"; "delitos que no son puros cibernéticos pero que tienen una dimensión muy especial con Internet", y los que son "delitos cibernéticos puros".

Por su dimensionamiento, en la práctica policial creo que los más importantes son los primeros: cada vez más investigaciones concluyen con el registro de sistemas informáticos de grandes empresas o instituciones públicas. No se da abasto, para la práctica de estas diligencias se viene requiriendo a especialistas de la Unidad Central; pero tenemos que tener en cuenta que cada vez es mayor el número de dispositivos que tenemos que analizar y que estos aumentan su capacidad de almacenamiento, lo que se traduce en muchas horas de trabajo. La manera en la que se está intentando dar respuesta a esta necesidad es mediante el laboratorio "Skylab", que lleva mucho tiempo su ajuste y configuración; aunque queremos pensar que en un tiempo razonablemente corto, si somos capaces de instalarlo en los ordenadores de la Unidad que nos ha requerido, podremos proporcionar acceso on-line a esa información y un importante pre-proceso, ya veremos.

Otro mensaje que quisiera transmitir tiene que ver con la prudencia en las actuaciones policiales, ya que infinidad de ellas concluyen con la incautación de dispositivos de almacenamiento masivo; a efectos de investigación yo no se qué hacer con esto; en cualquier cacheo, en cualquier actuación policial, nos podemos encontrar con un teléfono móvil o con un pen drive... tenemos que ser selectivos, incautemos únicamente aquellos de los que nos conste una relación fehaciente con un hecho delictivo.

Un aspecto más de esta relación genérica del mundo digital con cualquier delito puede encontrarse en lo que en ámbito europeo se llaman "Cross cutting relevant factors": desarrollos tecnológicos que lo traspasan todo, y por tanto también las investigaciones: hablamos de los criptovalores, los mercados clandestinos, el Internet de las cosas. Tenemos que instruir a nuestros investigadores, a algunos especialistas ubicados tal vez en unidades de inteligencia, por ejemplo, en cómo se pueden trazar transacciones de bitcoin, siquiera una primera aproximación.

En cuanto al desarrollo e innovación, que es, según las definiciones, la aplicación de los resultados de la investigación para el diseño de nuevos procesos o sistemas en temas de producción; tenemos que cambiar los planes de estudio de nuestros policías, de nuestros investigadores. Igual que el CNP no recluta a ninguna persona que no sepa conducir vehículos a motor, tenemos que empezar a pensar en no reclutar a quienes no tengan una mínima pericia en el manejo de ordenadores, que, digamos, tras su paso por la Escuela Nacional de Policía sean capaz de extraer determinados ficheros de un sistema informático. La Unidad Central de Ciberdelincuencia, como unidad de especialistas tenemos que dedicarnos a las cosas más difíciles, no podemos asistir a todos los registros que se dan en España, simplemente no es posible.

De manera que, así como tradiciomalmente en la Escuela Nacional de Policía se han impartido e imparten materias como Derecho Penal, Policía Científica y Criminalística, Psicología, Tiro y Derecho Procesal Penal; humildemente creo que también tenemos que empezar a incluir contenidos relativos a Internet, redes, informática forense ... En cuanto al conocimiento de criptovalores, mercados clandestinos, probablemente seamos las unidades especializadas las que tengamos que dedicarnos, al menos en una primera aproximación, a instruir al resto de compañeros.

En referencia a los delitos de pornografía infantil y fraude electrónico, es obvio que lo más importante es la investigación policial; pero también, en este entorno de I+D+i, tenemos que hablar de la Investigación científica. Debe indicarse que esta investigación científica se asienta en tres soportes, es un trípode con tres patas de colaboración: colaboración con agencias policiales de otros países; con la industria de Internet, que tiene mucho que decir y aportar, y la Universidad y el mundo académico. Baste mencionar que estamos involucrados en proyectos Horizon 2020, como Titanium y Ramses, e invertimos muchos recursos materiales y humanos en viajes internacionales y horas de trabajo en estos proyectos.

En cuanto a los delitos informáticos puros, déjenme que les diga que acabo de regresar del Consejo de Europa donde he tenido el inmenso honor de explicar lo que ha sido la operación "Carbanak", la operación más compleja que ha culminado en marzo de este año con rotundo éxito la UCC. En esta conferencia he tenido la oportunidad de explicar el cambio copernicano que ha supuesto el ataque a las instituciones financieras en lugar de al cliente, con dispositivos de seguridad mucho más precarios. Ajustándome a las líneas de investigación que se han desarrollado hasta detener al "mastermind" del grupo criminal Carbanak, tuve oportunidad de aportar algunos detalles sobre las líneas de investigación tradicional que se llevaron a cabo; otros de investigación tecnológica, con la aportación de brillantes

y novedosas ideas que requerían una instrucción actualizada. Unas y otras nos llevaron a obtener surtidas pruebas de blanqueo de dinero, también de evidencias de que miembros de Carbanak habían actuado como mulas, lo que venía a dar razón de ser al blanqueo; pero no teníamos ninguna vinculación con lo que son ataques informáticos propiamente dichos, aquellos a través de los cuales los cibercriminales conseguían traspasar el perímetro del banco y establecerse en sus redes para permanecer escuchando; aprendiendo el funcionamiento del banco y escalando privilegios hasta acceder a los sistemas críticos, los de negocio, los que permitían, como fue el caso, el control remoto de los cajeros de la red para hacer que vaciaran sus depósitos de billetes cuando las mulas estabas presentes y preparadas a su lado; los que permitían cambiar a voluntad los saldos de los clientes, y cambiar el destinatario de las transferencias más jugosas a cuentas controladas por la organización... ¿cómo podíamos vincular a los miembros de esta organización con estos ataques?... el trabajo sistemático y bien orientado llevó al hallazgo de que algunos elementos de la infraestructura cibernética habían sido pagados con criptovalores desde unas direcciones que controlábamos. Es decir, se llegó a la conclusión y así se demostró que necesariamente tenían que haber sido ellos, por decirlo de una manera sencilla: El que esos recursos cibernéticos hubieran sido comprados desde estas direcciones de bitcoin, era un elemento probatorio tan robusto como encontrar una huella dactilar sobre el arma homicida.

Pero un dato para la reflexión: esa magnífica operación, que ha tenido un reconocimiento internacional sin parangón, que ha aportado dos teras de valiosísima información, contabiliza en nuestro sistema estadístico DOS DETENIDOS y CERO ESCLARECIDOS, pues los hechos delictivos que dieron origen a la operación tuvieron lugar en el extranjero y muchos de ellos están aún en trámite de denuncia.

Muchas gracias por su atención.

TURNO DE PREGUNTAS

Pregunta en sala: Carmen Martínez, Comisaria Principal de Policía Científica. Quiero poner en valor, no voy a preguntar, esto que se ha expuesto aquí, porque me pongo en el lugar de un juez de instrucción que tenga que instruir un tema como este y se me ponen los pelos como escarpias, solamente esto.

Pregunta en sala: Miguel Méndez, Comisario Provincial de Ciudad Real. En este momento, supongo no solo en Ciudad Real sino en toda España, hay una tipología delictiva que se está disparando exponencialmente que son precisamente los fraudes electrónicos, entiendo que desde la Unidad Central habrá una orientación importante y que seguro que nos puedes dar.

Respone: Antonio López Melgarejo

Sí, de hecho, así viene reflejado en las estadísticas de la Secretaría de Estado de Seguridad que hacen corresponder un quesito muy generoso al tema del fraude electrónico. Hay que hacer una observación sobre este particular y es que las cuestiones de fraude electrónico se denuncian siempre, porque cuando el cliente acude al banco a reclamar, el banco le dice: sí, puede que le devolvamos lo detraído; pero lo primero que tiene que hacer es denunciarlo... y esto es así simplemente porque el repudio de esa operación tiene que constar de manera fehaciente en la contabilidad del banco.

Con independencia de esto, los últimos desarrollos de operaciones punteras tienen que ver con el fraude electrónico. Sí, hay que dar una respuesta; es una especialidad muy difícil de tratar pero, por ejemplo, puedo decir que en la Unidad Central, estamos estableciendo un protocolo de colaboración con los bancos, totalmente puntero e innovador y que si todo marcha razonablemente bien, nos va a dar resultados a medio plazo. Arrancarlo cuesta mucho, son muchas horas de trabajo, muchas reuniones, muchos ajustes finos, pero a medio plazo esperamos obtener unos resultados interesantes que, además, vamos a poder compartir con la estructura periférica.

MESA REDONDA: HITOS Y OPORTUNIDADES PARA LA INVESTIGACIÓN EN LA POLICÍA NACIONAL

Mª Pilar Allué Blasco.
Participan: Juan Carlos Castro Estévez; Antonio López Melgarejo; Casimiro Nevado Santano; Miguel Camacho Collados; José Miguel Sánchez España

Interviene: Mª Pilar Allué Blasco

Quisiera hacer un apunte al inicio de esta mesa redonda, creo que se debería haber incorporado en el título de la jornada alguna cosa más, porque si bien la jornada se denomina "Futuras oportunidades para la Policía Nacional en I+D+i", creo que había que haber incorporado también la palabra desafíos, visto lo que han expuesto todos los ponentes, pues no solo se ha hablado de las oportunidades para Policía Nacional en este ámbito, sino también de los desafíos, los nuevos espacios de trabajo, los nuevos horizontes que se abren como consecuencia del trabajo en el ámbito de la investigación del desarrollo y la innovación, pero, también han quedado patentes los nuevos límites a la actuación policial, los límites al tipo de investigación policial tradicional y que incorpora un espacio tan grande como es el ciberespacio y la ciberdelincuencia. También, creo que, como resultado de toda la jornada, podemos marcharnos todos muy satisfechos de haber participado en ella pero, sobre todo, creo que nos vamos mucho más conscientes de nuestras vulnerabilidades, no solamente como personas sino como integrantes de diferentes organizaciones.

Cierto es que cada vez somos más vulnerables a la delincuencia y especialmente a la ciberdelincuencia pero, también es verdad, que ha quedado patente que nuestras capacidades investigadoras, no solamente las tradicio-

nales, sino las técnicas científicas, cada vez son mayores y cada vez respondemos con mayor eficiencia y con mayor dedicación y profesionalidad; habida cuenta del ejemplo de los grandes profesionales que hemos tenido ocasión de escuchar.

Se ha hablado de la importancia de fundamentar la actividad probatoria de cara a las actuaciones judiciales en el ámbito criminal pero, también se ha hablado y con profundidad, de la importancia de la inteligencia artificial, de los nuevos sensores biológicos, de toda la trascendencia que tiene la ciencia y la técnica en el mundo actual y, sobre todo, dirigido a la protección de los ciudadanos y a la investigación de la delincuencia. Como visión general, me voy satisfecha de una jornada como la de hoy y, por lo que veo, va in crescendo esa satisfacción de los conocimientos que hemos obtenido a lo largo de una jornada de estas características. En cualquier caso, como lo importante es ahora darles, a los ponentes de esta jornada la oportunidad para que maticen lo que crean conveniente, a la luz también de. alguna pregunta más que se ha quedado en el tintero a lo largo de las anteriores intervenciones, me complace daros la palabra.

Interviene: Casimiro Nevado

Quería hacer una reflexión sobre las cosas que hayan podido salir a lo largo de la jornada, porque cada vez estamos más conectados y pasamos más tiempo en lo que antes decíamos Internet o en la vida digital y que es, ahora mismo, algo tan real como puede ser el mundo físico o analógico. A mayor conexión, tenemos que ser conscientes de que vamos a tener mayor número de vulnerabilidades, si nuestra vida va a depender de lo que tengamos en un Smartphone, en un ordenador personal..., tenemos que ser conscientes de que debemos ser responsables de que igual manera que mantenemos una serie de medidas de seguridad en el mundo físico, en el mundo analógico. Me ha gustado el término que han sacado de las vulnerabilidades porque no somos conscientes de lo que hacemos cada día con nuestro teléfono ¿Pensamos en la cantidad de datos que vamos almacenando en nuestro teléfono, día tras día, de fotografías, de metadatos? Seguro que no somos conscientes de ello. Tengo amistades, que todas las noches, antes de acostarse, regresan su teléfono a estado fabrica para volver a empezar de cero al día siguiente. Porque son conscientes de todo lo que han acumulado durante ese día, si han visitado redes wifi, ... Y, regresan por la noche su teléfono a estado fábrica y vuelven a comenzar de cero ¿Puede parecer un poco paranoico eso? En el Mando Conjunto de Ciberdefensa Español no permiten la entrada a sus miembros con ningún dispositivo móvil ni portátil que sea personal y no sea de la empresa, porque dan por hecho que van a ser ciberatacados. El que quiera entrar en el Mando Conjunto de Ciberdefensa Español, debe dejar en la taquilla su teléfono móvil ¿Somos conscientes nosotros, como institución, que esto también nos puede pasar a nosotros? Estába-

mos hablando antes del *Crime as a Service*, supongamos que, a lo mejor, yo monto una organización criminal, me es rentable gastarme diez millones (10M) de euros en contratar a un pirata informático que me hackee todos los teléfonos de una plantilla determinada de Policía, logre enviar un enlace malicioso a cualquier miembro de esa comisaría y que, a su vez, este policía, que pertenece a un grupo de WhatsAp de esa comisaría, le va a dar difusión y todos vamos a participar de este mensaje; conclusión: voy a tener el control de todos los teléfonos de todos los policías. Me ha salido por diez millones de euros (10M) y a lo mejor lo que quiero conseguir son cien millones (100M), me va a salir rentable ¿Somos conscientes, como institución, de que esto nos puede suceder a nosotros también?, porque, por ejemplo en el Mando Conjunto de Ciberdefensa sí son conscientes. Me parece muy importante el termino vulnerabilidades y el de ser conscientes de lo que hacemos en el ciberespacio.

Nos hemos preguntado ¿qué es el ciberespacio? En mi opinión, es el conjunto de información que se tiene contenida en móviles, en servidores, en ordenadores personales... Por lo tanto, la base es información. Y el conflicto actual que vamos a ver y que estamos viendo entre países y empresas, es el de intentar destruir los flujos de información de nuestro oponente, la famosa *face new* ¿Qué se pretende con esa *face new,* con esas falsedades? Lo que se pretende, al final, no es difundir un bulo sino que el resto de personas dejemos de creer en las cosas que creíamos antes, vamos a dejar de creer en la Policía, en las instituciones... Y esto, al final, es un ciberataque en cuanto que es una movilización de información dentro del ciberespacio.

Interviene: José Miguel Sánchez

Uno de los ingenieros que está trabajando en el proyecto de sistemas olfativos artificiales; pues bien, cada vez que quiero contactar con él es imposible llamarlo por el móvil porque no tiene móvil. Él piensa que si tuviera un móvil podrían saber dónde está, con quién está hablando y por eso no lo tiene. Dice que desde el ordenador de su casa con el software adecuado te puede decir toda esa información. Ellos lo ven sencillo, nosotros lo vemos más complicado. Pero es verdad que existe esa posibilidad; la única forma, señales de humo, correos electrónicos y poco más para hablar con él.

En relación a la nariz electrónica, decir que todas las medidas que se han mostrado en la presentación son todas medidas de laboratorio, lógicamente el siguiente paso es hacer medidas de campo, es decir, llevarse la nariz electrónica fuera del laboratorio y detectar qué sustancias están en el ambiente. Todas las medidas han mostrado ser eficientes, repito, en el laboratorio y faltaría ese siguiente paso. También, me han preguntado a qué distancia hay que poner la nariz electrónica para poder detectar una sustancia. Pues, si

ahora mismo, la nariz electrónica, la pongo en un ambiente en el que esté amoniaco, como ese amoniaco está distribuido de forma homogénea por toda la habitación, no hace falta que me pegue exactamente a la fuente donde está, directamente la nariz electrónica me va a detectar amoniaco. La sensibilidad puede llegar a ser de partes por millón hasta partes por trillón, es decir, que lo puede detectar aunque no esté al lado.

Un prototipo que han desarrollado también los ingenieros, es un robot olfateador que mide los gradientes de concentraciones; imagínense una mini aspiradora con la nariz electrónica y el robot va detectando según el gradiente de concentración dónde hay más concentración, y hacia ahí se dirige; con lo cual, establece un ángulo. Imagínense, que cuando va girando el robot en un ángulo, de ciento ochenta grados, pues donde más concentración le da, pues ahí se dirige, con lo cual, podría localizar la fuente de la que emana el olor en cuestión. Esto, también está en fase de desarrollo. A mí, como Tedax, ¿me interesa exactamente dónde está la fuente? A mí lo que me interesa, lógicamente, cuanto más información mejor; pero, no es necesario, porque cuando estamos al aire libre hay corrientes de aire, con lo cual, el hecho de que la fuente esté en una corriente de aire me equivoca al robot a la hora de que ese aire va a mover esa concentración de sustancias y lo va a distribuir de otra forma, con lo cual, podría equivocar un poco. Si estamos en una habitación cerrada y el robot me indica, sin corrientes de aire, de donde viene la fuente de emanación, pues sí me puede valer, pero en campo abierto no lo veo tan útil.

La nariz electrónica se puede programar para lo que queramos; puede ser para una sola sustancia, con lo cual sería más fácil, por ejemplo, yo quiero que detecte simplemente el jamón cinco jotas, pues se cogen un montón de jamones y que sea solo ese jamón el que me detecte; y solo lo hago para ese jamón en concreto y solo tengo que programar un olor. A los Tedax, les interesan las sustancias que son más comunes, con las que nos podemos enfrentar, como por ejemplo: dinamita, pentrita, TATP,... Hace poco que falleció una mujer de la limpieza, mezclo amoniaco con cloro, qué es lo que la mató el amoniaco, el cloro, la mezcla de las dos (cloramina) que es una sustancia bastante más tóxica. Pues, para este tipo de sustancias como la cloramina, también vamos a ensayar la nariz. Lo vamos a ensayar para todas aquellas sustancias que más nos podemos encontrar en un incidente real, no le vamos a meter mil sustancias porque sería meterle mucha información y acabaríamos la nariz electrónica dentro de cincuenta años. Se trata de meterle lo más normal, lo más usual y si alguien lo quiere para una cosa en concreto como las aplicaciones médicas, para la enfermedad de Crohn, pues solo se programara para el olor que da en las heces ese tipo de enfermedad.

Pregunta en sala: Francisco Javier Oterino, comisario, jefe de información de Valladolid. Este tema lo he tratado con el jefe de grupo nuestro de Tedax y somos conocedores de tu trabajo, sin embargo, nos surge siempre la duda respecto a la nariz electrónica y que es capaz de detectar y discernir distintos componentes que forman los actuales explosivos. El problema que nos suscita es que son componentes de uso común, entonces, imaginemos que vamos a un aeropuerto, la acetona de las uñas, el agua oxigenada, es decir, múltiples componentes que son de uso común, ¿cómo se podría valorar eso?, ¿darían muchos falsos positivos?; al mismo tiempo, creo que los perros tienen un papel fundamental, sobre todo, en el área de información y de seguridad ciudadana, en el sentido de que nos hacen un trabajo de prevención importante que nos puede ser complementario al trabajo que se está desarrollando. Creo que son imprescindibles, muchas veces tiramos de los perros, en el sentido de ir a la estación de tren y el área que nos abarca es importante; creo que la complementariedad es vital. Cuando tenemos un incidente, evidentemente el detector químico nos va a certificar realmente lo que está pasando, por eso ambos son buenos métodos.

Responde: José Miguel Sánchez

En el tema de los perros, estoy con usted; sí, son complementarios; lógicamente no en todos los casos. En un gas Sarín o en un amoniaco o en una cloramina, lógicamente, el perro no tendría sentido. Estoy totalmente de acuerdo que valen como labores de prevención, pero estamos en aquellos casos en los que pueda sumar; lógicamente, si es el tema de una acetona o de un agua oxigenada, el perro se puede entrenar para la acetona o para el agua oxigenada, pero ese perro que vale para el agua oxigena y la acetona no te vale para el TATP según fuentes de guías caninos. Aunque hagamos el TATP con agua oxigenada y acetona, el olor del TATP, que es un compuesto químicamente distinto, no huele a acetona ni a agua oxigenada, huele a TATP. La nariz electrónica la puedo programar para que me huela el agua oxigenada, la acetona y el TATP. Los perros que valen para agua oxigenada y para acetona no valen para el TATP. Digo esto como un inciso aparte. Lo que quiero hacer hincapié es que la nariz electrónica la puedo programar para lo que quiera; si estamos en un aeropuerto y me huele la acetona de las uñas de los bolsos de las mujeres, pues no pongo acetona y le pongo solo TATP; o le pongo los dos, la nariz electrónica me los va a discernir. La cuestión es que según programe la nariz electrónica así me lo va a detectar, pero que el TATP no huele igual que el agua oxigenada ni la acetona aunque sean estos sus precursores.

Lógicamente, está el siguiente problema y hay que ser realista. Cuando nos vamos a hacer medidas de campo, los olores se combinan entre ellos y la combinación de los olores no me da la mezcla de olores, me da un olor

distinto. No huele lo mismo la colonia mezclada con acetona que esa misma colonia con otra sustancia; pero tampoco me huele a una suma de los dos, sino otro compuesto químicamente distinto que tendrá su olor determinado, con lo cual, todo esto, también es complejo.

¿Se puede utilizar en la detección de restos humanos? Un muerto siempre va a desprender una sustancia que es común a la de todos los muertos y un vivo dependerá de la hora, de lo que ha comido, de que haya hecho más o menos ejercicio, es decir, una misma persona puede oler de diferente forma dependiendo de la hora del día y del paso de los años. La cuestión ¿podría identificar con una nariz electrónica que el olor corporal proviene de esa persona y no de otra en concreto? Eso, es muy complicado; porque incluso una sola persona me desprende olores distintos. A mí, lo que me interesaría, en todo caso, es que si todas las personas emitieran el mismo olor, un compuesto en común químico, que me dijera que viene de una persona y no de un animal. Por lo tanto, de restos de humanos podemos decir que sí, por el olor que emiten; pero en personas vivas, nos vamos a conformar con que, por lo menos, te diga que viene de una persona y que no es de perro, de un animal.

Pregunta en sala: José Carlos da Silva, inspector adjunto de promoción interna. Toda mi vida he estado en Policía Científica y dentro de esta, concretamente, en la investigación de incendios. He tenido la oportunidad de participar en investigaciones de incendios grandes como los de Campo Frío, donde estuvieron los perros. Me gustaría saber si la nariz electrónica que ha diseñado, sería factible para detectar compuestos de acelerantes de la combustión en un incendio.

Responde: José Miguel Sánchez

Me da pie a contestar dos cosas, una que no comenté en la presentación y otra que le voy a decir. Los sensores que se le pueden poner a la nariz electrónica son los sensores que se quieran, desde sensores de gases hasta sensores de temperatura y, todos, tienen en común sensores de humedad, porque dependiendo de la humedad ambiental la medida que da es una u otra, cosa esta que hay que calibrar y tener en cuenta. En relación a un incendio, si le colocamos un sensor de temperatura, la nariz electrónica se puede programar para que me diga cuál es el foco de ignición o el foco de máxima temperatura desde la que se ha podido producir el incendio, con lo cual, valdría para localizar de dónde viene ese posible foco primario y, por otro lado, todo lo que son acelerantes de combustión -gasolina, gasoil, hidrocarburos-, se han hecho medidas y han sido comprobadas perfectamente. Además, de que ya de por sí, si lo huelo yo, también la nariz electrónica lo huele. Pero es que no tiene por qué oler. No porque yo la huela, la nariz electrónica

funciona; la nariz electrónica va a funcionar siempre que esa sustancia emita la suficiente presión de vapor, es decir, que el vapor que está en equilibrio con esa sustancia, tenga una presión de vapor lo suficientemente alta como para que cuando llegue a la nariz electrónica y que está hecha a base de semiconductores, se adhiera a la superficie, cambie la resistencia eléctrica o la conductancia, o lo que quiera medir. Pues eso ya me produce una variación de la señal y esto quiere decir que, aunque la sustancia no huela, la nariz electrónica va a responder, sin embargo, la nariz humana huele lo que huele; los acelerantes de combustión huelen bastante pero, aunque no huelan, la nariz electrónica también me lo detecta.

Por lo tanto: me vale para detectar focos primarios con sensores de temperatura y con acelerantes de la combustión. Se han hecho pruebas y los resultados han sido satisfactorios porque los discriminaba muy bien.

Pregunta en sala: Puntualizar una cosa que se ha comentado; cualquier detector *in situ* que se desarrolle, es trasversal para la Policía Científica, por supuesto, lo que es necesario es protocolarizar la toma de muestras que es la continuación. Porque, una cosa es que nos dé la información en el lugar de los hechos que, además, nos va a permitir coger las muestras adecuadas para llevarlas a los laboratorios y no saturarlos, pero luego, lo que hay, porque yo también estuve en el Tedax NRBQ, es el tema de protocolarizar lo que es la toma de muestras. En esto también hemos de pensar cuando se desarrollan estos equipos.

Responde: José Miguel Sánchez
A colación de lo que ha dicho, no dejan de ser detectores que lo que te dan es una primera valoración de lo que puede ser pero, lógicamente, como prueba judicial no te va a valer, es indicativo, igual que cuando hacemos el test de cocaína o heroína, da el color y dice ¡vale!, me da positivo. También, hay falso positivo, hasta que no esté la prueba de laboratorio no te vale.

Réplica: La toma de muestras es lo intermedio que es fundamental.

Responde: José Miguel Sánchez
Sí claro.

Al margen, existe la posibilidad de colocar biosensores en la nariz electrónica, dependiendo de las interacciones que se producen, por ejemplo, como una reacción antígeno-anticuerpo. Para la bacteria "X", coloco este sensor que solo me responde para esta bacteria; qué es lo que pasa, pues hay que colocar, a lo mejor, un biosensor para cada una de las sustancias en concreto. Un sensor de gases no solo responde a un gas sino que responde

a una multitud de gases, por eso, se colocan varios para que contrastando la respuesta de sensores de distintas tecnologías, poder confirmar las sustancias. Pero para un bichito biológico tendría que colocar un biosensor especifico, por ejemplo para el ántrax, coloco un biosensor para que cuando la nariz electrónica lo detecte me de Ántrax, me de la variación eléctrica o lo que programe.

Interviene: José Antonio Cebrián

Me gustaría hacer unas reflexiones, la primera de ellas es respecto a los dispositivos móviles, ordenadores, ... Estamos dando la sensación de que estamos permanentemente amenazados, ¿y qué? Es cierto, no hace falta más que meternos en Google, en nuestra cuenta, y decirle Google dónde he estado durante los dos últimos años, y te lo dice perfectamente. Un diario precioso, sin necesidad de escribir nada ¿Esto significa que estamos en peligro? Desde mi punto de vista no, simplemente vamos paralelos a la evolución tecnológica. Hay que tener algo en cuenta, la delincuencia; salvo los crímenes pasionales y algunas excepciones, el que es delincuente, es delincuente por dinero, con lo cual, si nos quieren intervenir el teléfono móvil tenemos que tener algo que les interese o se trate de micro estafas que también existen, y que se están dando en mucha gente. Pero, habitualmente, no estamos tan en peligro como la gente cree; hay más rumorología de lo que realmente estamos hablando. Como curiosidad métanse, algún día, en una página que se llama Zerodium, una empresa británica que se dedica a vender vulnerabilidades a Fuerzas y Cuerpos de seguridad; se darán cuenta de que una vulnerabilidad para Iphone cuesta un millón de euros ¿Me voy a gastar un millón de euros en ver que es lo que usted lleva en el teléfono móvil? No me interesa ¿Podemos sacar datos? ¿Realmente datos muy sensibles? Hay que trabajarlo mucho, con lo cual, vamos a estar tranquilos, al respecto, porque la cosa no es tan grave. Hay otro problema, si cerramos todas las vulnerabilidades, la Policía también trabaja con esas vulnerabilidades, si hacemos dispositivos totalmente seguros, yo me voy al paro.

Como segunda reflexión, estas jornadas se llaman I+D+i; vuelvo a reiterar que sería importante el centralizar todas las innovaciones, ideas y nuevas tecnologías en el servicio de I+D+i de logística y que tuviera conocimiento de todos los proyectos Horizonte 2020; no única y exclusivamente de estos, sino tanto de vuestros desarrollos y, a partir de ahí, desde ese punto, fuera como una ventana única desde la cual se pudiera transmitir conocimiento al resto de Unidades y no solo a las centrales y a Comisarías Provinciales, y evitar gasto de dinero. Estamos comprando equipos, que son muy caros, duplicados ¿Por qué? Por qué no hay alguien que diga ¡no!, de esto se compra solo un equipo. O, por ejemplo, respecto de servidores informáticos o de todo lo que está de moda en inteligencia, big data y demás. Si, actualmente

la política cliente servidor, la nube y demás, se basan en permisos. Vamos a hacer infraestructuras potentes para Policía Nacional, pero no vamos a hacer veinte, vamos a hacer una y, piramidalmente, vamos a ir distribuyéndolo.

Tercera reflexión ¿Tenemos dinero para hacer I+D? No, no tenemos dinero, pero tenemos la marca de la Policía. Tenemos unas ideas fantásticas que podemos ofrecer tanto a las universidades como a empresas privadas. Y, a partir de ahí, que realicen desarrollos y les damos la marca Policía; les damos la idea, que es lo que más cuesta en cualquier desarrollo tecnológico. Vamos a tratar de formar gente, directores de proyectos y vamos a beneficiarnos de esas ideas que tienen nuestros policías y que, por lo menos, para nosotros salga gratis, ya que hemos dado la idea, el conocimiento. Permitimos que utilicen la marca España que, sinceramente, si salen al extranjero, no tiene nada que envidiar de otras Policías del mundo. Que pongan la marca Policía España y que saquen los beneficios que tengan que sacar.

Y cuarta, y última reflexión, a nivel judicial. Las tecnologías van mucho más rápido que los desarrollos legislativos o judiciales. En el caso de sistemas especiales se tiene un grave problema, nos cuesta mucho encontrar y desarrollar nuevas tecnologías. Si de repente llegamos a juicio y esa tecnología sale a la luz, no podemos volverla a utilizar ¿Qué problemas nos estamos encontrando? Por un acuerdo del Consejo de Ministros todo el material que se utiliza en la lucha contra el terrorismo y el crimen organizado está declarado secreto. Llega el abogado de turno y empieza a preguntar y, al final, el juez obliga al Policía a contestar. Algo que no debería ser. Nos acabamos de cargar un medio que quizás haya costado, quitando el dinero que son medios muy caros, un conocimiento y el preparar a ese personal para poder colocarlo y, sobre todo, explotarlo. Hay que empezar otra vez de cero.

Es necesario tener una legislación que permita proteger los medios con lo que trabajamos y que, judicialmente, nos ofrezca garantía; pero que no pudieran salir a la luz pública. Cada vez que se produce una detención, lo primero que sale es, "se acaba de encontrar un barco con dos mil kilos de cocaína, el barco había sido balizado en tal punto y llevaba la baliza en tal punto".

Una persona perteneciente al Cuerpo de Policía, hace unos meses, salió en televisión española, explicando cómo se colocaban las balizas.

Interviene: Mª Pilar Allué Blasco

Soy consciente de que has lanzado un desafío al servicio de José Francisco, con el tema de la ventana única para el I+D+i, pero yo, también he de decir que rompo una lanza en favor de ellos, porque han mejorado sensiblemente el tema gracias, precisamente, a la participación en estos proyectos del servicio de innovación y desarrollo de la Jefatura Central de Logística. En lo

que respecta a Policía Científica, hemos tenido muchas más facilidades para poder participar en estos proyectos, con lo cual, está bien lanzado el desafío pero la respuesta ciertamente está siendo, cada vez, más adecuada.

Interviene: Mario Hernández Lores

Me ha gustado mucho un aspecto que has dicho y es que tenemos que perder el miedo a las amenazas; pero me hubiese gustado en otro foro. Aquí, me adhiero más a las tesis de Casimiro, no olvidemos que nosotros somos un objetivo rentable para muchas organizaciones, con lo cual, esa tranquilidad que debe tener el común de los ciudadanos, tal vez nosotros no la debamos tener, debemos de estar más alertas y en atención, sin llegar a los extremos, tal vez, de los que contaba Casimiro; creo que en algunos momentos somos algo descuidados.

Responde: José Antonio Cebrián

Evidentemente, en todo ataque, el factor humano es lo más vulnerable, con lo cual, se responde todo.

Interviene: Antonio López

Voy a intentar resumir mi intervención en dos frases. La primera ya se ha mencionado; dicen que la Ley va siempre mucho más despacio que los avances tecnológicos, y cada vez más. Y, los avances tecnológicos están impulsados por un vector que es el éxito. Cuando un desarrollo tecnológico funciona, todos los demás le copian, lo que constituye, de algún modo, un sistema de propagación más veloz. Por contra, la legislación se basa en el consenso que es algo más lento. Tenemos que acostumbrarnos a trabajar con ello.

Y, segunda, si cabe, más importante. En la investigación, la fuerza de producción es la inteligencia de los investigadores, su formación, su concienciación y su actualización. Tenemos una ventaja estratégica sobre otros cuerpos de seguridad, de otras agencias policiales, y es que, en nuestra manera de selección y de formación, incorporamos muy distintos profesionales; contamos con magníficos ingenieros pero, para que esas personas puedan desarrollar bien sus capacidades, tenemos que contar con una formación básica. La Escuela de Policía tiene mucha tarea por delante.

Entiendo que hay una parte de crítica y que, probablemente, no sea la persona más indicada, pero me he asomado a los planes de formación para escala ejecutiva y no han variado mucho de cuando yo estaba allí. Hay aspectos, en cuanto a Policía Científica, que desde luego estarán actualizados, pero los contenidos son prácticamente los mismos. No he visto nada de informática; el mundo digital se nos ha colado y se nos colará mucho más. Estamos conectados, permanentemente, a nuestros teléfonos; tenemos que asumir este tipo de cosas. Nuestros profesionales tienen que estar formados en materia digital.

Pregunta en sala: José Ángel Sanz, jefe regional de operaciones de la Jefatura de la Rioja, y la pregunta es si se ha sopesado lo siguiente: que dentro de poco -porque nos ponemos como una línea estratégica y lo vemos como la ciberdelincuencia-, no vamos a tener que, en judicial sobre todo, salir a la calle a buscar delincuentes, y esto va a ser una realidad cada vez más, vamos a tener que buscarlos en la red. Pero, a nivel territorial, la dotación tecnológica del material que tenemos es muy deficiente. Sí, esta bien, como ha dicho el Comisario General, en relación a los vehículos dotados de todos esos medios.

Yo, por lo menos, me doy cuenta de que nos estamos quedando, en este aspecto, muy rezagados, que sí que lo tenemos como una medida estratégica muy potente, que no sé si es de ámbitos superiores a la Dirección General de la Policía, pero que se está dejando muy de lado la dotación técnica. Gente, informáticos tengo unos cuantos en Logroño, pero los medios materiales son muy justos, a lo mejor la Comisaría General de Policía Judicial, podría hacer una línea estratégica de dotación, a las Unidades territoriales, de líneas decentes de investigación para abrir cuentas y poder investigar ..., y que no sean descubiertas por los delincuentes. Esto es una cosa que me preocupa.

Interviene: Casimiro Nevado

En relación con la Escuela Nacional de Policía, se han presentado varios proyectos para modificar el plan formativo de la escala ejecutiva, uno de ellos en relación con la creación de una asignatura que se llame ciberinteligencia y destinada para segundo de ejecutiva. No queremos llamarlo ni ciberdelincuencia ni ciberdelitos, queremos que sea algo transversal y que pueda ser válido para cualquier especialidad o cualquier destino que pueda tener un Policía. Seguramente el Comisario General escuchó una frase, una vez, conmigo, en una ponencia: "en el futuro los Guardias Civiles que vayan a un accidente de tráfico, no van a saber si es un accidente o si ha sido un hackeo en coche, y a lo mejor es un homicidio". Tienen que tener las capacidades suficientes como para manejarse y no echarse abajo, a la hora de analizar un dispositivo electrónico. El proyecto de la Escuela es ese, crear una asignatura que sea totalmente transversal, darles esa habilidad a los inspectores que salgan de la Escuela para afrontar cualquier novedad que se tenga en la investigación y que esté relacionada con las nuevas tecnologías.

¿Cuál es el problema? Nosotros, como policías, para modificar cualquier cosa, de cualquier temario; dependemos del permiso que nos de una entidad como es Aneca. Si queremos modificar una coma, nos lo tiene que autorizar esta entidad. Yo no puedo formar a mis policías en este asunto, este año; porque no me lo permite Aneca. Este es el problema real, no es que no haya iniciativas para actualizar los temarios, sino que al final, nosotros que somos la institución, que estamos interesados en formar a nuestros miembros, no nos deja una entidad totalmente ajena a nosotros.

Interviene: Carlos Granada

Creo que para nosotros sí es más fácil, desde el CAE. No tenemos programas, no estamos encadenados a Universidades, a hacer formación. Estaba reflexionando esta tarde, sobre la cantidad de cosas que se han visto hoy y cómo trasladarlas a nuestros especialistas. Yo, voy a los especialistas, no voy a ir en genérico a trasladar esos conocimientos porque creo que es imposible; es imposible dar esa cantidad de conocimientos a todos los policías. Creo que es mucho más útil trasladar esos conocimientos a futuros especialistas, gente seleccionada. Y sí que es posible; pero tenemos que contar con el gran apoyo, como está haciendo la Policía Científica que ha pensado en nosotros. Nosotros, desde la División de Formación, apoyamos la formación especializada, igual que lo podemos hacer en temas tan especializados como el de la ciberdelincuencia. Es un reto, pero si todos nos ponemos, si se ponen las unidades especializadas, nosotros, desde la División de Formación, podemos apoyar esa formación y poner todo lo que tengamos al alcance de las unidades. Dinero no, porque no lo tenemos.

Intervención en sala: efectivamente, en el CAE predomina la idea de especialización, hace unas semanas tuvo lugar, en Guadalajara, el curso de negociación policial. Al curso de negociación policial, que puede ser algo muy especializado, tuve que asistir a dar una conferencia de dos horas de "Uso e investigación de redes sociales", porque, al parecer, los secuestradores, ahora, quieren negociar a través de Twitter, Faacebook..., y los negociadores no saben manejar esas redes sociales. Ya no es cuestión de especialización sino de tener unas bases, un mínimo para afrontar cualquier problema que nos pueda surgir con una tecnología.

Pregunta en sala: José Francisco López

Tengo una pregunta en el sentido de que hay una cosa que no la tengo nada clara y es que dentro de la Policía ¿cómo está estructurado el tema forense, el análisis de temas digitales, informáticos, etc? Hace poco, se ha planteado el tema que está de moda en toda Europa que es el denominado, en ingles, *Automotive*; es decir, análisis forense de la electrónica de vehículos. La cantidad de información que se puede sacar de la electrónica del vehículo, tanto a nivel de investigación judicial como, evidentemente, a nivel de accidentes, es muy grande. Ya los coches vienen teniendo tres o cuatro centralitas diferentes de almacenaje de todo tipo. Los navegadores son una cosa que ya son fáciles de hacer, etc. Yo, a la hora de mandar a un experto, al curso este, no sabía dónde acudir y, entonces, me dijeron que de eso se ocupaban los del Área de Telecomunicaciones; yo creía que los del Área de Telecomunicaciones solo hacían lo de los móviles, pero ahora resulta que hacen todo tipo de electrónica, temas forenses de todo tipo; no sé si tienen la capacidad para firmar un documento pericial, etc. Y, por otro lado, nos hablan de que en la sección térmica de Antonio, hacen análisis forenses en el espacio ciber y es lo mismo que hace Policía Científica ¿Me pueden explicar, de una forma clara, como está distribuido el análisis forense del mundo digital dentro de la Policía?

Interviene: Antonio López

Las labores forenses que hacemos nosotros son de dos tipos. Una es de apoyo a las Unidades de la Comisaría General de Policía Judicial y a algunas otras Comisarías Generales; y luego, se supone, que deberíamos ser capaces de gestionar nuestras propias necesidades. En el primer aspecto, en el de apoyo a la Comisaría General y otras Comisarías Generales, la situación se puede resumir diciendo: "achicando agua". Estamos sacando barriles de agua, para que la cosa no se hunda, no damos abasto, sencillamente. La única manera que tenemos de contener es ilustrar a nuestros clientes y es la de no nos pidáis mucho, pedirnos exactamente lo necesario. Tener en cuenta que vamos a dar una respuesta en un plazo tardío. Esta es la situación.

En lo que se refiere a nuestras propias necesidades, improvisamos sobre la marcha, tal es el cúmulo de nuevas aplicaciones, de nuevos procedimientos en materia forense; de lo que se describe como ciberespacio o el mundo digital, que cuando se nos plantea un desafío -que suele ser para mañana-, tenemos que reservar una serie de profesionales y ver lo que podemos hacer; y así son las cosas. Y, dentro de los vehículos, los servidores simplemente; porque cuando tenemos que analizar un servidor eso es tremendo, no tenemos protocolos. Llevamos un montón de tiempo diciendo que tenemos que traspasarlo al resto de la corporación pero, materialmente, estamos desbordados.

Interviene: Mª Pilar Allué Blasco

Me temo que esto no es solo lo que quería oír José Francisco López, aunque está muy bien respondido, pero me consta que tú querías oír otra cosa y yo no tengo inconveniente en comentarlo, es la pregunta del millón, en la que yo incluiría también a la Comisaría General de Información, es decir: cuatro tipos de unidades policiales trabajando en ámbitos, no voy a decir los mismos, pero sí muy similares ¿Cómo nos coordinamos? Pues con dificultad y como ha dicho el anterior interviniente, en un ámbito en el que tenemos mucha demanda, pocos medios, poca gente y poco tiempo; para dar respuesta a todas las necesidades. Era una de las primeras preguntas que me hice yo al llegar a la Comisaría General ¿Dónde estaba la línea difusa entre la UIT y lo que hacía Informática forense? Y, la respuesta que obtuve, que más o menos me satisfizo y que hemos ido manteniendo durante todo este tiempo; es que Policía Científica responde a los Juzgados y Tribunales en los requerimientos que hacen y Policía Judicial lo que hace es investigar per se. Bien es verdad que, como los que estamos dentro de una corporación global, en la que tenemos que ayudarnos los unos a los otros, cuando no llegan a ayudar a sus unidades territoriales de Policía Judicial, Policía Científica o las Unidades territoriales, echan una mano a Policía Judicial. Este es el resumen tan sencillo y tan complejo al mismo tiempo.

Quiero decir, con ello, que a lo mejor hay que poner encima de la mesa que tenemos que reorganizarnos, ordenar la especialidad, la situación, las

competencias. Claro que hay que ponerse a trabajar, a remangarse para ver cómo nos organizamos y ver cómo rentabilizamos la inversión que hacemos todos y que vienen más o menos a ser parecidas. Tenemos nuestras sinergias, nos cuestan los servicios a nosotros, a vosotros y a Policía Judicial. Información, a lo mejor, es un poco más independiente, tiene más medios y no los pone a disposición porque tiene bastante ocupación con lo que hacen ellos ¿Que quiere decir esto?, ¿que nos lo tenemos que plantear?, pues debo decir que creo que sí, y ayer de hecho se lo comenté al nuevo Director General de la Policía, tal cual. Tenemos que plantearnos rentabilizar el trabajo que hacemos en el ámbito de la informática, al que yo me refiero como informática forense, porque es el nuestro, la investigación electrónica, por decirlo de alguna manera. Creo que tal vez es esto lo que querías oír, Antonio, aunque a esto le puedes añadir mi pregunta respecto de los que "tienen el dinero", los de Logística, que no es otra que porqué ellos tienen unos medios que no tenemos nosotros. Bien es verdad, que los ponen a nuestra disposición y los ponen cuando los necesitamos, pero claro, hay prioridades. Quien tiene los medios, primero intenta solventar sus problemas y luego los de los demás ¿Hay que solucionarlo o solo hay que coordinarlo mejor?

Pregunta en sala: José Francisco López

Se ha planteado desde Comisaría General, utilizar determinadas investigaciones forenses, de una forma externalizada.

Responde: Mª Pilar Allué Blasco

Sí, lo único que ocurre es que no debo dar pistas al respecto en estos momentos, pero sí, se ha planteado y ha sido muy bien recibido por parte del Director General de la Policía actual y, seguramente que abramos el campo; pero el problema siempre está en la financiación, es decir, cuando tú contratas servicios externos para trabajos puntuales lógicamente tienen que estar en el presupuesto y estos están muy limitados, recordad que en algún momento he comentado que solamente se satisface el 15% de la demanda del material inventariable que necesitamos en el ámbito de Policía Científica, como media del presupuesto de los últimos seis años. Contra eso, yo no puedo hacer mucho más; entonces sí que hay que plantearlo, pero no por el hecho de que no podamos hacer ese trabajo o esa investigación, sino porque el volumen es cada vez mayor, la demanda de procesamiento de aparataje electrónico, es cada vez mayor, se han incrementado exponencialmente las capacidades de los ordenadores, de las tablets, de los teléfonos; y necesitas más tiempo, más medios y más gente trabajando. Pero, también, porque hay una faceta de la que hemos hablado que es la de participar en la investigación científica que es cada vez más necesaria.

Nuestro trabajo realmente no es la investigación, científicamente, estos señores, hacen las investigaciones y han ganado los premios trabajando en esos

proyectos en horas de su tiempo libre. Lo que necesitamos es tener la ciencia a nuestro servicio y, para tenerla a nuestro servicio, hay que pagarla. Porque, si destinamos policías a investigar no les destinamos a trabajar que es para lo que los hemos formado, para trabajar como policías. Entonces, necesitamos saber, dónde están los mejores científicos, las mejores técnicas, los mejores profesionales de determinadas materias y, el día que los necesitemos para una investigación propia, poderles contratar. Esto es lo que hay que agilizar. Existía, anteriormente, y sigue existiendo, la figura del contratado laboral y nosotros, todavía, tenemos contratados laborales en la Comisaría General Científica, que fueron los primeros que empezaron con el tema del ADN; y se han mantenido siendo contratados laborales. Esa figura existe, pero económicamente, en periodos de crisis es muy complicado incrementarla.

En definitiva sí, pero mi opinión es que esa figura del contratado ha de ser, sobre todo, para un momento puntual en el que se necesita un servicio muy especializado, y lo puedas pagar y ponerlo a disposición de los jueces con la tutela policial, el respaldo policial y con la garantía policial de trasparencia y fiabilidad.

Interviene: Juan Carlos Castro Estevez

En primer lugar, quiero felicitar a nuestro creativos y alentarles a que sigan creando, innovando, si es posible, para lo que hace falta, evidentemente, inversión. Quizás habría que plantearse si podemos seguir con un presupuesto que data de hace no sé cuánto tiempo, cuando ahora las amenazas, los riesgos y las vulnerabilidades, han cambiado radicalmente y la tecnología para cualquier cosa de estas que estamos hablando aquí o de ciberdelincuencia, cuesta un montón de dinero. Es que, a lo mejor no podemos seguir como hasta ahora. En cualquier caso, yo abogo por la concienciación institucional de cara a la I+D+i, en todos los ámbitos. Concienciación institucional de cara a los presupuestos, institucional y política en el tramo que corresponda. En todos los ámbitos, en el presupuestario, en la remoción de las conciencias; hay cosas que no cuestan dinero, es simplemente querer hacerlo, porque tienes que tener el convencimiento de que eso, en este tiempo, en la actualidad, es así, y tiene que ser así.

Hablaba en mi conferencia de la alineación de recursos en las diferentes administraciones o en el ámbito de una misma administración. En la administración central, no podemos continuar dando seguridad con el policía de la puerta a un montón de edificios a los que tradicionalmente se ha venido dando, incluyendo otros ramos ministeriales al margen del Ministerio del Interior. Hay que concienciar y hay que implementar medidas físicas y/o electrónicas cuando no, seguridad privada, y me atrevo a decir, que personal laboral. Porque, no todas las funciones que desarrolla un Policía en la puerta o en el entorno de la entrada de un edificio público, como puede ser un

simple control de accesos, lo tiene que hacer un vigilante de seguridad, lo podría hacer personal laboral que es infinitamente más barato.

Yo no sé si alguien se ha parado a pensar lo que nos cuesta el DNI a la Policía, no sé si alguien se ha puesto a pensar lo que nos cuestan los policías que desarrollan el trabajo de los cuerpos generales en cualquier dependencia policial. Yo, desde luego, soy partidario de que los creativos de la Policía puedan crear y no solo en su tiempo libre. Tenemos que pensar en un lugar donde esté toda esta gente, tenemos que desarrollar una unidad que sea capaz de saber qué es lo que se ahorra una empresa cuando entra en el capítulo de innovación, no solamente con beneficios fiscales nacionales, sino con beneficios fiscales de I+D+i, de la Unión Europea y, sabiendo lo que se ahorra, podremos llegar a un convenio, a un acuerdo, para que, por ejemplo, la nariz artificial o el big data, le salga gratis a la Policía, porque ponemos un esfuerzo, independientemente de que la empresa pueda materializar el proyecto.

Estoy completamente a favor de la externalización de servicios. Lo están haciendo los bancos, desde hace mucho tiempo, que manejan una información muy similar a la nuestra, con datos de carácter personal, por ejemplo en materia de informática. Tenemos un montón de ingenieros informáticos, algunos de los cuales están cambiando el tóner de las impresoras en las comisarías. Esto es una realidad. Por tanto, concienciación.

Respecto a la intervención de la tarde, todos los perros huelen, unos mejor y otros peor y ¿qué huelen?, todo lo que desprende algún olor. Nosotros, lo que hacemos es jugar con ellos y modificarles las conductas de respuesta, es decir, cuando huelas heroína, lo muerdes, lo sacas y juegas conmigo; cuando huelas un explosivo no te muevas, es más, no te acerques, huélelo de lejos y siéntate.

Los compuestos no huelen a la suma de todos sus ingredientes, por eso entrenamos a los perros para oler TATP; si fuera la suma de cada una de las sustancias, siendo el explosivo tan inestable como es, no tendríamos que ir al INTA, les enseñaríamos a detectar cada uno de los ingredientes, por separado, pero eso no nos llevaría a concluir que nos encontramos ante ese explosivo concreto.

Ahora bien, si al final la nariz artificial se desarrolla de tal manera que identificara, por ejemplo, la tinta y otros componentes de los billetes de euro, que supuestamente huelen todos igual, por lo menos en cada tipo de billete, no tendríamos que entrenar perros para eso. Tampoco para detectar explosivos que, además, encierra un peligro importante. Hay determinadas razas que tienen un olfato extraordinario, pero no servirían para pertenecer a la especialidad de explosivos, porque no lo pueden coger ni tocar, sin embargo,

la respuesta ante la droga es justo la contraria. Pero, si la nariz oliera eso, eliminaría esa especialidad concreta, no la de guías caninos. También lo dije en mi ponencia, una cosa son los olores y otra cosa la presencia, tenemos perros de defensa y ataque, y podemos promover otros desarrollos; se imaginan que yo enseño a un perro a tener una respuesta concreta ante un individuo señalado por una luz roja de un puntero láser. Hay que tener en cuenta que la compra y el mantenimiento de los perros tiene unos costes y, además, no podemos disponer permanentemente de ellos, de todas las especialidades, en todas y cada una de las plantillas.

Y, por último y hablando de mi intervención, creatividad e innovación se diferencian en la inversión solo y exclusivamente. En un desarrollo oportuno y consciente, racional y lógico. La innovación no se ciñe exclusivamente al campo de la tecnología, hay mucha innovación en la forma de hacer las cosas.

Hay que remover conciencias, obtener sinergias y alinear recursos de los organismos del Estado. Alinear los recursos del Estado significa, por ejemplo, que con Instituciones Penitenciarias tenemos que llegar a un acuerdo pero en la cúpula; no puede ser que cualquier preso se ponga ligeramente enfermo y tengamos que poner un "Z" para llevarlo al hospital, manteniendo una pareja de policías custodiándolo durante su estancia en el mismo, que puede ser de varios días. Hay que abogar porque haya un médico en la prisión que pueda atender este tipo de cosas o porque los hospitales dispongan de módulos especiales para atender esta problemática, que nos llevaría a gestionar estos asuntos de manera más eficiente, con un número de policías mucho más ajustado.

Desde el punto de vista de la judicatura, no puede ser que una persona, un viernes por la tarde, a última hora, realice una denuncia que conlleva un riesgo extremo y tengamos paralizado un "Z" durante todo el fin de semana, hasta que el lunes llegue el juez y se pronuncie sobre dicho asunto ¡No puede ser! Tendría que haber un juez de guardia, algo; porque el Policía no es gratis y, además, ese "Z" de una plantilla intermedia de España -no hace falta que sea la más pequeña- saca dos o tres "Z" por turno, de forma que tiene que prescindir de un porcentaje importante de efectivos si paraliza ese recurso.

Invertir adecuadamente significa establecer un equilibrio adecuado entre problemas y soluciones, asignando prioridades. Yo necesito muchos policías en Seguridad Ciudadana; estos señores necesitan mucha inversión en tecnología y alguien tiene que ser capaz de poner en valor toda estas cosas, independientemente de que a lo mejor lo primero es abogar por incrementar el presupuesto, porque si no, acabaremos en la locura de Einstein, haciendo siempre lo mismo no vamos a salir del atolladero.

En formación, evidentemente, tenemos que incluir todas estas cosas novedosas que estamos viviendo desde hace unos años, las tenemos que incluir en nuestros programas de formación.

Hace dos años, se puso en marcha, desde el Centro de Altos Estudios Policiales, del que fui director durante un tiempo, un master en ciberdelincuencia, a mí me hubiera gustado más llamarle ciberseguridad. Me consta que hubo una segunda edición y desconozco si habrá una tercera. Nos ocupamos de incluir en el programa todo esto de la ciberdelincuencia forense y no forense, nos ocupamos de que las Comisarías Generales de Policía Científica, Información y Judicial, estuvieran representadas. En fin, tiene que haber una formación de carácter global y otra para especialistas, como era esta.

Echo de menos la concienciación institucional; para haber concienciación tiene que haber información. No podemos hablar de seguridad informática o del mundo ciber, sin decir a la gente que tiene que recoger los papeles de su despacho, todos los días, porque ahí entra un señor o señora de la limpieza. De mi despacho, poco se puede llevar, pero hay otros despachos de los que se pueden llevar muchas cosas, y probablemente haya papeles rodando por ahí.

Tenemos que comenzar a concienciar de lo básico. A lo mejor no todos somos conscientes de que debemos recoger los papeles de nuestro despacho, que cada despacho debe tener una llave, que la llave no la puede coger cualquiera. A lo mejor tenemos que pensar en "capar" los ordenadores para no poder meter o sacar información en CD o pendrives que nos pueden incluir algún virus. Deberíamos conocer todos que un programa instalado en un ordenador personal puede distribuir un documento oficial sin que nos demos cuenta, cuando trabajamos con él en casa para adelantar nuestro trabajo.

Pregunta en sala: El Policía de futuro, por dónde van las cosas.

Responde: Juan Carlos Castro Estevez

El Policía del futuro, en el ámbito de las unidades básicas de seguridad ciudadana, es un poco como el coche inteligente. El Policía de futuro es alguien perfectamente formado, que va en un vehículo dotado con las herramientas suficientes y necesarias para garantizar la realización de un servicio efectivo y su propia seguridad, que dispone de una tablet que puede sacar del coche en un momento dado para entrar en determinadas bases policiales de una manera fácil y sencilla, pasando los documentos sin tener que teclear un DNI, un NIE o un pasaporte de cualquier país, para comprobar una filiación. O le haces una foto al pasaporte y lo mandas a extranjería, para complementar la información que solo un especialista puede aportar. El Policía del futuro es alguien que pudiera llevar una pistola taser ¿Todas las unidades? Habría que matizar. Con una cámara asociada para que cuando

haces uso de la taser, se ponga en marcha el prerecording que graba las imágenes visualizadas con anterioridad al uso de la taser, determinado por qué se ha utilizado y cómo. El Policía del futuro es alguien que lleva un chaleco antibalas de alta protección.

Pregunta en sala: ¿Va a poder participar, en estos programas, la Policía Local?

Responde: Juan Carlos Castro Estevez

Como dije en mi exposición estamos obligados a colaborar con las Policías Locales, son nuestros cómplices en las ciento setenta y siete (177) ciudades más importantes de España, donde la delincuencia acucia y la problemática policial relacionada con cualquier tipo de evento genera acumulaciones de masas y numerosas actuaciones de orden público muy complejas. Además, mientras estemos en el nivel cuatro (4) de prevención y protección antiterrorista, tenemos que colaborar y coordinarnos intensamente con las Policías Municipales y los Ayuntamientos, solicitando la implementación de medidas relacionadas con restricciones del tráfico rodado y la colocación de grandes estructuras, maceteros y bolardos en determinados lugares de las ciudades para establecer zonas seguras ante cualquier celebración multitudinaria.

En este sentido, hemos conseguido que las Fuerzas Armadas nos cedan un BMR que pesa dieciocho toneladas (18T) y nos están preparando otro para esos dispositivos multitudinarios, como pueden ser las celebraciones de determinados partidos de futbol o cualquier otro evento que lo requiera. Este tipo de vehículos es fundamental en este tipo de circunstancias, pues permite cambiarlo de posición en muy poco tiempo, de acuerdo con las necesidades operativas de las unidades participantes

Interviene: Mario Hernández Lores

Un apunte sobre el curso de ciberdelincuencia; se hizo la primera edición con mucho éxito, se volvió a hacer una segunda edición y está aprobada una tercera que se convocará en el mes de julio de 2018; y el curso lo patrocina la Fundación Policía Española. También, promociona becas en esta materia. Pero es la Policía y los Cuerpos Generales del Estado los que deben promocionar estas cosas ya que la Fundación está limitada con sus recursos económicos y hace lo que puede.

Interviene: Mª Pilar Allué Blasco

Quería lanzar un envite al director de la Fundación Policía Española y a los presentes de la mesa que, al fin y al cabo, no dejan de ser el futuro de lo que será la Policía; entonces, como decía Forges: "Y no os olvidéis de ...". Yo voy a decir: "no os olvidéis de la gestión del conocimiento", de la que no hemos hablado nada. Hemos hablado de gente que sabe mucho, de lo que

está trabajando, de que tienen mucha formación pero que cuando cambia de destino, se va con la formación puesta y no se queda en el lugar de trabajo, creo sinceramente que es una asignatura que tenemos pendiente.

Interviene: Mario Hernández Lores

Tenía medio pensado el tema del siguiente curso y, después de la conversación que tuvimos, lo he puesto en duda; por lo tanto, ya tengo dos, el que tenía antes y el otro que será la gestión del conocimiento en la Policía.

Quinto Panel: i+d+i en la seguridad privada y en la gestión de la seguridad en inmigración y fronteras

POLICÍA NACIONAL: INNOVACIONES TECNOLÓGICAS EN EL ÁMBITO DE LA SEGURIDAD PRIVADA

JAVIER GALVÁN RUIZ
Comisario del CNP, Jefe Brigada Central de Inspección e Investigación de la Unidad Central de Seguridad Privada

España es un país seguro por las políticas públicas de seguridad que ejerce el Ministerio del Interior, por el desarrollo de la actividad planificada y estratégica de la Policía Nacional y demás cuerpos y fuerzas de seguridad, y sería injusto no citar a la seguridad privada.

Existe un gran abanico de miles y miles de servicios, de seguridad privada, en los que participa en la seguridad ciudadana y, por qué no decirlo, en la seguridad nacional; dando cobertura en asuntos de seguridad ciudadana a los servicios de seguridad y a los servicios de inteligencia.

Los objetivos de la seguridad privada en España han cambiado paralelamente a los objetivos de la seguridad pública, es decir, a las demandas de seguridad que tenemos en España. Cuando se hace la Ley del año 1994 de Seguridad Privada, los problemas para cubrir las incidencias delictivas eran diferentes a las que hay hoy. Estamos hablando de dar cobertura a estancos, farmacias e incluso entidades bancarias, aunque estas sigan teniendo sus medidas, para evolucionar en cuestiones de ciberdelincuencia, contraterrorismo, protección de infraestructuras estratégicas, etc.

Todos los productos que ofrece la empresa a las demandas de la seguridad privada, tecnológicos y de desarrollo para que puedan prestar sus servicios,

van en paralelo al resto de empresas que establecen sus otros productos para el tejido empresarial o el tejido personal.

Estos avances, esta innovación tecnológica en el ámbito de la seguridad privada se ha visto reforzada y utilizada por los servicios públicos de seguridad.

Vamos a establecer dos parámetros: la carga presupuestaria de la Administración Pública y la normativa que puede comprometer la utilización de determinadas cuestiones, en concreto los datos que generan estos instrumentos. Desde el ámbito de la seguridad pública y desde el ámbito de la Policía Nacional, nuestros sistemas tecnológicos y de innovación, van en paralelo con la seguridad privada, pero en muchas ocasiones los de seguridad privada, van por delante y nosotros, gracias a los marcos de colaboración que tenemos con ellos, en concreto, con el plan de colaboración "red azul"; evidentemente nos podemos aprovechar de ellos en beneficio de los ciudadanos; habrán oído hablar de los centros inteligentes de mando y control, es decir, la transformación de las salas del 091.

Pues bien, ¿qué tiene que ver la seguridad privada y sus instrumentos y sus avances tecnológicos con esos centros inteligentes? Desde la Unidad Central de Seguridad Privada, se está trabajando en diversos proyectos para dar más seguridad al ciudadano y a los policías actuantes, por ejemplo, se están estableciendo plataformas tecnológicas para el traspaso de archivos de vídeo e imágenes de las centrales receptoras de alarma en el caso de intrusismo o robos con fuerza en vivienda para que, de manera automática y en el tiempo real, se trasladen a estos centros inteligentes de mando y control y estos, a su vez, puedan derivarlos a nuestras patrullas; con lo que el patrullero, en los componentes del vehículo zeta y cuando se aproximan a un domicilio en el que ha saltado una alarma, pueda saber qué está sucediendo y pueda tomar las medidas de protección oportunas.

También, en el ámbito bancario se están desarrollando este tipo de plataformas en las que las propias "TRAs" (central de alarma del banco) de uso propio, van a trasladar en tiempo real el grupo de archivos de vídeo y de imágenes de una sucursal, cuando se produzca un salto de alarma con incidente crítico, por ejemplo, un atraco. Y, esto va a permitir que tanto el Centro de Inteligencia de Mando y Control y las patrullas actuantes realicen con mayor seguridad sus actuaciones.

Por otro lado, en el ámbito del Registro Nacional de Seguridad Privada que está también en el ámbito de la seguridad ciudadana, porque nosotros, la Unidad Central, pertenecemos a ese ámbito; es donde se inscriben y donde

se graban todos los servicios y todas las entidades de seguridad privada; y queremos geoposicionarlo. Estamos trabajando para que todos los servicios que se almacenan en las propias empresas de seguridad privada, con un servicio de vigilantes de seguridad plasmado aquí, en la puerta, sean posicionados y trasladados a nuestros centros inteligentes de mando y control.

Un ejemplo, hace unas semanas, un vigilante de seguridad fue agredido en una planta de un hospital de Madrid, se llamó al 091; llegado el 091, revisó todo el hospital y no lo encontraba; tuvo que ir otra patrulla y lo encontraron herido con un apuñalamiento en el estómago y con varios golpes en la cabeza; bien, en el área de Policía Científica, nuestros compañeros han participado en el diseño reglamentario de la Ley de Seguridad Privada y nos han trasladado que, para hacer la verificación, para hacer la vídeo identificación o la captura de imágenes y de video vigilancia, nuestros peritos a la hora de actuar ante tribunales se ven muy comprometidos; y nos han establecido una serie de características que deberán tener las cámaras de video vigilancia para poder realizar ese tipo de actividades; pues bien, hoy ya se incluyen.

En el ámbito de la seguridad privada ¿qué herramientas se utilizan? El avance y la innovación de la seguridad privada y de los servicios de seguridad privada tienen una base que es la biblio vigilancia. Hoy en día, el servicio cerrado de cámaras de televisión se ha visto prominentemente superado por los servicios de biblio vigilancia que son sistemas adscritos a la red y que se encuentran securizados. A través de repositorios sobre el análisis de vídeos de los propietarios se coge, en la nube, un espacio para grabar todo lo que las cámaras de video vigilancia de mi empresa y de todos los servicios que se dan -pues están dando servicio al cliente-; o a través del servicios contratados. Contrato un servicio de almacenamiento que lo que hace es expandir el sistema empresarial, es decir, dan la oportunidad a la empresa de utilizar más resolución en las cámaras y más almacenaje y esto les reporta beneficios. Y también se crean una serie de megadatos, el famoso Big Data, que no solo se utiliza con capacidad empresarial sino que, a través de los canales de colaboración, son trasladados a la Administración Pública, a los servicios de seguridad y de inteligencia; y esos megadatos son importantes porque tras su análisis y tratamiento así como su conversión en inteligencia nos dan zonificaciones, flujos de personas, vehículos, horarios de concentración; nos dan clasificación de sexo y tramos de edad.

Otro aspecto innovador es el de las cámaras móviles que se utilizan por la seguridad privada. Las cámaras móviles de alta resolución la ley las permite ubicar en vehículos, animales, personas …, como la utilizan nuestros grupos especiales, la seguridad pública o nuestro ejército y, además, han evolucio-

nado, por ejemplo, las cámaras que se mueven en cuatro ejes en los estadios de alta resolución que se llaman "cámaras cautivas" y que dan una visión de trescientos sesenta grados "tres d".

La maculación de billetes, el entintado de billetes. Un gran problema que tiene el sector bancario a nivel delincuencial es el robo con fuerza y con explosivos en los cajeros automáticos o en el transporte de fondos -los blindados-. Se está trabajando en la Unidad Central de Seguridad Privada, Policía Nacional, con las cuatro empresas de referencia, de nivel internacional, que se dedican a crear cajetines geoposicionados con una tecnología espectacular entintando billetes para que se puedan reducir costes y demos mayor seguridad y garantía al transporte. Que no nos explote un cajero por la noche cuando pasa una persona y la pueda matar.

Otro sistema de innovación es el sistema de ofuscación; este sistema de ofuscación ¿qué quiere decir? Cuando se pone una alarma en casa o establecimiento se puede crear un dispositivo, contratar un servicio, en el que se establezca una herramienta química que produzca humo. Esto está siendo eficaz al cien por cien. La innovación ha ido a más, ha cambiado de los químico a lo pirotécnico, y esto está dando un gran resultado en la prevención con robos con fuerza; delitos que han sido los que más nos han perjudicado según las estadísticas MIR, del Ministerio del Interior, de toda España y del exterior. A título de curiosidad, cuando saltaba este sistema, los bomberos salían y claro se producían falsas alarmas; ahora se han creado protocolos en los centros de inteligencia de mando y control de la Policía y de los servicios de emergencia de toda España para que se avise antes de salir en casos de detectar el humo.

En ciberseguridad, imagínense los presupuestos que tienen las empresas privadas, negocios para dar seguridad privada en España para proteger sus activos, pues bien, la Policía Nacional como autoridad nacional de control de las seguridad privada y habiendo elaborado el borrador de la ley que se ha aprobado en al año 2014 y el borrador del reglamento que se va a aprobar en un futuro, ha tenido en cuenta la regulación de la ciberseguridad; de los servicios de ciberseguridad elaborados por la seguridad privada; así, en ese borrador, en ese reglamento y en esa ley se incluyen las actividades de seguridad informática, los requisitos de las empresas prestadoras así como el régimen general de auditorías externas, es decir, es un avance espectacular en algo que se estaba haciendo ya a nivel de ciber, de protección, por parte de la seguridad privada, por parte de la Administración Pública y por parte de la Policía Nacional.

La biometría de voz. Aquellos sistemas de verificación en los accesos y controles y en la gestión propia de una empresa, a ellos, a las empresas, les preocupa mucho su activo, que es la información, la de todos. Están evolucionando en el establecimiento de sistemas de contraseña de voz, pero a la vez, están estableciendo sistemas de reconocimiento de lenguaje natural, es decir, la empresa tiene que tener controlado todo tipo de información y evitar que haya fuga de información por parte de sus dispositivos telefónicos.

Este sistema permite identificar a cualquier empleado que use cualquier medio tecnológico o medio telefónico de empresa y por último, fíjense hasta donde está avanzando la empresa privada que suministra este tipo de herramientas en el ámbito de la seguridad privada, se está elaborando un sistema de análisis del sentimiento de los hablantes que analiza el vocabulario utilizado en una conversación y el estado emocional de los interlocutores. Esto genera a nivel empresarial mucho dinero.

No quiero terminar sin hablar del problema que supone el terrorismo internacional que sufrimos; hoy en día toda innovación tecnológica está condicionada al establecimiento de medidas flexibles de seguridad; hay que quitarlas y ponerlas, ante incidentes terroristas en la pública.

Un desarrollo importante: en el grupo especial de operaciones GEO, y en un ámbito de trabajo de seguridad privada, nos decían que tienen un grupo SOT encargado de la innovación y el desarrollo tecnológico de todas aquellas actividades que beben de todas las asignaciones que les hacen faltan a este grupo especial de operaciones.

Se está analizando, en este momento, cómo debe ser la protección de los chalecos antibalas que utilizan nuestros agentes tras el incidente que se produjo en Guadarrama y en el que una bala penetró en el cuerpo del agente. En un estadio de futbol podrán comprobar que hay quinientos o seiscientos vigilantes en un partido, por ejemplo, de la copa de champion y van a cuerpo descubierto. Existe una actividad tremenda por parte de los sindicatos, de los trabajadores de seguridad privada, para que se implementen medidas de protección corporativa no solo en los espectáculos públicos sino en zonas públicas. Si alguien quiere saber los que se produce un sábado por la noche en el puerto de Alicante …, intervienen ellos primero. Por lo tanto, hay que trabajar toda esa innovación.

No quiero terminar sin recalcar que España sigue siendo un país seguro gracias a la seguridad pública y, por supuesto, a la seguridad privada.

LA TECNOLOGÍA AL SERVICIO DE LA SEGURIDAD EN LAS FRONTERAS

FERNANDO ALONSO AVILÉS
Comisario del CNP,
Jefe Actual de la Unidad Central de Fronteras

La situación que se presenta en las fronteras es algo que el ciudadano normal percibe diariamente porque todos viajamos. En este ámbito, el número de personas que tenemos destinados en puestos fronterizos está limitado por un gasto presupuestario y el flujo de pasajeros que nos encontramos en los puestos fronterizos va aumentando de una manera exponencial. Manejar esos flujos de pasajeros con los medios tradicionales ya sabemos todos que es imposible. De hecho, cuando llegamos al aeropuerto hay determinados medios técnicos a los cuales cada vez estamos más habituados. Nuestro objetivo, dentro de la Comisaría General en colaboración con los responsables y las empresas que gestionan también los puestos fronterizos, es intentar agilizar el paso de los pasajeros y que la seguridad sea máxima. Es así de sencillo pero, a su vez, así de complicado. Normalmente, los policías cuando estamos en nuestro ámbito, percibimos de una manera diferente los retrasos o las esperas en el aeropuerto. Cuando nos pasamos a pasajeros somos los propios policías los que, también, protestamos. Esa capacidad de empatizar con esa situación es importante. Cuando viajéis y guardéis una fila o tengáis que pasar un control, os daréis cuenta que os enfadáis.Y ¿a quién se mira? Se mira a quien está de uniforme y muchas veces hacemos responsable a quien no lo es.

El número de pasajeros ha aumentado de una manera exponencial ¿cuáles son las medidas que tecnológicamente tenemos para controlar esto? Unas que las vamos a establecer a priori y que son muy comunes como son el VIS, cuando viajamos a un país necesitamos que, en determinados países,

nos otorguen un visado y, por lo tanto, hay un control previo de esa persona cuando acude a nuestro país. Ahora bien, no todos los países tienen necesidad de visado y no se les hace ese control previo.

Al que se le hace ese control previo va a ser una persona a la que se toman todos sus datos biométricos, sus huellas, su fotografía y se incluyen en su etiquetado y visado y que va a ir en su pasaporte. Este es un control previo que nos posibilita que, antes de que esa persona llegue a nuestro país, tengamos un conocimiento sobre esa persona.

De la misma manera, otro sistema de control sería la información avanzada de pasajeros. Las compañías tienen la obligación de transmitirnos la información de todos los pasajeros que van embarcados ¿Qué nos posibilita esto? Chequearlo contra nuestras bases de datos, es decir, que un pasajero antes de llegar a nuestras fronteras sufra un control previo, que haya tenido un control sobre su persona. Una, por parte de la compañía aérea que tiene la obligación, bajo sanción si no lo cumple, de mandarnos la lista de pasajeros, y que es chequeada con nuestras bases de datos; y otra, si esa persona necesita visado -el chequeo en profundidad de la situación de esa persona y de su identidad, de todos sus datos biométricos, de las condiciones y del lugar al que a va ir dentro de nuestro país-.

La Unión Europea entiende que hay que reforzar más estas medidas. Dentro de los proyectos de Smart borders ha establecido un supuesto similar al que Estados Unidos tiene con el "ESTA" (Sistema Electrónico para la autenticación de viaje). En breve, todos los ciudadanos que quieran entrar en la Unión Europea -aparte de los que necesiten visado, de los que no necesiten visado o de cualquier ciudadano-, van a tener que registrarse mediante el sistema denominado "ETIAS" que es como el "ESTA", todos los ciudadanos tendrán que registrarse en un registro previo y comunicarlo a las fuerzas de seguridad para hacer un chequeo y tener más información de esa persona antes de que llegue al país ¿De qué se trata? Se trata de hacer el control fuera del país, si lo podemos hacer fuera, mejor; nos va a dar menos problemas que una vez que llegue a la frontera.

Esto genera mayor seguridad, mayor información y menores denegaciones de entrada. Posibilita denegar menos la entrada a ciudadanos que acuden a nuestras fronteras. Este proyecto es fundamental en la Unión Europea porque abarcamos a todos los países y no solo a los que tienen visado sino a los que no lo tienen también. Tendremos una información previa que Policía puede manejar. Y digo Policía porque, por ahora, Policía Nacional es la responsable de la entrada y salida del territorio nacional de los ciudadanos, una responsabilidad que tienen la Policía Nacional que no es delegadable y que se tiene que ejercer.

Estas son medidas que se tomarían antes de que el ciudadano entrase en nuestro país; pero una vez que ya está en nuestras fronteras, en nuestro puesto fronterizo, también la Unión Europea -la Comisión-, ha entendido que dentro del proyecto Smart Border, concepto de fronteras inteligentes, que se creó a partir del año 2011, la Comisión Europea entiende que debe formar parte de la actividad en fronteras de todos los países de la Unión en cuanto que establece un proyecto ambicioso y que: el que haya una entrada y salida, o sea lo que denominan Entry-exit a nivel europeo, es decir, que cualquier ciudadano que entre por cualquiera de nuestras fronteras sea chequeado de manera telemática o informática, de tal manera que quede registrado su paso por nuestra frontera. Pero, también su salida, y no sea un sistema no a nivel nacional como ocurre hasta ahora, sino a nivel europeo, integrado a nivel europeo. El caso parece, aparentemente sencillo, pero realmente es bastante complejo, organizar a todos los países de la Unión Europea y establecer que en las fronteras, que para el año 2025 habrá cerca de unos trescientos millones de movimientos dentro de la Unión Europea, todos esos movimientos queden registrados informáticamente y puedan ser consultados posibilitando, de esta manera, quién ha entrado en nuestro país, si tiene sobre estancia y si ha pasado su tiempo de sobre estancia. Que nos posibilita también, que no sea necesario el sellado de su pasaporte, en cuanto que el sellado es electrónico.

Todo este tipo de cuestiones van a afectar en gran medida a la seguridad y van a influir en la gestión de política de visados y de inmigración, puesto que vamos a saber dónde se quedan las personas, por dónde entran, por dónde salen y las nacionalidades que inciden más en la inmigración irregular.

Por poner un caso, de una nacionalidad cualquiera, se detecta que entra una gran cantidad de personas en la Unión Europea y no salen; eso quiere decir que esa nacionalidad podría ser sometida o cambiada su situación respecto al visado; que se le requiera o no se le requiera el visado. A la hora de gestionar la inmigración dentro de la Unión Europea resulta un elemento fundamental. A parte de la posibilidad de denegaciones de entrada de una manera mucho más ágil y de un mayor control en materia de seguridad.

Hay que tener en cuenta que en España tenemos ochenta y un puesto fronterizos Schengen, cuarenta y tres fronteras aéreas, treinta y cuatro marítimas y cuatro terrestres, muy complicadas. La gestión de todos estos a nivel europeo está focalizada en EU-LISA, Agencia Europea de la Gestión Operativa de Sistemas Informáticos de Gran Magnitud y que es la responsable de gestionar la interoperatividad de todos los sistemas informáticos, de todos los sistemas, de todas las bases de datos que tenemos en la Unión Europea, y que lo que pretende es que cuando una persona sea chequeada en un puesto fronterizo se la consulte, de manera automática, en todas las bases de datos.

Los que llevan un pasaporte electrónico y, como sabemos, gracias a la evolución de los documentos de viaje, que a la vez tienen más medidas de seguridad, más información, podemos chequear la identidad de la persona, como a la vez realizar una consulta en la base de datos de una manera mucho más ágil. Esta interoperatividad es el reto que tiene la Unión Europea a corto plazo por motivos de seguridad.

Unir la seguridad a las fronteras es algo evidente, pero también unir la libertad de movimientos, que estas fronteras no supongan una falta de libertad de movimientos para el ciudadano, un entorpecimiento de la economía, de las empresas que intentan funcionar desde la Unión Europea hacia fuera y viceversa; y ese es el objetivo.

Ahora mismo, en estos mismos instantes, en el aeropuerto de Madrid-Barajas se está implementando un número de ABC (Automated Border Control), de puertas inteligentes de acceso, con conexión a las bases de datos de manera automática. Este mismo verano ya estarán implementados. En Palma de Mallorca, ya están implementadas en un número bastante elevado. En Barcelona también se han incrementado. En este verano 2018 está previsto la implementación en Málaga, Granada, Alicante … Esto no es el futuro, es el presente y el objetivo es que la agilidad en los puestos fronterizos sea cada vez mayor, que el ciudadano se sienta seguro, pero que a la vez se realice un control exhaustivo de las personas que entran.

No solo es el control de seguridad del pasaporte; esa es una cuestión que nosotros discutimos mucho con las compañías y con otros gestores. La inspección de seguridad en un puesto fronterizo conlleva no solo que le chequeen el pasaporte, conlleva que se pueda detectar una víctima de tráfico de personas, una víctima de trata de personas, un menor en desamparo o un tráfico de menores o cualquier otro tipo de delito. En este sentido hago una pequeña referencia al PNR que todos llevamos escuchando bastante tiempo y que no gestiona la Comisaría General de manera directa, la gestiona el Cisco; porque el PNR no es un elemento de seguridad fronteriza propiamente dicho, no es un elemento de control fronterizo, es un elemento de lucha contra el crimen organizado y contra el terrorismo y que afecta de manera directa al paso fronterizo, puesto que la información la facilitan las compañías que gestionan los viajes.

Fundamentalmente, esta es la imagen que quiero enviarles respecto a los objetivos que tiene la Comisión Europea y hacer suyos España respecto a la mejora de los puestos fronterizos, la mejora de la tecnología aplicada y que el ciudadano, ahora, cuando viaja, lo pueda comprobar; porque vamos a introducir el pasaporte electrónico tanto en la entrada como en la salida

del puesto fronterizo por el sistema ABC y va a ser chequeado y registrado contra las bases de datos.

Ese sistema no es que impida que el policía de fronteras siga cumpliendo con un trabajo fundamental, sino que le va a posibilitar lo que hemos dicho, que enfoque su trabajo a otra serie de trabajos más policiales y más especializados y que son la detección de víctimas, de organizaciones y la de cualquier hecho delictivo que se pueda producir en fronteras.

POWERPOINT


POLICIA NACIONAL
FRONTERAS INTELIGENTES
¿Cuál es la situación?
✓ Incremento considerable en el flujo de pasajeros.
✓ Imposibilidad de manejar esos flujos con métodos tradicionales.
✓ Facilitación, agilidad en el cruce de fronteras / mejora de la seguridad.
✓ Necesidad de incorporar nuevos sistemas tecnológicos con protocolos comunes.
2


POLICIA NACIONAL
FRONTERAS INTELIGENTES
✓ Se espera que para el año 2025 el número de pasajeros fuera de la UE casi se duplique.
✓ La gestión del control fronterizo actual y no será viable:
• Aumentar el número de aeropuertos, puertos y puestos fronterizos terrestres es demasiado caro.
• Tener en cuenta los inconvenientes que genera al pasajero principalmente por el aumento del tiempo de espera y las filas.
• El aumento en el número de agentes fronterizos no garantiza un control óptimo.
300 million
190 million
2014
2025
3


POLICIA NACIONAL
FRONTERAS INTELIGENTES
CONCEPTO
¿Qué son las fronteras inteligentes?
❖ La Optimización de recursos técnicos y humanos, así como la implementación de criterios homogéneos para lograr:
✓ Coordinación y gestión integral de todos los puestos fronterizos.
✓ Control óptimo del pasajero
✓ Procesamiento de grandes cantidades de información.
4


POLICIA NACIONAL
FRONTERAS INTELIGENTES
¿Qué son las fronteras inteligentes?
1. El concepto de Fronteras Inteligentes nació en octubre de 2011 dentro de la Comisión Europea.
2.- La Policía Nacional ya lo recoge en el Plan Estratégico, proponiendo la interconexión y el uso de todos los sistemas técnicos dedicados a la inspección fronteriza.
5


POLICIA NACIONAL
FRONTERAS INTELIGENTES
Operativa de las fronteras inteligentes
Interconexión de todos y cada uno de los sistemas informáticos y técnicos de todos los puestos fronterizos europeos.
Acceso ágil a la información operacional por el agente fronterizo.
Un sistema avanzado que ofrece la información de los pasajeros en conflicto antes de su llegada, con el fin de discriminarlo del resto.
Acelera el paso a través de los cruces de fronteras exteriores de los viajeros "habituales".
Creación de una herramienta capaz de recopilar y gestionar la información de los pasos de entrada y salida de los viajeros y su posterior explotación a nivel europeo.
Reducir los tiempos de espera de los viajeros en los controles fronterizos y al mismo tiempo respete los niveles de seguridad requeridos por la Unión Europea.
6


POLICÍA NACIONAL
SISTEMAS TÉCNICOS IMPLANTADOS EN LAS FRONTERAS ESPAÑOLAS
ABC – Automated Border Control (2010)
API – Advanced Passenger Information System (2007)
VIS – Visa Information System (2011)
FADO – False & and Authentic Documents On line (IFADO)
Sistema Nacional de Entrada / Salida
EN DESARROLLO POR LA UE O EN CONSIDERACIÓN
ETIAS - Sistema Europeo de Información y Autorización de Viajes
PNR – Información Completa sobre Pasajeros (*)
EES – Sistema UE para registro de entrada / salida de TCN (ABC4EU, EU-LISA, RTP/NFP)
(*) No es un sistema de control en fronteras


POLICÍA NACIONAL
E.E.S Y R.T.P
El programa Smart Boders se compone de dos sistemas:
E E S (Entry - Exit System / Sistema Entrada y Salida) en el que s integra el RTP (Registered Traveller Programme) actualmente NFP (National Facilitation Programme
ETIAS Sistema Europeo de Información y Autorización de Viajes.
EES
RTP/NFP


POLICIA NACIONAL
FRONTERAS INTELIGENTES
SISTEMA ABC
ABC
Automated Border Control
9


POLICIA NACIONAL
FRONTERAS INTELIGENTES
SISTEMA ABC
NUEVO CONCEPTO DE CONTROL
ABC system
Aumento de los ciudadanos de la UE cruzando las fronteras.
Más Paises Europeos con ABC..
Permite la reducción de recursos humanos y mantiene un control óptimo.
10


POLICIA NACIONAL
FRONTERAS INTELIGENTES
SISTEMA ABC
REQUISITOS PARA EL USO DE A.B.C.
•Ser ciudadano de la Unión Europea, de E.E.E. o de un país que firmó el acuerdo de Schengen.
•Tener 18 años
• Presentar un pasaporte electrónico o D.N.I. Electrónico español.
18<
10

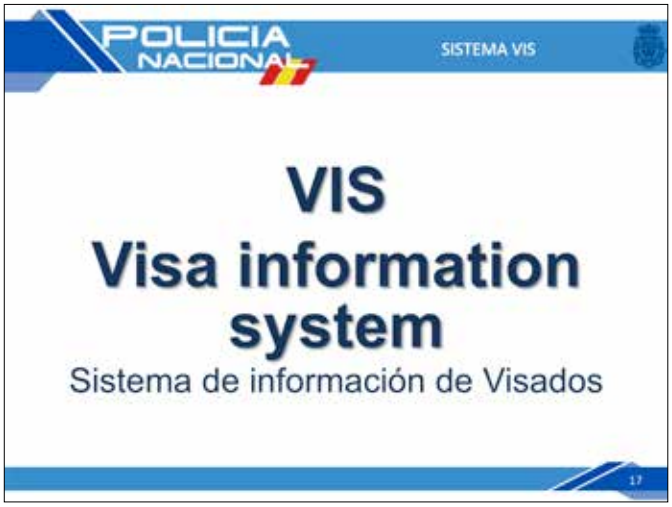

POLICIA NACIONAL
FRONTERAS INTELIGENTES
SISTEMA ABC
DOCUMENTOS ELECTRÓNICOS(CHIP)
ESPAÑA
PASAPORTE
1ª Generación (Foto): Julio 2003
2ª Generación (Foto y huella): Junio 2009
Marzo 2006 (foto y huella)
11


POLICIA NACIONAL
FRONTERAS INTELIGENTES
SISTEMA ABC
Cámaras
Lector de Huellas
Lector DNI
3 Luces
Pantalla táctil
Lector de pasaporte
13

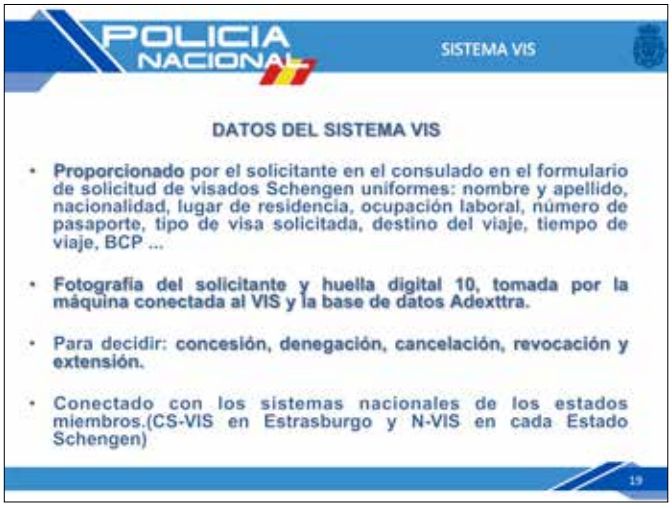

POLICIA NACIONAL
FRONTERAS INTELIGENTES
SISTEMA ABC
VIZ & MRZ
PASAPORTE
Consulta bases datos
Inserta pasaporte o DNIe
Verificación
Captura facial
Cotejo biometría
Captura huella
Cotejo biometría
2ª generación
OK
Cruza frontera
NOK
14


POLICIA NACIONAL
TIPOLOGÍA DEL ABC
MADRID T4S
BARCELONA T1
ALICANTE
Tipo A
Esclusa
Tipo B
Puerta Simple
Tipo C
15


POLICIA NACIONAL
FRONTERAS INTELIGENTES
SISTEMA ABC
CONTROLES EN 2017
ABC
44%
VERIFICADOR Y MANUAL
56%
ABC STEPS
3.685.000
16


POLICIA NACIONAL
SISTEMA VIS
VIS
Visa information system
Sistema de información de Visados
17


POLICIA NACIONAL
SISTEMA VIS
BASE DE DATOS - VISA TIPO C - CORTA DURACIÓN-
MIEMBROS DEL ESPACIO SCHENGEN
Toma de huellas dactilares y datos biográfcos en el consulado
Control de Seguridad en el Puesto Fronterizo
18


POLICIA NACIONAL
SISTEMA VIS
DATOS DEL SISTEMA VIS
• Proporcionado por el solicitante en el consulado en el formulario de solicitud de visados Schengen uniformes: nombre y apellido, nacionalidad, lugar de residencia, ocupación laboral, número de pasaporte, tipo de visa solicitada, destino del viaje, tiempo de viaje, BCP ...
• Fotografía del solicitante y huella digital 10, tomada por la máquina conectada al VIS y la base de datos Adexttra.
• Para decidir: concesión, denegación, cancelación, revocación y extensión.
• Conectado con los sistemas nacionales de los estados miembros.(CS-VIS en Estrasburgo y N-VIS en cada Estado Schengen)
19

POLICIA NACIONAL

FRONTERAS INTELIGENTES
FADO

FADO

False & Authentic Documents Online

20

POLICIA NACIONAL

FRONTERAS INTELIGENTES
FADO

OBJETIVO:

- FADO permite el **rápido intercambio** entre los países de la UE de imágenes de documentos falsos, falsificados y auténticos, para ayudar a combatir la inmigración ilegal y el uso de documentos fraudulentos.

21

POLICIA NACIONAL

FRONTERAS INTELIGENTES
FADO

- **FADO**

Un **servicio central en cada país de la UE** está vinculado a la Secretaría General del Consejo de la Unión Europea (sede Bruselas), pero cada país de la UE tiene libertad para desarrollar su propio sistema de transmisión de datos internos seguros. Cada país de la UE es el responsable de agregar estos datos a su propio sistema.

- **IFADO**

Para **acceder a FADO a través de intranet** por los estados miembros de la UE, la Comisión Europea y Europol. Solo consulta (control de fronteras).

- **PRADO**

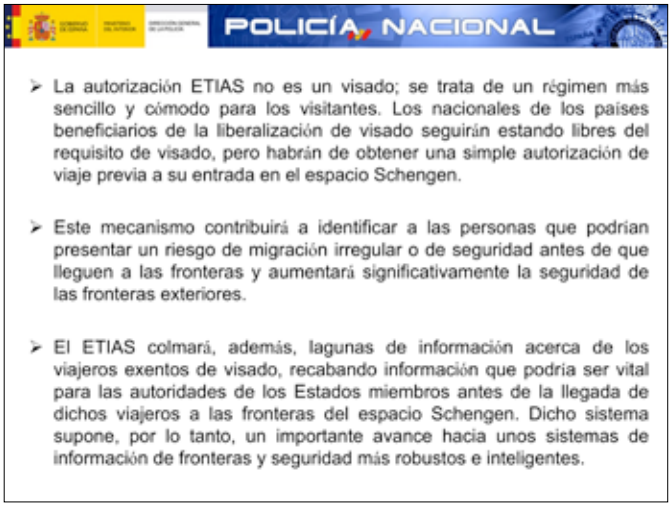
Acceso gratuito a datos a través de internet. Contiene documentos de identidad y documentos de viaje emitidos.

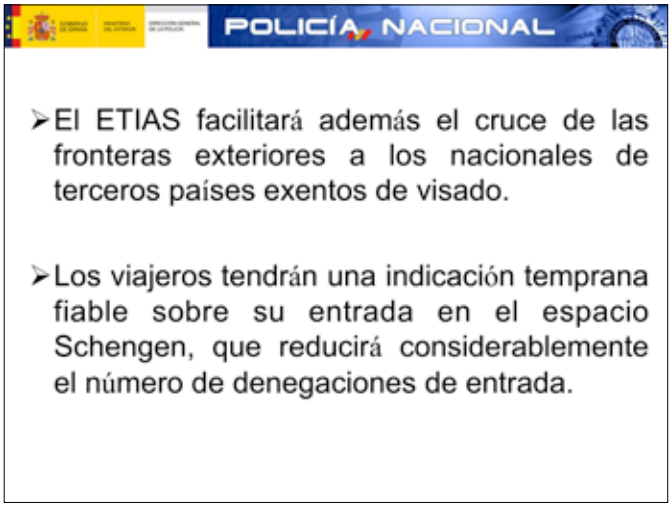
21


POLICIA NACIONAL
FRONTERAS INTELIGENTES
FADO
¿Que información contiene IFADO ?
- Imágenes de documentos AUTENTICOS
(Documentos de identidad y de viaje, visados y sellos).
- Imágenes de Documentos falsos y falsificados
Información sobre técnicas de falsificación y medidas de seguridad
23


POLICÍA NACIONAL
ETIAS (SISTEMA EUROPEO DE INFORMACIÓN Y AUTORIZACIÓN DE VIAJES)


POLICÍA NACIONAL
Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL establishing a European Travel Information and Authorisation System (ETIAS) and amending Regulations (EU) No 515/2014, (EU) 2016/399, (EU) 2016/794 and (EU) 2016/1624.
Sistema Europeo de Información y Autorización de Viajes para reforzar los controles de seguridad de los viajeros exentos de visado. El ETIAS recabará información sobre todas las personas que viajen a la Unión Europea sin visado con el fin realizar unos controles de migración y seguridad más avanzados. Ello contribuirá a una gestión más eficaz de las fronteras exteriores de la UE y mejorará la seguridad interior, facilitando al mismo tiempo los viajes legales a través de las fronteras del espacio Schengen.


POLICÍA NACIONAL
La autorización ETIAS no es un visado; se trata de un régimen más sencillo y cómodo para los visitantes. Los nacionales de los países beneficiarios de la liberalización de visado seguirán estando libres del requisito de visado, pero habrán de obtener una simple autorización de viaje previa a su entrada en el espacio Schengen.
Este mecanismo contribuirá a identificar a las personas que podrían presentar un riesgo de migración irregular o de seguridad antes de que lleguen a las fronteras y aumentará significativamente la seguridad de las fronteras exteriores.
El ETIAS colmará, además, lagunas de información acerca de los viajeros exentos de visado, recabando información que podría ser vital para las autoridades de los Estados miembros antes de la llegada de dichos viajeros a las fronteras del espacio Schengen. Dicho sistema supone, por lo tanto, un importante avance hacia unos sistemas de información de fronteras y seguridad más robustos e inteligentes.


POLICÍA NACIONAL
El ETIAS facilitará además el cruce de las fronteras exteriores a los nacionales de terceros países exentos de visado.
Los viajeros tendrán una indicación temprana fiable sobre su entrada en el espacio Schengen, que reducirá considerablemente el número de denegaciones de entrada.


POLICIA NACIONAL
FRONTERAS INTELIGENTES
E.E.S.
EES
ENTRY-EXIT
NATIONAL
SYSTEM

POLICIA NACIONAL

FRONTERAS INTELIGENTES
E.E.S.

Objetivos (I)

- **Mejorar** la gestión de las fronteras exteriores.
- **Facilitar** el cálculo de la duración de la estancia de corta duración para nacionales de terceros países.
- **Permitir** la identificación de una persona que ya no cumple con las condiciones de entrada o estancia en el área de Schengen.

29

POLICIA NACIONAL

FRONTERAS INTELIGENTES
E.E.S.

Objetivos (II)

- **Crear** estadísticas fiables de entradas y salidas de pasajeros desde o hacia un tercer país.
- **Eliminación** del sellado en los documentos de viaje.

30

POLICÍA NACIONAL

SELLADO

- ✓ *Práctica laboriosa - colocación sello*
- ✓ *No proporciona datos fiables sobre los pasos fronterizos*
- ✓ *No permite detectar el rebasamiento de la estancia autorizada de una manera viable*
- ✓ *No puede hacer frente de manera eficaz a los casos de extravío o destrucción de la documentación de viaje*


POLICIA NACIONAL
PROYECTOS CON LA UE
OTROS PROYECTOS CON UE.
EQUIPAMIENTO MOVIL
Controles móviles a pie de avión o barco e identificación con datos biométricos en Servicios de Seguridad Ciudadana
32


POLICIA NACIONAL
NUEVOS VERIFICADORES Y LECTORES DE HUELLAS
NUEVOS VERIFICADORES Y LECTORES DE HUELLAS
• Una consulta única para todas las bases de datos (VIS y policía).
• Es posible extraer información del chip: datos biográficos de ZLM y fotografía.
• Mayor eficiencia policial y menor tiempo de espera para los pasajeros.
33


POLICÍA NACIONAL
EU-LISA / Proyecto Smart Borders
European Agency for the Operational Management of Large-Scale IT Systems in the area of Freedom, Security and Justice.

POLICÍA NACIONAL

PROYECTO PILOTO – SMART BORDERS (II)

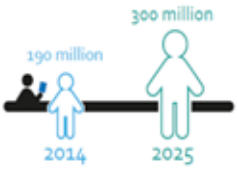
- OBJETIVOS: Durante la fase de pruebas.
- Poner a prueba las opciones técnicas identificadas en el estudio técnico para las EES y RTP/FNP con unos criterios específicos y medibles:

PRECISIÓN
✓EFECTIVIDAD
✓IMPACTO SOBRE EL TIEMPO DE PASO EN LA FRONTERA
✓

POLICÍA NACIONAL

PREVISIÓN NÚMERO DE VIAJEROS PARA CRUCE FRONTERAS / TCN

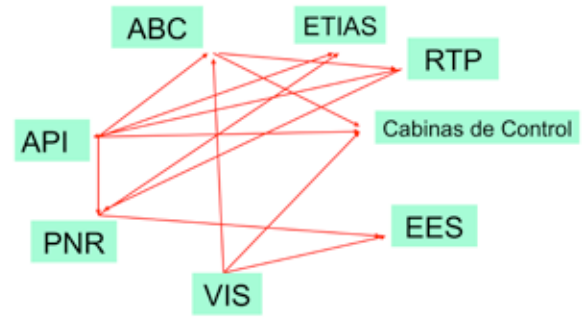
*Se espera que para el año **2025** el número de pasajeros de fuera de la UE que pretendan cruzar la frontera del espacio Schengen casi se duplique hasta los **300 millones** de cruce de fronteras, comparado a día de hoy.*



POLICÍA NACIONAL

- **Objetivo SMART BORDERS**: Lograr la interoperabilidad de todos los sistemas.
- **Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL** on establishing a framework for interoperability between EU information systems (borders and visa) and amending Council Decision 2004/512/EC, Regulation (EC) No 767/2008, Council Decision 2008/633/JHA, Regulation (EU) 2016/399 and Regulation (EU) 2017/2226.

POLICÍA NACIONAL



Interconexión de todos los sistemas = Fronteras inteligentes

POLICÍA NACIONAL

OTROS SISTEMAS

EURODAC.

REGLAMENTO (UE) N o 603/2013 DEL PARLAMENTO EUROPEO Y DEL CONSEJO de 26 de junio de 2013 relativo a la creación del sistema «Eurodac» para la comparación de las impresiones dactilares para la aplicación efectiva del Reglamento (UE) n o 604/2013, por el que se establecen los criterios y mecanismos de determinación del Estado miembro responsable del examen de una solicitud de protección internacional presentada en uno de los Estados miembros por un nacional de un tercer país o un apátrida, y a las solicitudes de comparación con los datos de Eurodac presentadas por los servicios de seguridad de los Estados miembros y Europol a efectos de aplicación de la ley, y por el que se modifica el Reglamento (UE) n o 1077/2011, por el que se crea una Agencia europea para la gestión operativa de sistemas informáticos de gran magnitud en el espacio de libertad, seguridad y justicia (refundición)

POLICÍA NACIONAL

EURODAC almacena información sobre tres tipos de colectivos que son de interés para esta Comisaría General:

1.- Solicitantes de asilo mayores de 14 años.

2.- Nacionales de terceros Estados vinculados al cruce irregular de fronteras exteriores.

3.- Nacionales de terceros Estados que se encuentran de forma irregular en el territorio de un Estado miembro.

Los Estados de la UE que envían datos a EURODAC deben asegurarse de garantizar el respeto de la legalidad en la toma de huellas y en el tratamiento, transmisión, conservación o supresión de datos.

Para el envío de huellas se utiliza escáneres tipo **Live-Scan**, que son dispositivos mediante los cuales se obtiene la impresión electrónica de huellas dactilares sin necesidad de usar tinta, permitiendo el mismo dispositivo la transmisión y envío de estas huellas a determinados organismos o departamentos, en el caso que nos ocupa al **Sistema de Información EURODAC**, cuyo punto focal en España se encuentra en Comisaría General de Policía Científica.

LAS NUEVAS HERRAMIENTAS EN MATERIA DE ANÁLISIS DEL RIESGO EN FRONTERAS

DAVID AGORRETA RUIZ
Comisario del CNP,
Jefe del Centro Nacional de Inmigración y Fronteras

El régimen general de base legal en que se apoya la competencia de extranjería del cuerpo y por tanto de obligado cumplimiento es la entrada y salida de personas, que es lo que produce información. Al final, es verdad que uno puede parar un contenedor por ahí, de hecho la Policía lo hace en régimen general de competencias comunes en demarcaciones propias de la Policía, pero un contenedor, al final, no deja de ser más que la plasmación de un delito o de algún tipo de infracción.

Hoy, para bien o para mal, como es evidente y lo vemos todos los días en la prensa, más desde este último mes de junio de 2018 -pero esto ya viene desde los últimos tres años-, el problema es la inmigración irregular. Este es el problema al que nos enfrentamos hoy, es el problema que tiene que gestionar la Policía en exclusiva, es verdad que hay otra serie de factores que son complementarios, otra serie de capacidades que van desde el apoyo humanitario, el rescate, el border patrol, a vigilar la línea fronteriza que es de lo que se encarga fundamentalmente la Guardia Civil y la Armada, que es una de las grandes olvidadas y que está ahí siempre; y rescate marítimo.

En este escenario general de incremento de un problema que tiene muchos componentes sociales y muchos componentes de uso político, a modo de arma arrojadiza como es la inmigración, pero que sin duda es un problema de seguridad pública. En la Comisaría General se trató de crear una estructura de inteligencia que es a la que responde el Cenit y que es la Uni-

dad a la que yo represento, una unidad de inteligencia que atendiera a unos criterios que no son los criterios al uso de inteligencia en lo que es más pura la investigación policial ¿Qué nos encontramos? Que la información o la inteligencia en materia de extranjería es uno más de los elementos con los que se mercadea en este mundo de las fronteras, de la extranjería. No solo están los detenidos, no es que no tenga importancia, pero la información para la toma de decisiones es vital; nos encontramos con que es un mundo donde la información está esencialmente desestructurada, hay multitud de fuentes, de flujos irregulares, regulares, complementarios, contradictorios entre sí que van desde la información que puede dar un colaborador, hasta la entrevista que hace un compañero que inicia las actuaciones cuando llega una patera que entra en una playa en el sur de España, hasta la que proporcionan las redes de análisis de riesgo de Frontex, Interpol, Europol …

Integrar esto es realmente difícil, básicamente por volumen y, también, por fiabilidad; porque este es un fenómeno que tiende al alza pero que es inestable, hay momentos del año que inexplicablemente baja, hay momentos del año en que tenemos un riesgo creciente y se plasma que efectivamente llega más gente; es un escenario complicado y un volumen de información muy difícil de gestionar. Esto tampoco ayuda a definir procesos de gestión de esta información, de hecho la propia Frontex tiene un auténtico problema con sus análisis de vulnerabilidad porque todavía llevamos tres años buscando a ver si hay algún país de Europa que sea capaz de decirnos qué procesos de análisis usa Frontex, esto no quiere decir que esa información sea mala, pero es verdad que a veces no es la más ajustada a la realidad.

Entonces, ante este escenario, la Comisaría General tuvo que tomar una serie de decisiones y reorganizarse, elegir una serie de fuentes estables a riesgo de equivocarnos y sin perjuicio de que esto no fuera algo exclusivo o inamovible, se eligieron una serie de fuentes de todo tipo, personales, institucionales… y se van ampliando regularmente y algunas de estas listas se van cayendo. Esta elección de fuentes, también nos obligó a controlar una serie de flujos de información en términos de calidad y nos obligó, también, a pensar en el cliente. Nuestro cliente es, desde donde estoy yo para arriba, el resto de jefes de unidad y el comisario general; y del comisario general para arriba los jefes centrales en estos momentos, director adjunto y director general, secretario de estado, ministro; y desde ministro, entiendo yo que subirá hacia arriba.

¿Qué ocurre? La materia es tan compleja y tiene tantos perfiles que obliga a generar productos, o sea que la tendencia general es generar productos de inteligencia muy complejos y muy largos ¿Qué vimos en el Cenit? Que no se los leía nadie, nadie lee; nadie tiene tiempo para leer en esos niveles

de decisión, con lo cual, después de detectar flujos, de elegirlos; después de monitorizar esas fuentes, tuvimos que elegir una serie de productos ¿Cuál fue la opción de la Comisaría General? Productos en los que, dicho llanamente, en los que no haya que leer, en los que un tipo cualquiera de un solo vistazo pueda tener elementos para la toma de decisiones en su escalón. Y productos, porque las capacidades que tiene una unidad como el Cenit, que es pequeña, limitada a productos que sean reutilizables en distintos escalones, desde el táctico hasta el operacional, hasta el estratégico. Esto en términos de inteligencia es algo que está sacralizado, son compartimentos separados, información; sobre todo la UCIP, que habla de análisis operativo, de prospectiva, de estratégico…, como compartimentos estancos.

La Comisaría General se orientó más al modelo americano en el que se habla, generalmente, de inteligencia y utilizas el sistema lo que ellos llaman *need to know* o sea, qué necesitas conocer y qué es lo que el sistema te da. Te da lo que tu necesitas, por ejemplo, si en Logroño existe un problema de extranjería y necesita conocer algo sobre una red, la Comisaría General si tiene la información le servirá lo que necesita. Pero lo que él trascienda irá al escalón superior que actuará en régimen de apoyo en la lógica organización del cuerpo.

Por lo tanto, elegimos esa serie de productos en los que hubiera que leer poco y que fueran lo más multidimensionales posibles ¿A qué me estoy refiriendo? Básicamente a informes muy cortos definiendo siempre las claves de decisión y los parámetros sobre los que pivotamos trasladando la problemática; pocas veces, generalmente en extranjería, se trasladan elementos de mejora, hay veces que sí pero pocas veces y, en el actual escenario, esto va a ser una constante. Y, ¿en qué formato? Además de los informes cortos las infografías, que se pueden ver en la página web del Cenit, de la Comisaría General del Cenit, ahí hay productos. Esto se renueva cada semana de tal manera que si una persona de una comisaría de Albacete quiere ver cómo está la extranjería, se mete ahí y ve las pateras que han llegado cada semana, de dónde vienen, de qué nacionalidades son, el número de inmigrantes que llegan, más o menos las rutas que siguen … ¿Y qué le importa a una persona que está, por ejemplo, en Calatayud, esto? El problema de la extranjería ha dejado de ser un problema en fronteras, es un problema que nos aplasta a todos, porque son flujos de gente que desfilan por todo el país, van hacia Europa y Europa cuando se acredita a través del sistema, entre otros Eurodat y otros más, que han entrado por España, te los devuelve, y ahí está Alemania metiéndonos aviones con personas que recibieron asilo en España y han aparecido en Alemania. Este es otro problema que no es solo de España pero que es el desenlace que está teniendo.

Este tipo de productos lo puede ver todo el mundo y lo que contribuye es a que todo el mundo sea más sensible con el problema y ese extranjero que era objeto de una actuación básicamente administrativa en la mayoría de los casos, pase a ser, por supuesto, o sea una actuación administrativa, por supuesto, eso va a estar ahí siempre, los expedientes correspondientes bien sean de expulsión, bien sean del tipo que sea; pero tratar de convertirlo en una fuente ¿Qué ha ocurrido? Es verdad que estos procesos son lentos pero es verdad que cada vez tenemos más *feed-back* de comisarías impensables. Hace poco apareció una persona en una comisaría de Castilla la Mancha y esta persona nos daba información. Y nos dio información porque esta persona decía yo veo estas infografías y veo que las modificáis y que las podemos consultar y dice ¡oye mira! ha venido una persona que dice que no ha venido por donde decís que han venido estas nacionalidades; era una persona de las Islas Comores. Pues eso, una comisaría de Castilla la Mancha se encontró con una persona, instruyó el expediente, alguno perdió el tiempo en hablar y eso llegó a la Comisaría General. No es una gran aportación en términos estratégicos pero es una demostración de que el sistema funciona y que una persona cuyo objetivo no es la inmigración irregular es primer escalón.

¿Qué hicimos además de elegir los productos? En un escenario de precariedad presupuestaria absoluta, decidimos elegir qué herramientas desarrollamos. Teníamos la ventaja de tener algún ingeniero informático allí, esto te lo encuentras o no en las unidades, yo tuve la suerte de encontrármelo, concretamente a dos de ellos y decidimos desarrollar alguna herramienta propia y comprar o intentar comprar otras, baratas, por supuesto; las que compramos: Maltego y Social links, que son herramientas para consulta en régimen de fuentes abiertas en Internet que nosotros las asociamos a consultas, sobre todo, de redes sociales. Que las redes sociales son el medio publicitario de todas las redes de inmigración irregular, de todas las tramas de inmigración irregular que van desde Níger hasta cualquier sitio de Europa; y están todas interconectadas. Es verdad que son distintas organizaciones pero tú, cuando compras tu billete para venir a Europa en Niamey y entras en contacto con una determinada organización, esa organización ya tiene sus contactos en cadena y te garantizan que te pueden llevar pagando y sufriendo mil penurias hasta la costa española. Y esto, que es algo que todos decíamos a raíz de este tipo de herramientas, lo hemos podido comprobar poniéndoles nombres, apellidos, teléfonos … a todas estas redes. Esto fue una, Maltego y Social links, luego optamos por otra cosa que es lo que nosotros llamamos *mapping* que utilizamos otra herramienta que ya tiene cuerpo pero que compramos en una versión un poco más desarrollada que es SRIG que nos permite lanzar todos los datos que tenemos a mapas y esto nos permite ver, por ejemplo, una nacionalidad determinada, por ejemplo, Gandianos, por

dónde pasan por toda África y por dónde pasan por Europa. Te lanza unos puntos que los va diseñando de mayor o menor tamaño o intensidad en función del volumen de paso de esas nacionalidades.

¿Qué nos permite a nosotros esto? Nos permite redireccionar nuestros esfuerzos, decidir en qué comisaría tenemos que incidir más con unas nacionalidades; nos permite, por ejemplo, a los de la UCER, decidir qué flujos de llegada van a tener en determinados sitios para intentar reorganizar la escasa capacidad de los CIES y poder alojar a la gente, …

Bueno, esta fue la otra. Una sobre redes sociales y otras sobre mapas ¿Por qué? Porque toda la información era imposible ponerla en un informe, con lo cual decidimos elegir flujos, rutas, llegadas, nacionalidades, frecuencia y lugares de paso; y lanzarlo a mapas. Que cualquiera lo coja y pueda saber por dónde vienen los argelinos o los sirios a España, y sé que puntos de paso tienen y cuanto tiempo les cuesta. Algo rápido, algo que no haya que leer.

Y la otra parte, que es la de desarrollo propio, vino condicionada no tanto por necesidades de tipo operacional o de toma de decisiones relacionadas con la inmigración irregular, sino con una cosa que está muy de moda en el mundo de fronteras, bueno en general, en todas partes, que se llama el análisis de riesgo. Esto vino de la mano de Frontex y de la propia Comisión Europea ¿Qué ocurre? Todos hemos llegado a la conclusión de que uno de los elementos de riesgo, a controlar en la inmigración irregular en todos los fenómenos de inmigración irregular, son tus propias fronteras. No se puede obviar que eso es un elemento favorecedor o disuasorio. De esto, también se ha dado cuenta la Unión Europea y ha generado sistemas de análisis de riesgo que están basados en sistemas de auditoría que tienen dos escalones y son complementarios; y todos intuimos que van a acabar integrándose el uno en el otro. En esto, nosotros hemos cogido la delantera con respecto a otros países de Europa, de hecho somos los únicos que lo hemos integrado. Los escalones son: la evaluaciones Schengen que las hace la Comisión que son de dos tipos, una reglada y que cada cierto tiempo un equipo de la Comisión multidisciplinar, un montón de países vienen y hacen una inspección reglada, por ejemplo en el aeropuerto, de Madrid-Barajas o en puerto de Barcelona, en una serie de sitios, y tu te puedes, más o menos, preparar, y ellos evalúan tus capacidades. Esto lo hace la Comisión y se llaman evaluaciones Schengen, es un sistema de auditorías. Sobre esto, se construyen una especie de actas de inspección que tienen cierta trascendencia política en la que luego los presidentes, los ministros…, les sacan los colores la Comisión Europea al país que sea, si están mal las cosas y, sobre esto, también hacen cierta predicción basado en un análisis de riesgo.

Además de esto, en el ámbito de la Unión Europa y como agencia dependiente de la Comisión está Frontex, que hoy por hoy en términos europeos es la gran joya de la corona en temas de inmigración. Frontex ha desarrollado su propio sistema de análisis de riesgo también para el análisis de puestos fronterizos, este sistema se llama vulnerability asessment (análisis de vulnerabilidad), y esto se va a oír mucho, ya se oye mucho pero se va a oír más.

Es una suerte, yo siempre lo explico así, no es lo más ajustado pero cuando tratas de transmitir la idea es lo mejor. Todos hemos oído hablar de los test de estrés de la banca, bueno pues esto es lo mismo pero para las fronteras. Hay tres escalones, te hacen una inspección de propia iniciativa, hay otros que te piden información y te hacen simulaciones, te dicen: "oiga mire usted, usted es el jefe de la comisaría de Algeciras, a usted le llega una oleada de cincuenta pateras con quinientas personas en un día, los mete en el CIE y el CIE se le incendia ¿dónde les lleva usted?"Y tú tienes que ir dando respuestas en función de tus capacidades, ellos van viendo lo que vas diciendo y te evalúan. Alguien estará pensando, tu cuentas lo que quieras y dices: así respondería yo como si fuera el caso práctico de comisario ¡No! porque luego vienen y dicen ¿no decía usted que tenía estas capacidades?¿Dónde están?

Y luego hay un último escalón que cuando ya la situación es catastrófica ellos, digamos, te intervienen como hacen con los bancos, despliegan su contingente obligatorio. Esto solo ha pasado en la frontera búlgara y a petición propia de Bulgaria, en el año 2017. Despliegan el contingente obligatorio o te crean otra cosa, un *hospot*. Las dos cosas son cesiones de soberanía a todas luces. Para controlar esto, hemos creado el *risky tool*, que es una herramienta que se ha creado para análisis de riesgo. El *risky tool* es una herramienta que no necesita instalación, se ejecuta directamente, se construye sobre la base excel, toda la Policía la tiene disponible; en los puestos fronterizos todos los que los han pedido lo han tenido, a todos les aplicamos lo mismo, analiza la vulnerabilidad sobre los parámetros que nos analiza Frontex, que son básicamente, en puestos fronterizos, flujos de entradas, denegaciones de entradas por tipos, fraude documental por tipos, peticiones de asilo en frontera y personal en primera y segunda línea. Sobre esos parámetros crea, le da a la persona que está ahí, que solo tiene que meter números, da igual que sea un Policía recién salido de la escuela que el más viejo de la plantilla; abre el programa y le sale una casilla y le dice: meta usted las denegaciones de entrada que ha tenido hoy, si ha tenido cincuenta, mete cincuenta; y así va rellenando las casillas, o sea, no es nada complejo. Integra estos datos y te da un análisis de riesgo ¿Cómo te da el análisis de riesgo? O bien en un formato excel o te lo da en unos indicadores como los marcadores de las motos en los que tu ves de menos revoluciones a más. Aquí, lo que hace es utilizar

los colores que utiliza la propia agencia Frontex que van de menor riesgo a mayor riesgo, del azul claro (menor riesgo) pasando por amarillos, anaranjados y rojos que son los de mayor riesgo; y lo van indicando con una aguja en un semicírculo que es como si fuera el marcador de un coche o de una moto, de manera que cada uno de estos colores lo ves; cada indicador lo ves.

En flujo de entradas, hoy tengo riesgo en flujo de entradas, el programa ya esta basado en unos algoritmos que se sacaron de los algoritmos que el CNI provee a determinadas empresas para análisis de riesgo; esto está en la página del CNI, se puede consultar. Y, sobre esto, lo construyeron los informáticos y luego, además de todo esto, les da una predicción a dos meses, sobre tres escenarios. El escenario que tú tienes mejor con esos datos que has metido, el escenario peor, el intermedio y, sobre eso, dibuja tu línea, tus datos que van en negro, tú lo ves en tres colores. Tú ves si te aproximas al mejor escenario, si estás en la media, si te aproximas al peor escenario y todo esto en cada uno de estos parámetros. Cualquiera puede tomar una decisión con estos datos, hasta la persona que está ahí pidiendo el pasaporte.

Os pondría el power point pero en aproximadamente un mes se va a poder ver en la página web del Cenit porque se publicará el último análisis de vulnerabilidad que integra las evaluaciones Schengen y el *vulnerability asessment* de Frontex que es el único sistema que hay en Europa que integra las dos auditorías que hace la Unión Europea. No hay que hacer ninguna instalación, cualquier miembro de una comisaría de Policía Nacional puede pedir el *risky tool* y puede tenerlo para su puesto fronterizo. Estamos haciendo alguna simulación a petición de alguna jefatura en cosa de judicial o seguridad ciudadana, concretamente hemos hecho simulaciones con datos de jefaturas pequeñas como la UPEC, como Logroño que se las pedimos a la UPEC, y más o menos funciona; tenemos que adaptarlo pero para fronteras es bastante fiable ¿Qué fiabilidad tiene? El 70% que en proyección o en prospectiva es mucho, cuando casi todo el mundo se está moviendo en informes de prospectiva en un 30% de fiabilidad.

DESAFÍOS Y RESPUESTAS A LA MOVILIDAD HUMANA EN LA PRÓXIMA DÉCADA

EUGENIO PEREIRO BLANCO
Comisario Principal del CNP,
Comisario General de Extranjería y Fronteras

En diez minutos hay que priorizar porque habría que decir muchas cosas, pero como no hay tiempo, hay que priorizar, y cuando uno prioriza puede cometer errores por dejar en el tintero algo que debería decirse. Me estoy curando en salud.

Voy a hacer unas breves referencias al ámbito mundial, europeo, con el continente africano, España y a la Policía Nacional ¿Qué hacemos en este ámbito? Ya poco tengo que decir porque ya se ha dicho por parte de Fernando y de David.

Primer dato, cuando hablamos de movilidad humana a nivel mundial, en el año 2017, se produjeron treinta millones de desplazamientos afectando a ciento cuarenta países, y las dos principales causas de esos treinta millones de desplazamientos son, por un lado los desastres naturales y por otro lado los conflictos. Son las dos principales causas que motivan los desplazamientos, la movilidad humana a nivel mundial. Los desastres naturales ocupan el 60%, aproximadamente, de esa movilidad; el 40% restante se lo atribuimos a los conflictos; y si hablamos de conflictos ese 40%, de los aproximadamente treinta millones de desplazamientos, nos salen doce millones y más de la mitad de los desplazamientos originados por los conflictos y que se centran solo en cuatro países: Siria, República Democrática del Congo, Irak y Sudán del Sur. Bastante cerca de España y con afectación

en el ámbito de la extranjería de la inmigración y de las fronteras. Los motivos de los desplazamientos en esta movilidad humana, motivos internos y transfronterizos, hay mucho movimiento interno interpaís pero también mucho transfronterizo. Los motivos son diversos: económicos, sociales, políticos y ambientales. Y hablando de ambientales, tenemos que hablar de los desplazamientos por motivos climáticos, dentro de los inmigrantes hay una nueva categoría que son los inmigrantes climáticos, por razones climáticas. La hipótesis más negativa, aunque realista, para las próximas dos o tres décadas se habla de ciento cuarenta millones de desplazamientos a nivel mundial, pero en tres áreas muy concretas, ciento cuarenta millones de desplazamientos. América latina, Asia meridional, Bangladesh, India, Paquistán, Afganistán, Sri Lanka y el África subsahariana, de especial afectación para Europa y para España, de esos ciento cuarenta millones de desplazamientos que se prevén para estas dos, tres próximas décadas, digamos que a África subsahariana le corresponden unos ochenta millones de desplazamientos. Los motivos para estos desplazamientos en el ámbito climático son las sequías, la reducción de las cosechas y el aumento del nivel del mar; sirva como ejemplo, aunque me voy a ir un poco lejos, a Bangladesh, unos veinte millones de habitantes de las zonas costeras de Bangladesh ya están sufriendo en su salud las consecuencias de la intrusión de agua salada en las reservas de agua potable provocada por el aumento del nivel del mar, veinte millones de personas.

Entradas irregulares vía marítima por el mediterráneo en Europa, básicamente España, Italia, Grecia y Malta:

Año 2014: doscientas cincuenta mil
Año 2015: más de un millón
Año 2016: trescientas sesenta mil
Año 2017: Ciento setenta mil

Y en lo que llevamos del año 2018 en torno a cuarenta y ocho mil.

La tendencia de entradas irregulares vía marítima en Italia está decreciendo, ya sabéis por qué, siguiendo los medios de comunicación está claro. Y en España está subiendo. La tendencia a la baja por un lado se contrarresta con la subida a la alta por otro -nosotros tenemos un problema-. Las dos rutas principales en el mediterráneo y una del atlántico; la ruta del mediterráneo central, básicamente desde Libia a Italia y Malta. La del Mediterráneo Occidental; la nuestra, que entra por España desde Marruecos, Argelia, menos Túnez, El magreb. Y la ruta Atlántica, la que nos entra en Canarias desde las costas del Sahara.

En España ¿qué nos entra por estas vías? Los flujos marítimos irregulares magrebíes y, especialmente, subsaharianos. Y ¿por qué los subsaharianos? Hay dos características que son las más relevantes y que sirven para el presente y para el inmediato futuro. Primera: el espectacular aumento de la población en el África Subsahariana; se prevé que en dos, tres o cuatro décadas se duplique. La población subsahariana es muy joven, aproximadamente el 60% tiene menos de veinticinco años, jóvenes y enganchados a las nuevas tecnologías, es decir, no son ignorantes de lo que está pasando fuera de su región, saben perfectamente lo que está ocurriendo en el mundo exterior y les llama la atención

Y segunda: los problemas endémicos. Los conflictos, la escasez de recursos y la degradación medioambiental. En este tipo de flujos tenemos que hablar de origen, tránsito y destino. Los subsharianos tienen como destino el Magreb, España y otros países de la Unión Europea; entonces España es país de destino por un lado y tránsito por otro. El Magreb, Marruecos, Argelia son países de origen de los flujos, son países de tránsito, de los flujos, sobre todo con los subsaharianos, pero también son países de destino; parte de los subsaharianos no quieren pasar del Magreb.

Hay otra clave que quiero reflejar y que no se debe olvidar, en África se encuentran dieciocho de los veinte países más pobres del mundo, este no es un dato baladí. En África se desarrollan la mitad de los conflictos mundiales y en África se encuentran doce de los veinte países más corruptos del mundo ¡vayan sumando circunstancias! ¿Qué hace Europa? Incentiva a los países del Magreb para reforzar las fronteras, para impedir los cruces irregulares, en definitiva para que los flujos irregulares no entren en Europa; repatría a los países de origen y ayuda a los países afectados.

¿Qué hace la Policía Nacional de España? Trabaja en el ámbito humanitario y en el ámbito seguritario. Trabajamos en la extranjería, en la inmigración y en las fronteras y, además, con competencias exclusivas en la inspección fronteriza y en el régimen de extranjería; solicitudes de protección internacional, repatriaciones, expulsiones, devoluciones… Pero, además, somos Policía Judicial e investigamos, porque detrás de los flujos migratorios hay organizaciones criminales dedicadas al tráfico de personas, a la trata de seres humanos incluso de menores, etc. Y, además, hacemos inteligencia. Tenemos presencia permanente en los países afectados y en los principales países que, desde el punto de vista estratégico, son de interés para la Policía Nacional Española en la lucha contra la inmigración irregular, incluso en el ámbito humanitario, porque trabajamos en la detección de víctimas de trata y, además, tenemos interlocutores no solo a nivel central, sino también a nivel territorial.

Un último apunte, en el ámbito inmigratorio irregular intervienen muchos actores ajenos a la Policía, a veces, con intereses contrapuestos, y nosotros estamos en el medio. Y, cuando llueve, que llueve bastante, en el tejado de la Policía llueve siempre, de un lado o del otro. No hay que olvidar que en la inmigración hay controversia política y en la controversia política se tiran los trastos de forma seria, y nosotros estamos en el medio.

TURNO DE PREGUNTAS

Pregunta en sala: ¿Qué porcentaje hay de expulsión?

Responde: Eugenio Pereiro Blanco. Depende de las nacionalidades, con unas nacionalidades el porcentaje es bastante elevado y con otras nacionalidades muy baja, sobre todo en los países subsaharianos, porque existen dificultades para que esos países reconozcan a sus nacionales y no porque haya especiales dificultades para que reconozcan a sus nacionales.

Clausura

MARIO HERNÁNDEZ LORES
Director gerente de la Fundación Policía Española

Señora Secretaria de Estado, Señora vicerrectora de la Universidad Complutense de Madrid, Señor Director General de la Policía, Patrón de la Fundación Policía Española Félix Simón, Junta de Gobierno, Comisarios y demás policías y resto de amigos, hace cinco días comenzamos con el curso "I+D+i en la función policial"; llegamos a la conclusión, el primer día, que la seguridad para la mayoría de las actividades que tiene nuestra sociedad es completamente necesaria. El desarrollo económico y otras serie de actividades están fundamentadas en una seguridad que la respalda; pero si esto es así, el turismo, fuente de riqueza de nuestra nación, es uno de los que más destacaron.

El mismo lunes, día nueve, planteamos el *iter* de lo que iban a ser estos cinco días. Nos planteamos establecer los conceptos generales del I+D+i; considerábamos que la innovación es el paso a donde se llega desde la investigación y el desarrollo es el retorno del dinero que se invierte. Vimos las oportunidades que se planteaban en la Policía Nacional para desarrollar esta investigación y esta innovación y se presentó el servicio de I+D+i de la Jefatura Central de Logística. Intentamos determinar también las oportunidades que nos proporciona Europa y los organismos españoles que lo coordinan, en especial el CDTI (Centro para el Desarrollo Tecnológico Industrial). Pero, sobre todo, vimos las inquietudes de cada una de las grandes áreas del Cuerpo Nacional de Policía: Formación, Policía Científica, Policía Judicial, Seguridad Ciudadana, Extranjería. Este en especial lo quiero destacar porque era uno de los objetivos prioritarios para lo que van a ser los proyectos marcos de la Unión Europea para el próximo decenio.

También, vimos instituciones paralelas a nosotros como es Defensa y Policía Local. Hemos llegado a la conclusión, y reflexionado, que ante todo, está claro que el futuro no se puede adivinar, pero podemos prepararnos

para él a través de la prospectiva, para dar las respuestas que en su momento nos demandará la sociedad.

Creo que dentro de las limitaciones que tenemos lo hemos conseguido ¿A quién hay que dar las gracias? Por supuesto hay que dárselas a la Universidad Complutense de Madrid que nos ha dado la oportunidad un año más de estar aquí, es el vigésimo año que estamos aquí; ¡veinte años ya que estamos aquí!, y creo que eso nos ha dado una experiencia para estar haciéndolo lo mejor que podemos. Por ello hay que dar las gracias, por supuesto, a la vicerrectora Isabel Durán Gimenez Rico, a Manuel y a Yanna. Enhorabuena por la organización del curso, en especial en este incomparable marco que es El Escorial; gracias a la Fundación Policía Española por habernos subvencionado y apoyado; también al Banco de Santander y, por supuesto, a la Caixa en su doble vertiente, tanto como "Caixabank" como "Fundación La Caixa" que son las que nos vienen subvencionando normalmente. Gracias a los excelentes ponentes que hemos tenido, gracias al equipo del Área de Publicaciones del Gabinete Técnico, en especial a Carmen, Secretaria del Curso, a María Jesús, David, Alfonso y, en general, al equipo que se ha quedado también en Madrid. Gracias a Félix que hará posible que todas las ponencias estén editadas en un futuro, como en los veinte años que lo venimos haciendo, imprimiendo y publicando los cursos que hemos desarrollado.

Pero no quiero olvidar al equipo de apoyo de la organización de los cursos, a Oscar, a Larrubia, Paqui, Luis que han hecho posible que el día a día haya sido más fácil y eficaz. Gracias, especialmente, a todos vosotros, los asistentes, a los alumnos que realmente sois el objetivo final de este y del resto de los cursos. Y, en definitiva, como director gerente de la Fundación, ya no solo como director del lo curso quiero garantizar que en el futuro seguiremos promocionando este tipo de actividades, que es enriquecimiento para todos y en especial para el Cuerpo Nacional de Policía.

Doy la palabra al siguiente miembro de la Fundación Policía Española. Muchas gracias.

FÉLIX SIMÓN ROMERO
Patrono de la Fundación Policía Española

Señora Secretaria de Estado de Seguridad, Señor Director General de la Policía, Señora Vicerrectora de la UCM, Director del Curso, Miembros de la Junta de Gobierno del Cuerpo Nacional de Policía aquí presentes, funcionarios de este cuerpo, compañeros míos y alumnos todos.

Si me permiten, quisiera comenzar haciendo un comentario sobre la institución a la que represento en este acto que es la Fundación Policía Española.

Según sus estatutos, es una organización de carácter cultural, educativo, social, formativo y asistencial; y no tiene ánimo de lucro. Su objetivo prioritario es el de desarrollar todo tipo de actuaciones tendentes a lograr que los cuerpos policiales en general y específicamente el Cuerpo Nacional de Policía, contribuyan a mejorar el ejercicio de los derechos y libertades, por parte de los ciudadanos y, de esa forma, alcanzar el mayor afecto de la sociedad española. Hay que señalar que la Fundación funciona regida por su patronato con plena autonomía debido a su condición de fundación privada, por lo que no depende de ningún órgano de la administración. Al mismo tiempo, como no puede ser de otra forma, mantiene unas excelentes relaciones con la Dirección General de la Policía y, por ende, de la Secretaría de Estado de la Seguridad. En sus veinte años de existencia, la Fundación ha desarrollado una fecunda tarea en el cumplimiento de sus objetivos fundacionales, siempre en permanente sintonía con los responsables de la Dirección General de la Policía.

Entre sus actuaciones más relevantes que se están desarrollando, o lo han hecho recientemente, están las siguientes: creación de un fondo bibliográfico de interés policial que cuenta ya con treinta y nueve publicaciones, realización de cursos y seminarios de diferentes temáticas policiales, entre estos destaca este que se está realizando aquí y que ahora se clausura en su

vigésima edición, como ha dicho el director de los cursos; y, también, se hacen cursos patrocinados por la Fundación, muy interesantes, aquí está la Comisaria de Policía Científica, en la Universidad Internacional Menéndez Pelayo, son ya once los cursos que se han realizado.

Se otorgan becas a funcionarios del Cuerpo Nacional de Policía para proyectos de investigación en el ámbito policial. Este año se van a otorgar diez becas de tres mil (3.000) euros cada una; se otorga anualmente un premio a los valores humanos, para premiar actos de funcionarios del Cuerpo Nacional de Policía que resalten la vocación de servicio y el sacrificio; y que está premiado con seis mil (6.000) euros. Son ya más conocidos por la repercusión mediática que tienen los premios de periodismo, y que se otorgan a los mejores trabajos publicados que analicen la labor de la Policía Nacional en aras a la seguridad ciudadana; por supuesto, atendiendo a criterios de calidad y de rigor periodístico. Se otorgan en tres categorías: prensa escrita y digital, televisión y radio; también están premiados con seis mil (6.000) euros para cada una de estas categorías.

Ahora mismo, está convocado un premio anual de investigación que busca aportaciones de carácter científico que permitan el avance de las organizaciones policiales con especial atención a las nuevas tecnologías, es anual y está dotado con veinte mil (20.000) euros y tiene un accésit de diez mil (10.000)euros.

Una cosa que se sale de esta línea, pero que también nos parece muy importante y que la echábamos de menos los que tantos años hemos estado en el Cuerpo Nacional de Policía, es un himno del Cuerpo Nacional de Policía. Por iniciativa de la Fundación se procedió a la selección de la letra en primer lugar y posteriormente, como no podría ser de otra manera de la música. Se abrió la participación a todos los autores y compositores residentes en España. En el caso de la letra, la participación fue masiva, se registraron cuatrocientas cincuenta propuestas de letra. Fue elegida por el jurado compuesto por miembros del Cuerpo Nacional de Policía, de la Fundación de la Policía y compositores españoles de notable prestigio así como poetas. Se seleccionó y fue elegida la letra denominada "Tesón de Hierro" que da nombre finalmente a nuestro himno. Posteriormente, ya con la letra, se hizo otro concurso para elegir la música. Finalmente esta gestión de la Fundación se propuso al Ministerio de Interior, y este tuvo a bien dar la autorización para que fuera el himno oficial de la Policía. Son muchas las actividades que se vienen patrocinando por la Fundación pero no quiero ser más exhaustivo.

En cuanto al curso, que se clausura hoy, quisiera resaltar lo oportuno y acertado de su contenido. Igualmente, la selección de los distintos paneles y

el alto nivel de los ponentes a quienes les agradezco su esfuerzo como, también, a los alumnos por su atención y su activa participación.

Por todo ello, felicito al director del curso y a sus colaboradores porque un año más se ha conseguido alcanzar un gran interés respecto al tema a debatir, y con la selección de los ponentes igualmente, manteniendo las expectativas que este curso viene consolidando haciéndolo uno de los más prestigiosos cursos en este marco de los cursos de verano de la Universidad Complutense en El Escorial. Igualmente agradecer la generosidad y la hospitalidad que ofrece la organización de los cursos de verano año tras año.

Termino no sin antes reiterar el permanente propósito del patronato, de continuar al servicio del Cuerpo Nacional de Policía, por ello, nos ponemos a disposición del nuevo Director General de la Policía en todo aquello que, de conformidad con nuestros fines, contribuya a prestigiar a la Policía Nacional y coadyuve al cumplimiento de sus objetivos. Muchas gracias.

ISABEL DURÁN GIMÉNEZ-RICO
Vicerrectora de la Universidad Complutense de Madrid

Director gerente de la Fundación Policía Española, Director General de la Policía Española, patrono de la Fundación Policía Española, Secretaria de Estado de Seguridad. Buenos días, es un honor para mí como vicerrectora de la UCM estar aquí representando al rector en la clausura de este curso. Quiero agradecer a la Secretaria de Estado, especialmente, su presencia en la clausura de este curso" I+D+i en la función policial" que se ha celebrado a lo largo de esta semana. Para la Complutense es un honor contar con su presencia, con la presencia de todos ustedes, que otorga a este curso el máximo apoyo institucional.

Gracias, igualmente, a todos ustedes, a todos los participantes que de seguro no solo han aprendido sino que han enriquecido el curso que clausuramos con sus comentarios y apreciaciones. Y, enhorabuena por llegar a buen término.

Como universitaria y como vicerrectora de la Complutense creo que no puede haber un sitio más indicado para el debate en torno al I+D+i en la Policía Científica que la universidad, que el entorno universitario. Muchos pensábamos ingenuamente que la investigación se limita a la universidad, a los laboratorios, al Cesic y, a veces, olvidamos que nuestra Policía Científica está tan inmersa en proyectos de investigación como podamos estarlo los universitarios. Como bien señala el programa del curso, muchos de los retos de la investigación e innovación en nuestros días, están relacionados con la seguridad, bien porque su garantía exige, cada vez más, avances tecnológicos y un despliegue cada vez mayor de los recursos logísticos y humanos; o bien porque la aplicación de muchas de las innovaciones globales como las relativas, por ejemplo, a las del comercio electrónico o la banca por Internet o la movilidad de las personas, simplemente no serían posibles sin garantizar la seguridad. El contexto social y, por lo tanto, el entorno operativo en la Poli-

cía, han cambiado considerablemente las últimas décadas en todo el mundo. Y, en este contexto, se hace imprescindible prestar una especial atención a las actividades de investigación, desarrollo e innovación que conducen a mejorar las habilidades profesionales de la Policía y, en suma, a un mejor y más efectivo desempeño de las actividades policiales.

La Policía Nacional, todos los sabemos, se enfrenta hoy en día a retos muy distintos, a los presentes hace pocos años, solamente por citar algunos de los que se han debatido aquí: el terrorismo internacional, el ciberterrorismo, el tráfico y la seguridad en el transporte; el tráfico de seres humanos, el crimen organizado, la protección contra intrusos, robos y agresiones en el espacio real, y también y muy especialmente en el virtual, la presión del inmigrante en las fronteras de Europa y en España, y su adecuado trato una vez dentro del país. Estos son, solamente, algunos de los retos cada vez más complejos a los que se enfrentan los Cuerpos y Fuerzas de Seguridad del Estado en la actualidad.

Es innegable, por tanto, que el trabajo policial se ha diversificado y se ha vuelto más complicado y que muchas de las amenazas actuales son de carácter transfronterizo y exige un enfoque innovador para garantizar la seguridad de la ciudadanía. Y la universidad no debe mantenerse ajena a ninguna de estas cuestiones que afectan directamente a la vida de las personas y, por eso, es un honor haber acogido durante esta semana a los diferentes expertos en seguridad que han participado en este curso y haber brindado, a todos ellos así como a todos los asistentes, este espacio de reflexión y de debate.

Para terminar, quiero destacar lo que todos sabemos pero que hay que recordarlo siempre, deseo hacer constar que los miembros de la Policía Nacional, dedican sus vidas a salvaguardar la convivencia, la seguridad y la tranquilidad de sus conciudadanos y por ello merecen la admiración, el respeto y el apoyo sin fisuras del conjunto de la sociedad española. Por difíciles que sean los desafíos y amenazas que debemos afrontar, la Policía Nacional sabrá hacerles frente para garantizar que España siga siendo uno de los países más seguros del mundo, por ello, es un cuerpo del que todos los españoles nos sentimos orgullosos.

Quiero, finalmente, agradecer su labor al director del curso Mario Hernández Lores, director gerente de la Fundación Policía Española y a la secretaria del mismo, Carmen Baz Crespo, inspectora de la Policía, y darles, de nuevo, a todos mi bienvenida y mi agradecimiento.

ANA BOTELLA GÓMEZ
Secretaria de Estado de Seguridad

Señor Director General de la Policía, Francisco Pardo; Vicerrectora de Relaciones Internacionales de la UCM, Isabel Durán; Comisaria General de Policía Científica, Pilar Ayue; Patrono de la Fundación Policía Española, Félix Simón; Comisario General de Extranjería, Eugenio Pereiro; Director del Curso, Mario Hernández Lores; comisarios, mandos y funcionarios de la Policía Nacional, señoras y señores, estamos en un lugar emblemático. El rey Felipe II encargó la construcción de El Escorial al arquitecto renacentista Juan Bautista de Toledo que había sido, a su vez, ayudante de Miguel Ángel en la Basílica de San Pedro del Vaticano. Y la piedra fundacional que dio comienzo a las obras se colocó el veintitrés de abril de 1563, hace ya cuatrocientos cincuenta años; de aquí venimos. Esta es la huella de la historia que nos precede, porque la innovación es un proceso continuo. El impulso de la innovación no sería posible sin observar nuestra historia y continuamos innovando porque la creación, adaptación y transformación es, y seguirá siendo, lo que mueve a la humanidad; nos hace ser lo que hoy somos y de donde nos seguimos proyectando hacia el futuro.

A partir de la tradición, donde nuestra historia es la piedra angular fundamental, en estos cursos de verano de la Universidad Complutense, en la que me siento feliz de poder estar, aunque sea unos minutos; pero sentirme partícipe tanto de la historia del lugar como de esta iniciativa que lleva tantos años recorridos y que tanto conocimiento está aportando a la sociedad. Y a la vez, hacerlo de la mano de la Fundación de la Policía Española que tanto esfuerzo está haciendo para implicarse en esa modernización del Cuerpo con una voluntad directa que es servir mejor a los ciudadanos, servir mejor al progreso de la sociedad de nuestro país es un privilegio. Pues bien, en este curso venimos a celebrar unas jornadas en las que definitivamente fomentamos el trabajo en equipo, el hecho de esta convivencia de todas las personas que asisten, el conocimiento innovador a través de todos los ponentes que

participan y, desde luego, el plantel del programa no puede ser más representativo de la excelencia del conocimiento que tenemos aquí, a nivel muy próximo, entre nuestros propios representantes de fuerzas y cuerpos, entre representantes de otros organismos como el CDTI que es un organismo español, del cual nos sentimos orgullosos y, también, la mirada siempre puesta en el futuro que es lo que debe guiar nuestra actuación.

Venimos de una tradición, pero tenemos que mirar siempre hacia delante, estamos celebrando, como ha dicho el director del curso la vigésima edición y es un honor estar aquí para daros la felicitación y, además, transmitiros todo el entusiasmo y toda la fuerza para que nos podamos ver al año siguiente en esa nueva edición después de estos veinte años.

La formación es esa piedra angular de la que hablábamos, esa piedra que en un momento dado en la vida de todas las personas, igual que paso en el monumento de El Escorial, tiene un hito de partida y todos nosotros sí hemos tenido la oportunidad, yo creo que aquí sí que somos una representación de personas, de hombres y mujeres que hemos pertenecido ya a generaciones en las cuales hemos tenido la oportunidad de arrancar nuestras vidas con una base de educación, entonces hay que animar a que todos puedan hacerlo. La formación promueve la evolución de cada persona, de cada mujer, de cada hombre, que día a día ponen todo su empeño y todo su esfuerzo en educarse y en progresar; y, desde luego, consideramos que no hay mayor aportación para la transformación de nuestra sociedad, y aquí hablo ya como representante de un gobierno progresista social demócrata que cree que es la educación y la formación lo que nos va a hacer a todos mejores personas y vamos a poder contribuir mejor a un mundo global que, digamos, no está exento de aristas y de movimientos que caminan justamente en la dirección contraria; con lo cual, asentar nuestro progreso, y esto es lo que intentamos hacer desde el gobierno, recién llegados como estamos en esta etapa de la legislatura, asentarlo en valores, en educación, en formación, en conocimiento, en colaboración con todos los que lo tienen, en este caso, las universidades; para nosotros es un objetivo y una meta irrenunciable.

Para lograrlo, la Policía Española también se está implicando; y me consta porque su director Francisco Pardo que está recién incorporado a su puesto, tiene un firme compromiso en esta tarea y, entre todos, ya en estos presupuestos que estamos ejecutando recientemente aprobados del año 2018 y en la previsión del año 2019, queremos contribuir con actividades formativas dándole la prioridad que deben tener en esta hoja de ruta de modernización de las Fuerzas y Cuerpos de Seguridad del Estado, con carácter general y de la Policía Española con carácter particular, ya que estamos en unas jornadas en las que sois, la Policía, las que estáis liderando este desarrollo y con las

que queremos trabajar para una sociedad más justa, más humana y, también creemos que con eso correspondemos justamente a las necesidades de la sociedad. Mayor seguridad nos conduce a mayor libertad.

Y es evidente que hemos avanzado mucho, pero que sigue siendo necesario estimular a la sociedad para ampliar la base y la capacidad de innovar. No podemos permitirnos para nada aminorar el impulso en este ámbito, conocemos el reto y reconocemos la meta; y tenemos herramientas a nuestra disposición para alcanzar esos objetivos que van en esa dirección que hemos marcado, estas metas que hemos marcado.Y tenemos que empeñarnos porque fácil no es, ya saben ustedes que ahora estamos en la fase de definición del techo de gasto, de los límites presupuestarios, pero cuando se tiene, yo soy de las personas que cree que cuando se tiene la voluntad y creo que todos los que somos gestores públicos; cuando se tiene la voluntad, cuando se tiene el empeño de que hay una serie de objetivos, académicos, científicos incluso culturales dentro de las instituciones, siempre se puede hacer un hueco; como no se puede hacer es no teniendo la ambición de que se consiga, entonces, tenemos que tener esa ambición.

Y como bien dijo el Ministro Fernando Grande Marlasca con motivo de su comparecencia en el congreso, en la comisión de interior, estamos ante un Ministerio del Interior que, a pesar de las imágenes preconcebidas que todos podamos tener de un ministerio de esta naturaleza, nos estamos orientando y comprometiendo hacia lo que él ha insistido mucho y que yo lo traslado con toda la convicción, al concepto de seguridad humana, concepto más amplio de seguridad que podemos concebir, que está abierto a la calidad de vida de las personas, garantizando diversidad, garantizando valores cívicos pero, sobre todo, valores humanos.Valores que muchos filósofos hoy en día se están ocupando de ellos entre los cuales existe algo que es una palabra muy olvidada desgraciadamente como es la compasión, hacia aquellos seres humanos que tienen peores circunstancias que nosotros y ahí entraría todo en el debate que el Comisario Pereiro conoce bien, que es el tema de la extranjería, en el cual, hay que utilizar todos los recursos pero a veces también hay que tener esa consideración, respeto a la persona humana. Y valores que se adquieren también, no solamente de que uno forme parte de esa escala de valores, sino porque pueden ser estudiados, aprendidos objetivados y reconocidos.

Desde nuestra incorporación al Gobierno de España estamos trabajando convencidos de que esta formación y la innovación deben ser ejes centrales de nuestro trabajo para garantizar la seguridad pero, también, porque queremos actuar y es también una definición de este ministerio con transparencia, con certeza, con seguridad y siempre con humildad.

La innovación, entiendo bien y esta es la apreciación de una persona que también a lo largo de su trayectoria profesional, en la Administración Pública, ha trabajado en diferentes proyectos y proyectos europeos también, de fomento de la innovación y de la cooperación industrial, y cooperación tecnológica. La innovación entiendo que se escribe siempre en primera persona; quiero decir con esto que es irrenunciable. Si la propia persona a la hora de formar parte de un equipo, no tiene clara una posición innovadora, el proyecto nunca saldrá adelante, se escribe siempre a partir de la actitud con la que se conforman los equipos, los proyectos, a partir de los compromisos para evolucionar de ese sano inconformismo, de no resignarse a las rutinas, de no mirar a otro lado frente a los problemas; de personas capaces de pensar más allá del horizonte previsible y de promover la clase de cambios que son los que van a mejorar la vida de la sociedad. En definitiva, de promover una cultura generadora de ideas que, de alguna manera por lo que he estado viendo a lo largo del programa, es de lo que se ha estado tratando.

Una cultura generadora de ideas que debe conectar a la industria, al sector tecnológico y al ámbito investigador y generar sinergias capaces de provocar las mejoras que la ciudadanía nos exige. Saben ustedes que muchas veces se habla mucho de I+D y se olvida de la letra pequeña "i" que es la innovación; y en definitiva se trata de la investigación al mercado, porque la innovación es la posibilidad de que ese producto llegue al mercado y que llegue al mercado no solamente al ámbito del negocio, que es importante, porque sino las empresas no actuarían ahí, sino que significa que es el punto en el que sale de una sala de investigación para llegar a beneficiar a toda una sociedad.

Durante estos días han tenido ustedes la ocasión de conocer de la mano de profesionales policiales y de otros ámbitos, la actividad innovadora que estamos desarrollando desde el ámbito ya, y hablo por parte de Policía, de ámbitos como la seguridad ciudadana, la Policía Científica, las fronteras o la inteligencia en el campo de la formación y la cooperación internacional. Nos sentimos orgullosos, quiero trasladar que tanto el Director General de la Policía como yo misma, estamos orgullosos del alto nivel de la Policía Española y de todas las capacidades que han ido desarrollando, y hay que decirlo, en los últimos años con los presupuestos escuetos, austeros, cuando no congelados, con menos efectivos; pero no se ha bajado la guardia. Yo quiero tener un reconocimiento a esa implicación y esa profesionalidad persona a persona, y a las Fuerzas y Cuerpos de Seguridad, y en este caso de la Policía, que ha mantenido con esa situación tan complicada por la que hemos atravesado, un alto nivel de excelencia como se ve ahora. Y, quiero trasladar, también, que lo estamos haciendo y digo nos porque ya me implico con la Policía. Sepan, también, que en la lucha contra el terrorismo y el crimen

organizado estamos apostando por el desarrollo de una Policía predictiva que permitirá apoyar la toma de decisiones acertadas en tiempo oportuno.

Por su parte, la Comisaría General de Extranjería y Fronteras, continúa trabajando en la gestión inteligente de fronteras tanto a nivel nacional como europeo.

En el terreno de la seguridad ciudadana, la actividad innovadora, habrán podido comprobar, se centra en abrir nuevas vías de comunicación y participación y, además, en apostar por las tecnologías de movilidad y de apoyo a la actividad policial para poder ofrecer respuestas ágiles porque, realmente, cuanto más complejos son los movimientos de preocupación o de amenazas o de retos que amenazan a la sociedad, el tiempo, cada vez más, estamos viendo que es un factor esencial porque trabajamos con inputs informativos a distintos niveles, en distintas lenguas, a velocidades diferentes; y sincronizar toda esa información requiere capacidades tecnológicas y un cálculo de los tiempos en lo que es fundamental para que el momento de la actuación sea el momento del éxito policial.

En el campo de la Policía Científica, cabe destacar el intercambio trasfronterizo de vestigios forenses, el manual de las buenas prácticas en comparación facial o la construcción de una red europea de usuarios de aplicaciones biométricas. Y, de la misma manera, la cooperación internacional, la Policía Nacional, -me gustaría destacarlo muchísimo en este ámbito y delante de la vicerrectora de internacional porque ella también creo que tendrá esa sintonía-; el hecho de que estemos participando en la Policía Nacional en proyectos de ámbito internacional diferentes entre ellos seis proyectos en el programa marco, el programa H2020 que es el programa estrella europeo de investigación y de innovación 2014-2020, que es un programa de concurrencia competitiva muy potente, y el hecho de que España esté participando y teniendo retornos a través del mismo para financiar nuestros proyectos; yo creo que nos debe llenar de orgullo y da buena idea de lo que les decía antes del alto nivel en el que estamos.

Estos proyectos pretenden mejorar las comunicaciones policiales o la generación de inteligencia, así como el uso de drones en la Policía y crear sistemas de alerta temprana ante las amenazas cibernéticas.

Como bien saben, la historia se escribe a partir del esfuerzo colectivo, el esfuerzo de todos a través de la coordinación y la cooperación que es lo que nos permite estar a la vanguardia. Y, desde la Secretaría de Estado, uno de nuestros esfuerzos es que a lo largo de este periodo de legislatura consigamos también lograr la máxima coordinación entre las capacidades y las

fortalezas que tienen ambos cuerpos, Policía Nacional y Guardia Civil, para lograr también, en algunos aspectos, que esa coordinación sea un vector de fuerza que potencie, todavía más, las capacidades que tenemos en el ámbito de la seguridad.

Para nuestras instituciones, en este ámbito, pues, para la Policía Española especialmente, la innovación es lo que nos va a permitir seguir siendo un referente nacional e internacional, es esa llegada ya al punto de mercado, ya no solo nos estamos quedando en los desarrollos investigadores, sino que el estar ya aplicándolo día a día en nuestra actividad, es lo que creo que nos va a seguir acercando al ciudadano que en última instancia es nuestra razón de ser.

Y termino ya, esperamos que este curso haya sido del interés y del agrado de todos los que habéis tenido ocasión de participar; que haya fomentado un debate constructivo y, por qué no, que haya servido para aportar también nuevas ideas en ese ámbito de la I+D, de lanzar vías que los que estén en la línea, en la banda alta de investigación, recojan el testigo de nuestras necesidades y que nos ayuden a mejorar la función policial y el servicio público que prestamos.

Quiero decirles que este curso no termina aquí, para nosotros, es aquí donde creemos que todo empieza porque de ustedes depende la aplicación de lo adquirido, aquí empieza la verdadera transformación con vuestra actuación, con vuestra actitud y con vuestro compromiso.

A petición del director, queda clausurada la edición del presente curso y esperamos vernos en la próxima edición aquí, otra vez, en El Escorial, con la Universidad Complutense.

- SEGURIDAD PÚBLICA Y POLICÍA EN EL COMIENZO DEL SIGLO XXI (1999)
- LA CIUDAD Y LA SEGURIDAD DE SUS HABITANTES (2000)
- ¿HACIA UNA POLICÍA EUROPEA? (2001)
- BLANQUEO DE CAPITALES, FUENTES DE DINERO NEGRO (2002)
- PRESENTE Y FUTURO DE LA SEGURIDAD EN LA SOCIEDAD DE LA INFORMACIÓN (2003)
- CIENCIA POLICIAL CP 73 (2004)
  - Ciencia y tecnología policial
  - Ciencia y Policía
  - La delincuencia tecnificada
  - Tecnologías para la gestión e intervención policial
  - La enseñanza virtual para la gestión del conocimiento: una apuesta con futuro
- CIENCIA POLICIAL CP 74 (2004)
  - La inspección ocular
  - Análisis de ADN en la investigación criminal
  - La identificación lofoscópica
  - El estudio de registro de audio: técnicas de última generación
  - La documentoscopia
  - La balística identificativa y las trazas instrumentales
  - La investigación en el campo
- CIENCIA POLICIAL CP 78 (2005)
  - El negocio mundial de las drogas. Características
  - Estrategias de penetración. Evolución de la oferta y la demanda. Tendencias
  - Logística y distribución de droga
  - Impacto económico y sanitario de las drogas ilegales
  - El ser humano como mercancía: oferta y demanda
  - Negocios conexos. Las falsificaciones documentales
  - Explotación de la inmigración irregular: mercadear con la dignidad humana
  - Inmigración irregular incidencia económica y social
- VIOLENCIA, EDAD Y GÉNERO. CONTIGO PUEDO (2006)
- GLOBALIDAD Y DELINCUENCIA. PREVENCIÓN Y RESPUESTAS (2007)
- SEGURIDAD PÚBLICA - SEGURIDAD PRIVADA. ¿DILEMA O CONCURRENCIA? (2008)
- SEGURIDAD INTERIOR, SEGURIDAD EXTERIOR. DÓNDE QUEDAN LAS FRONTERAS (2009)
- LA SEGURIDAD EN EUROPA TRAS EL TRATADO DE LISBOA (2010)
- LA POLICÍA CIENTÍFICA. UN SIGLO AL SERVICIO DE LA JUSTICIA (2011)
- POLICÍA 3.0. REDES SOCIALES EN LA NUEVA DIMENSIÓN DE LA SEGURIDAD (2012)
- RETOS Y DESAFÍOS DE LA SEGURIDAD EN EL MEDITERRÁNEO (2013)
- LA POLICÍA GLOBAL (2014)
- VIOLENCIA FAMILIAR, DE GÉNERO Y SEXUAL (2015)
- LIBERTAD Y SEGURIDAD FRENTE A LAS NUEVAS AMENAZAS (2016)
- SEGURIDAD Y DESARROLLO ECONÓMICO (2017)

PUBLICACIONES
DE LA FUNDACIÓN POLICÍA ESPAÑOLA
Colección Estudios de Seguridad