PLAN ESTRATÉGICO CONTRA LA CIBERCRIMINALIDAD

MINISTERIO DEL INTERIOR

Secretaría de Estado de Seguridad

FEBRERO 2021

GOBIERNO DE ESPAÑA
MINISTERIO DEL INTERIOR

PÁGINA INTENCIONADAMENTE EN BLANCO

Contenido

1. LA CIBERCRIMINALIDAD: CONTEXTO Y SITUACIÓN 4

La cibercriminalidad en España 6

2. UN PLAN NECESARIO CONTRA LA CIBERCRIMINALIDAD 7

3. TENDENCIAS OBSERVADAS EN LA CIBERCRIMINALIDAD 9

3.1. Pandemia mundial provocada por la COVID-19 9
3.2. Explotación y abuso sexual de menores o personas con discapacidad necesitadas de especial protección 9
3.3. Estafas a través de las TIC 10
3.4. Dominios web maliciosos relacionados con situaciones excepcionales 11
3.5. Amenazas, coacciones y otros delitos 11
3.6. Falsedades documentales 11
3.7. Desinformación y amenazas híbridas 11
3.8. Ciberataques a infraestructuras críticas y operadores de servicios esenciales 12
3.9. Secuestro de información *(ransomware)* 12
3.10. Denegaciones de servicio 12

4. RETOS A AFRONTAR 13

4.1. Cultura sobre ciberseguridad 13
4.2. Las TIC como elemento facilitador para la comisión de delitos 13
4.3. Redes sociales y seguridad ciudadana 13
4.4. Cifrado de la información y de las comunicaciones 13
4.5. Servicios en la nube 14
4.6. Redes *Darknet* 14
4.7. Crimen como servicio (*CaaS*) 14
4.8. La dificultad de atribución de acciones delictivas 14
4.9. Criptovalores 14
4.10. Tecnología 5G 15
4.11. El *blockchain* 15
4.12. La inteligencia artificial (IA) 15
4.13. Dispositivos electrónicos y terminales telefónicos 15
4.14. Identidad digital 16

5. CAPACIDADES DISPONIBLES EN EL MINISTERIO DEL INTERIOR 16

6. PRINCIPIOS RECTORES Y OBJETIVOS DEL PLAN ESTRATÉGICO 18

7. EJES ESTRATÉGICOS Y LÍNEAS DE ACCIÓN 19

EJE ESTRATÉGICO I: CULTURA DE PREVENCIÓN DE LA CIBERCRIMINALIDAD 19
EJE ESTRATÉGICO II: POTENCIACIÓN DE CAPACIDADES 20
EJE ESTRATÉGICO III: GENERACIÓN DE CIBERINTELIGENCIA 22
EJE ESTRATÉGICO IV: COORDINACIÓN NACIONAL Y COOPERACIÓN INTERNACIONAL 24
EJE ESTRATÉGICO V: CONTRIBUIR A LA DISPONIBILIDAD DE UN MARCO NORMATIVO ADECUADO 26
EJE ESTRATÉGICO VI: COLABORACIÓN PÚBLICO-PRIVADA 28

8. GOBERNANZA DEL PLAN 29
8.1 Dirección y coordinación del Plan 29
8.2 Comisión de seguimiento 30
8.3 Mesa permanente de coordinación 30
8.4 Planes de acción operativos 30
8.5 Informe de desarrollo y ejecución del Plan 31

9. RECURSOS HUMANOS Y ECONÓMICOS NECESARIOS PARA LA EJECUCIÓN DEL PLAN. 31

10. VIGENCIA Y ACTUALIZACIÓN DEL PLAN 31

ANEXO I. DEFINICIÓN DE CONCEPTOS 33

ANEXO II. MARCO NORMATIVO DE REFERENCIA 36

1. LA CIBERCRIMINALIDAD: CONTEXTO Y SITUACIÓN

Como sucesivamente ponen de manifiesto los diferentes informes en la materia, el crecimiento de la cibercriminalidad en el mundo viene conociendo una fuerte progresión durante los últimos años, en paralelo con el incremento del uso y el desarrollo de las tecnologías de la información y las comunicaciones (en adelante TIC) en todos los ámbitos, tanto públicos como privados.

La Estrategia Nacional de Ciberseguridad de 2019 (en adelante ENCS) establece: "*El término cibercriminalidad hace referencia al conjunto de actividades ilícitas cometidas en el ciberespacio que tienen por objeto los elementos, sistemas informáticos o cualesquiera otros bienes jurídicos, siempre que en su planificación, desarrollo y ejecución resulte determinante la utilización de herramientas tecnológicas; en función de la naturaleza del hecho punible en sí, de la autoría, de su motivación, o de los daños infligidos, se podrá hablar así de ciberterrorismo, de ciberdelito, o en su caso, de hacktivismo".*

Continúa indicando que: *"son tres los ámbitos en los que se desenvuelve la lucha contra la cibercriminalidad: el ciberespacio como objetivo directo de los hechos delictivos, o de la amenaza; el ciberespacio como medio clave para su comisión; y el ciberespacio como medio u objeto directo de investigación de cualquier tipo de hecho ilícito".*

Las potencialidades y beneficios derivados del conjunto de redes, medios técnicos y servicios que conforman el ciberespacio no han hecho más que comenzar. Pero también lo han hecho ya –y con un fuerte y negativo impacto sobre la seguridad de los ciudadanos, sus instituciones, la opinión pública, la economía y las empresas, etc.– un amplio abanico de **amenazas,** frente a las que deben articularse estrategias y planes operativos de actuación para hacer frente a las mismas.

El más reciente Estudio sobre la Cibercriminalidad en España, cuya última actualización fue publicada por el Gabinete de Coordinación y Estudios en el año 2020, señala cómo la importancia de la cibercriminalidad va creciendo año tras año, como se demuestra con el aumento del número de hechos conocidos. Pero otro hecho innegable es el peso proporcional que va adquiriendo dentro del conjunto de la criminalidad, observándose en la tabla nº 1, que del año 2016 al 2019, se ha producido un incremento del 4,6% al 9,9%.

En el ámbito de la Unión Europea, en marzo de 2019, los representantes permanentes otorgaron un mandato a la Presidencia del Consejo de la Unión Europea para iniciar conversaciones con el Parlamento Europeo sobre la puesta en común de los conocimientos especializados en ciberseguridad, centrándose en dos iniciativas: establecer una base de conocimientos de alto nivel en materia de ciberseguridad, materializada a través de la puesta en marcha del **Centro Europeo de Competencia e Investigación en Ciberseguridad**; y la creación de una **Red de Centros Nacionales de Coordinación** en el ámbito de la ciberseguridad.

Unas iniciativas imprescindibles a la luz de los datos actuales sobre el impacto de la cibercriminalidad, ya que según las estimaciones de la Comisión Europea y del Parlamento Europeo se calcula que los ataques informáticos cuestan ya a la economía mundial más de 530.000 millones de euros cada año y porque según datos también de ambas instituciones, la incidencia económica de los hechos relacionados con la cibercriminalidad **se ha multiplicado por cinco desde 2013** y además el **87 % de los ciudadanos europeos** consideran que esta realidad es un desafío importante para la seguridad interior de la UE.

Frente a tal realidad ciberdelictiva, **Europol** y **Eurojust** –en un documento conjunto de junio de 2019, *Common challenges in combating cybercrime. As identified by Eurojust and Europol*– han puesto de manifiesto también las dificultades y las barreras existentes para la investigación por parte de los cuerpos policiales y la obtención de las necesarias **evidencias electrónicas** para investigar y perseguir este tipo de delitos y amenazas, sobre todo por la dificultad en el acceso a datos relevantes para llevar a cabo sus pesquisas con eficacia –y, a la postre, para el propio éxito del correspondiente proceso penal– y que proceden, por un lado, del recurso creciente a la encriptación por los delincuentes; ya por las propias barreras o deficiencias normativas que dificultan tal acceso; ya por las limitaciones de territorialidad jurisdiccional, frente a la inexistencia de fronteras en este tipo de delitos; bien por la propia sobrecarga de información de los servicios policiales, que precisan de más capacidades para gestionar la misma; y, también, por la todavía débil conciencia de usuarios, empresas e instituciones frente a los estándares de seguridad necesarios en la nueva realidad marcada por el uso constante del ciberespacio.

La **Estrategia Europea de Ciberseguridad,** revisada en septiembre de 2017, así como la reciente publicación de la Estrategia de Ciberseguridad Europea para el Decenio Digital en diciembre de 2020 también han puesto de manifiesto la necesidad de impulsar medidas que creen un entorno seguro en el ciberespacio para los ciudadanos, donde se establezcan sinergias en materia de ciberseguridad, no solo entre los estados miembros, sino también con el sector privado.

Esta Estrategia, al tratar la **lucha contra la cibercriminalidad,** afirma que nuestra dependencia de las herramientas *online* ha incrementado exponencialmente nuestra superficie de exposición a los ciberataques y ha llevado a una situación en la que la investigación de prácticamente todos los delitos tiene un componente digital. Ello explica los estrechos vínculos de la Estrategia con el resto de la política de seguridad de la UE, tal y como se refleja en las referencias “ciber” de la Estrategia de la UE para una Unión de la Seguridad para el período 2020-2025.

La cibercriminalidad en España

Los hechos conocidos relacionados con la cibercriminalidad son un problema creciente para todos los países, y España, al igual que el conjunto de los Estados de la UE, no escapa a esa realidad objetiva.

Los sucesivos Informes anuales sobre la evolución de la cibercriminalidad publicados por el Ministerio del Interior han venido ilustrando y poniendo de manifiesto en nuestro país esa constatación observada en el ámbito internacional.

HECHOS CONOCIDOS RELACIONADOS CON CIBERCRIMINALIDAD

	Policía Nacional, Guardia Civil, P. Foral de Navarra y Policías Locales				Todos los Cuerpos Policiales				
TIPOLOGÍA	**2011**	**2012**	**2013**	**2014**	**2015**	**2016**	**2017**	**2018**	**2019**
ACCESO E INTERCEPTACIÓN ILÍCITA	1.492	1.701	1.805	1.851	2.893	3.243	3.150	3.384	4.004
AMENAZAS Y COACCIONES	9.839	9.207	9.064	9.559	10.607	12.036	11.812	12.800	12.782
CONTRA EL HONOR	1.941	1.891	1.963	2.212	2.205	1.546	1.561	1.448	1.422
CONTRA LA PROPIEDAD INDUSTRIAL/INTELECTUAL	222	144	172	183	172	129	121	232	197
DELITOS SEXUALES	755	715	768	974	1.306	1.231	1.392	1.581	1.774
FALSIFICACIÓN INFORMÁTICA	1.860	1.625	1.608	1.874	2.644	3.017	3.280	3.436	4.275
FRAUDE INFORMÁTICO	21.075	27.231	26.664	32.842	62.038	70.178	94.792	136.656	192.375
INTERFERENCIA EN LOS DATOS Y EN EL SISTEMA	228	298	359	440	1.193	1.336	1.291	1.192	1.473
TOTAL grupo penal	**37.412**	**42.812**	**42.403**	**49.935**	**83.058**	**92.716**	**117.399**	**160.729**	**218.302**

Tabla 1. Último estudio sobre la cibercriminalidad en España 2019

Atendiendo a las estadísticas del Ministerio del Interior, en 2015 se conocieron un total de 83.058 hechos conocidos relacionados con la cibercriminalidad, cifra que ha ascendido a 218.302 a finales de 2019. Esta variación supone un fortísimo incremento del **162.8%** en apenas cinco años, lo que ilustra claramente la progresión de estas nuevas modalidades delictivas en España. De modo que, si en 2015 la cibercriminalidad representaba el 4.1% del total de nuestra criminalidad conocida, a finales de 2019 había escalado hasta un peso relativo de ya el **9.9%**.

Cabe resaltar con respecto a las cifras anteriores el elevado número de conductas que no son denunciadas por parte de los usuarios de las TIC, provocando una creciente "cifra negra u oculta" asociada a la cibercriminalidad que debería engrosar estas estadísticas, y que permite inferir que las denuncias presentadas suponen tan solo la punta del iceberg de este fenómeno delincuencial.

En cuanto a los incidentes de ciberseguridad en España, el CERT del Centro Criptológico Nacional **(CCN-CERT)** durante el año 2019 gestionó **42.997** incidentes. Asimismo el **INCIBE-CERT**; con el que el Ministerio del Interior cuenta desde 2012 con un Acuerdo Marco de Colaboración en materia de Ciberseguridad para la gestión conjunta del CSIRT en materia de infraestructuras críticas y servicios esenciales; gestionó durante este mismo periodo un total de **107.397** incidentes.

En cuanto a los ciberincidentes registrados en las redes y sistemas de operadores críticos y operadores de servicios esenciales a lo largo del año 2019, se ha constatado la existencia de un total de 818 (el 0.7% del total), con un incremento del **13.29%** con respecto al año anterior.

En los últimos años, se ha evidenciado que por parte de individuos u organizaciones terroristas, se hace un uso extensivo de internet y las redes sociales, mediante la construcción de falsas narrativas alejadas de la realidad social, con las que han intentado reclutar nuevos terroristas para socavar nuestra sociedad democrática.

2. UN PLAN NECESARIO CONTRA LA CIBERCRIMINALIDAD

La **Estrategia de Seguridad Nacional de 2017**, estableció como uno de sus objetivos el de *"garantizar un uso seguro de las redes y los sistemas de información y comunicaciones a través del fortalecimiento de las capacidades de prevención, detección y respuesta a los ciberataques, potenciando y adoptando medidas específicas para contribuir a la promoción de un ciberespacio seguro y fiable".*

Por su parte, la **Estrategia Nacional de Ciberseguridad 2019** (en adelante, **ENCS-2019**), aprobada por el Consejo de Seguridad Nacional en abril de 2019, y en línea con la estrategia homónima de 2013, estableció la posición de España ante una nueva concepción de la ciberseguridad en el marco de nuestra Política de Seguridad Nacional. En este sentido, **el presente Plan se alinea con lo recogido en esta Estrategia Nacional, a través del desarrollo de los Ejes Estratégicos y las Líneas de Acción** establecidas en el mismo.

Esa nueva posición y concepción pivota sobre la consideración del ciberespacio como un espacio común global caracterizado por su apertura funcional y fuerte dinamismo, por la ausencia de soberanía sobre el mismo, su débil jurisdicción, la facilidad de acceso y la dificultad de atribución de las acciones que en él se desarrollan, circunstancias todas ellas que se traducen en un escenario que ofrece innumerables oportunidades de futuro, pero que, a la vez, presenta serios desafíos para nuestra seguridad.

Entre dichos desafíos, la cibercriminalidad es, como ya ha quedado establecido, un creciente problema de seguridad y una de las amenazas más extendidas y generalizadas en nuestras sociedades, con un fuerte incremento año tras año y que victimiza cada vez de manera más importante a los ciudadanos, nuestras instituciones y las empresas.

Asimismo, la **Estrategia Nacional contra el Crimen Organizado y la Delincuencia Grave 2019-2023,** dentro de su **Eje 3** dedicado a la lucha contra los mercados criminales y las graves formas delictivas, persigue impulsar la investigación criminal sobre las principales actividades criminales en nuestro país, haciéndose referencia expresa y prioritaria a la cibercriminalidad e indicando que "*el riesgo de ataques informáticos contra instituciones,*

personas físicas y jurídicas a gran escala debe ser considerado alto en relación a otras formas de delincuencia".

Así mismo, en el octavo eje de esta estrategia expresa: "*potenciar la actualización y especialización de los operadores públicos de seguridad, mediante la continua adaptación de los procedimientos de trabajo a los nuevos métodos y técnicas empleados por las organizaciones criminales".*

Por otro lado, la **Estrategia Nacional Contra el Terrorismo 2019** se refiere al ciberespacio como un espacio global común, idóneo para la actuación del terrorismo y los extremismos violentos, e integrándolo por ello como espacio de actuación prioritaria en el marco de dicha estrategia que, además, señala como objetivo específico el desarrollo de manera coordinada de "*todas las capacidades necesarias para hacer frente al terrorismo y al extremismo violento en el ciberespacio*".

Otros documentos, como la **Estrategia de Seguridad Aeroespacial Nacional de 2019**, aprobada por el Consejo de Seguridad Nacional, abordan igualmente la necesidad de "*potenciar la cooperación policial internacional en la investigación criminal de temas aeroespaciales de su competencia para amenazas de crimen organizado, terrorismo y cíber*".

Todo ello pone de manifiesto la necesidad de elaborar y poner en marcha un Plan específico y de carácter estratégico contra la cibercriminalidad en nuestro país, acorde con el diagnóstico y los retos presentados hasta aquí, y que ha conducido a que la **ENCS-2019** se haya marcado como objetivo general para España *"garantizar el uso seguro y fiable del ciberespacio, protegiendo los derechos y las libertades de los ciudadanos y promoviendo el progreso socio-económico".*

Para alcanzar ese objetivo la **ENCS-2019** define cinco grandes objetivos específicos, siendo uno de ellos el de garantizar el *"uso seguro y fiable del ciberespacio frente a un uso ilícito o malicioso"*, y para cuyo logro se establece la tercera de las siete líneas de acción contempladas en esta Estrategia y que está dirigida a *"reforzar las capacidades de investigación y persecución de la cibercriminalidad, para garantizar la seguridad ciudadana y la protección de los derechos y libertades en el ciberespacio"*.

Esta específica Línea de Acción contempla, a su vez, un amplio abanico de medidas a desarrollar en diferentes ámbitos, marcando como finalidades principales:

- Reforzar el marco jurídico y la cooperación con los operadores judiciales para responder eficazmente a la cibercriminalidad, tanto en lo relativo a la definición de tipos penales como en la regulación de adecuadas medidas de investigación.
- Reforzar las acciones encaminadas a potenciar las capacidades de investigación, atribución, persecución y, en su caso, la actuación penal, frente a la

cibercriminalidad, fomentando el intercambio de información, experiencia y conocimientos, y la coordinación de investigaciones entre las unidades y el personal con responsabilidades en la investigación y persecución de la cibercriminalidad.

- Asegurar a los profesionales de las Fuerzas y Cuerpos de Seguridad del Estado (en adelante FCSE) y del Derecho el acceso a los recursos humanos y materiales que les proporcionen el nivel necesario de conocimientos para la mejor aplicación del marco legal y técnico asociado.
- Fomentar la colaboración y participación ciudadana y con el sector privado, articulando instrumentos de intercambio y transmisión de información de interés policial, y promoviendo el desarrollo de campañas de prevención de la cibercriminalidad orientadas a ciudadanos y empresas.

3. TENDENCIAS OBSERVADAS EN LA CIBERCRIMINALIDAD

En línea con lo que vienen poniendo de manifiesto los sucesivos ***IOCTA (Internet Organised Crime Threat Assessment)*** de ***Europol*** sobre la evaluación de la amenaza del crimen organizado en internet, y con la finalidad de reflejar las tendencias actuales en materia de cibercriminalidad, se exponen y plantean a continuación una serie de aspectos que ofrecen una aproximación a la actual realidad delictiva en este ámbito, tanto desde el punto de vista de modalidades de ejecución detectadas como de elementos perturbadores:

3.1. Pandemia mundial provocada por la COVID-19

La coyuntura económica y social derivada de la aparición de la pandemia provocada por la COVID-19 en el mundo ha derivado en un incremento sustancial del uso de las TIC por parte de la población.

Esta circunstancia lleva asociada irremediablemente un incremento de la superficie de exposición de activos sensibles en el ciberespacio y la consecuente irrupción de amenazas capaces de explotar vulnerabilidades de elevado impacto.

3.2. Explotación y abuso sexual de menores o personas con discapacidad necesitadas de especial protección

Estas conductas conforman un fenómeno delictivo en notable crecimiento, de gran repercusión y extremada preocupación mundial, situándose en la lista de las principales amenazas criminales que deben afrontar las Fuerzas y Cuerpos de Seguridad (en adelante FCS) en la actualidad.

La principal tendencia en esta área es el ingente volumen de material sexual infantil autogenerado (*sex-casting*) que circula en la red, y que continúa incrementándose significativamente. Dicho material es generado y posteriormente difundido a través de diferentes plataformas en internet y a través de las TIC, bien por propia iniciativa del menor, o bien a través de solicitudes *online*.

Cabe reseñar además el creciente uso de las TIC por parte de redes trasnacionales de trata de seres humanos.

En este sentido, sería necesario aumentar las capacidades de las FCS dedicadas a la prevención y respuesta de estas conductas.

3.3. Estafas a través de las TIC

Sin duda, aquellos delitos relacionados con estafas son el fenómeno con mayor incidencia en la actualidad, detectándose incrementos estadísticos muy significativos, según el estudio sobre la cibercriminalidad en España 2019 del Ministerio del Interior. En este sentido, se detecta un importante incremento de las estafas tradicionales que se valen de las TIC, consiguiendo así extender los efectos de su acción criminal a un número incontable e indeterminado de potenciales víctimas.

Como fenómeno emergente en el ámbito del fraude, destacan las **estafas** relacionadas con tarjetas bancarias, *phishing,* fraude en banca electrónica, fraude en comercio electrónico, o supuestos soportes técnicos.

Esta mecánica delictiva está siendo utilizada por grupos organizados de carácter transnacional y, aun cuando el perjuicio individualmente ocasionado no suele resultar muy elevado, genera un volumen muy importante de denuncias.

Otro fenómeno en auge es la generalización de las **estafas de inversiones** a través de ofertas engañosas de alta rentabilidad, tanto en moneda de curso legal en los diferentes estados como en criptomonedas.

También en el contexto de delitos relacionados con el fraude, uno de los principales *modus operandi* en la actualidad es el conocido como ***SIM swapping.*** En estos casos los cibercriminales tratan de burlar el doble factor de autentificación (2FA) establecido por las entidades bancarias para proteger las transacciones electrónicas de sus clientes.

Como fenómeno emergente de especial interés cabe destacar la adaptación del ***BEC (Business Email Compromise)*** a objetivos más rentables y menos cualificados. Las organizaciones criminales cada vez, no solo emplean técnicas más sofisticadas de *Information Gathering* a través de todo tipo de herramientas y técnicas de fuentes abiertas (OSINT) para obtener datos para explotar mediante ingeniería social, sino que además invierten en recursos técnicos para evitar las medidas de protección de las víctimas.

3.4. Dominios web maliciosos relacionados con situaciones excepcionales

Este tipo de acciones se erigen como elemento vertebrador de gran número de ciberataques, y buscan registrar y emplear recursos semejantes al dominio oficial de un determinado evento o circunstancia excepcional (Ejemplo: *COP-25, COVID-19*, etc.) con la finalidad de ser utilizado en actividades delictivas, como distribución de *malware*, estafas *online* o *phishing*.

3.5. Amenazas, coacciones y otros delitos

Fruto de la migración desde un plano físico tradicional al ciberespacio que ha experimentado la actividad relacionada con el acoso, las extorsiones y las amenazas, los delitos contra la libertad y conductas relacionadas con la violencia de género, y las diversas modalidades relacionadas con los delitos de odio, hechos en los que los autores encuentran en las TIC un aliado inmejorable.

3.6. Falsedades documentales

Han aflorado nuevas tendencias como el *morphing*, técnica consistente en realizar, mediante el uso de software especializado, modificaciones de la fotografía original de un documento previamente sustraído sustituyéndola por una fotografía del usuario final del mismo.

Por este motivo además de para el uso directo (sin alteración del documento) por parte de impostores, se produce un incremento de los hurtos de documentos y de su venta en redes sociales. Para ello las redes sociales son utilizadas por organizaciones criminales en toda la Unión Europea y el resto del mundo para centralizar los documentos sustraídos o perdidos para su falsificación, distribución y venta.

3.7. Desinformación y amenazas híbridas

Cobra especial importancia en los últimos tiempos la desinformación como medio para menoscabar la confianza en las instituciones del Estado, pudiendo formar parte de una "amenaza híbrida" más completa que impida o dificulte el avance de España, y por tanto Europa, en sus intereses geopolíticos, como viene reflejado en el Plan de Acción contra la Desinformación, de 5 de diciembre de 2018 de la Unión Europea.

Conforme a la normativa actual española en materia penal, estas conductas no siempre son delictivas, tan solo algunas de sus manifestaciones, en consonancia con lo recogido en la Constitución Española en su artículo 20, que reconoce el derecho a comunicar o recibir información veraz por cualquier medio de difusión.

3.8. Ciberataques a infraestructuras críticas y operadores de servicios esenciales

Los ciberataques cuya finalidad sea atacar las bases del funcionamiento de nuestra sociedad, como pudieran ser mediante la paralización o interrupción de los servicios esenciales y las infraestructuras tecnológicas que los sustentan (infraestructuras críticas) bien por una finalidad terrorista, ideológica o de cualquier otro tipo, siguen siendo prioritarios en su prevención y persecución.

Relacionado con lo anterior, otra de las amenazas a las que se sigue prestando una gran atención, por su incidencia y peligrosidad, son todas aquellas injerencias a través de las redes que dan lugar al ciberespionaje, logrando el acceso por actores no legítimos a información de carácter privado o confidencial que pudiera menoscabar el buen funcionamiento, o permitir la competencia desleal, de nuestras empresas, instituciones e intereses de individuos particulares.

3.9. Secuestro de información *(ransomware)*

La distribución de esta tipología de *malware* ha registrado un incremento muy significativo, no solo en el número de ataques registrados, sino especialmente en el impacto causado en individuos y organizaciones de diversa índole.

Los cibercriminales han escogido este tipo de ciberataque como una de sus principales herramientas para la obtención de beneficios, extorsionando a las víctimas, especialmente a grandes empresas, con la revelación de datos de carácter personal de clientes, proveedores o secretos de la empresa. En muchas ocasiones las víctimas ceden al chantaje y abonan fuertes sumas económicas ante la posibilidad de que no se recupere la información sustraída o, en muchos casos, se difunda la misma.

3.10. Denegaciones de servicio

Las denegaciones de servicio, pese a no representar actualmente una amenaza de primer orden en materia de ciberseguridad, pueden provocar a medio o largo plazo serios daños en la prestación de servicios esenciales, debido principalmente al incremento de conectividad tras la implantación del 5G.

Por otro lado, comienzan a detectarse extorsiones basadas en la amenaza de ejecución de ataques de Denegación de Servicio a compañías con alta dependencia de la disponibilidad en sus activos en su operativa.

4. RETOS A AFRONTAR

4.1. Cultura sobre ciberseguridad

El uso masificado, rutinario y habitual de infinidad de herramientas digitales en todos los sectores sociales, económicos y laborales provoca que no todos los usuarios dispongan de un suficiente nivel de autoprotección frente a los riesgos del ciberespacio.

Esta protección debe sustentarse, entre otros aspectos, en la implicación efectiva y la toma de conciencia por parte de los ciudadanos de las amenazas existentes en el ciberespacio en la actualidad de cara a evitar que las personas continúen siendo, con diferencia, el vector de ataque más explotado por los cibercriminales.

4.2. Las TIC como elemento facilitador para la comisión de delitos

El anonimato y la facilidad de transmisión actúan como elementos potenciadores de todas y cada una de las múltiples manifestaciones de la delincuencia en la red. Así como con carácter general en la difusión de todo tipo de contenidos ilícitos y en la planificación y ejecución de actividades delictivas de muy diversa naturaleza.

En especial, el uso de las TIC con estos fines supone un factor clave para atacar a instituciones de todo tipo, y a aquellas personas más vulnerables de la sociedad. Las dificultades existentes de cara a obtener las identidades reales que se encuentran detrás de los perfiles que divulgan el denominado discurso de odio, así como la ausencia de herramientas de medición fiables, capaces de cuantificar este sentimiento de odio en la red, dificulta en gran medida la capacidad preventiva y reactiva sobre este fenómeno.

Adicionalmente, cabe mencionar la difícil delimitación de estas conductas dada la necesidad de garantizar el respeto al derecho fundamental a la libertad de expresión.

4.3. Redes sociales y seguridad ciudadana

La gestión de la seguridad ciudadana por parte del Estado actualmente está condicionada en gran medida por la forma de movilización y comunicación a través de aplicaciones y redes sociales, que han permitido una mayor organización y agilidad de actuación entre los individuos o colectivos de carácter radical o violento.

4.4. Cifrado de la información y de las comunicaciones

La progresiva tecnificación de los ataques, caracterizados por un creciente uso de robustos protocolos criptográficos conduce, irremediablemente, a la imposibilidad de acceso a la información implicada en actividades delictivas, tanto en la vertiente que atañe a víctimas de ataques de secuestro de información como a las comunicaciones entre cibercriminales, caracterizadas por una elevada confidencialidad gracias a los cifrados implementados por fabricantes y empresas especializadas.

4.5. Servicios en la nube

En este sentido, se constata que un ingente volumen de los datos está migrando hacia redes de superficie, es decir, próximas a los usuarios y muy dispersas, en contraposición con el almacenamiento en los centros de proceso de datos tradicionales.

Esta circunstancia supone, por un lado, la disponibilidad de manera ubicua de cantidades masivas de recursos de información y computación, y por otro, la dificultad de la identificación de esos servicios en la nube empleados por los cibercriminales y el acceso a los mismos.

4.6. Redes *Darknet*

Estas redes han registrado un progresivo incremento en número de usuarios e infraestructura, y por ende, han fomentado la anonimización de individuos y grupos cibercriminales en sus actividades a través del uso de software específico que permite el acceso a estas redes (*TOR, Freenet, I2P*, etc.).

4.7. Crimen como servicio (*CaaS*)

En los últimos años se ha observado un crecimiento de los mercados clandestinos y foros de discusión en los que los cibercriminales ofrecen sus servicios y productos. Este sistema de negocio supone un elevado riesgo, en tanto que facilita que organizaciones criminales tradicionales puedan trasladar su actividad ilícita al ciberespacio sin necesidad de disponer de conocimientos técnicos.

4.8. La dificultad de atribución de acciones delictivas

El uso masivo de las TIC por parte de la sociedad continúa siendo uno de los principales retos a afrontar en el futuro por parte de los estados de cara a individualizar conductas delictivas de sus ciudadanos, motivado este hecho por el anonimato, la deslocalización y la ausencia de colaboración por parte de determinados estados que no solo no persiguen acciones delictivas, sino que incluso amparan a determinados grupos cibercriminales.

4.9. Criptovalores

Con una casuística extensa pero focalizada en el abono de servicios entre criminales, peticiones de rescate de información y blanqueo de capitales. La compleja fiscalización de transacciones en este tipo de medios de pago motiva el fuerte incremento de su uso por parte de delincuentes, por lo que supone un reto para la actividad investigadora de las FCS.

4.10. Tecnología 5G

La tecnología denominada 5G representa un nuevo paso en la evolución de las TIC, un cambio de las reglas técnicas en el ámbito de las comunicaciones y, por ende, representa uno de los retos más importante para las FCS, para mantener sus estándares de capacidad de investigación policial y judicial, en los próximos años.

Esta tecnología, junto con el consecuente y progresivo incremento de conexiones entre dispositivos IoT (internet de las cosas), será un foco de penetración en las organizaciones, siendo necesario bastionar y buscar fórmulas para aislar, en la medida de lo posible, las comunicaciones entre dispositivos.

4.11. El *blockchain*

Se constituirá como eje vertebrador alrededor del cual se podrá potenciar el desarrollo de aplicaciones con un mayor nivel de privacidad y seguridad en diversos ámbitos de la sociedad especialmente sensibles (sector financiero, sector salud, Administración Pública, etc.).

Para ello, la ciberseguridad jugará un papel crucial de cara a garantizar un uso seguro de este tipo de aplicaciones. Por otro lado, los *smart-contracts*, como elementos útiles para implementar acuerdos entre partes, pueden incrementar el negocio clandestino entre cibercriminales.

4.12. La inteligencia artificial (IA)

La utilización de la IA por la cibercriminalidad para cometer acciones delictivas se incrementará en los próximos años, tanto evitando los sistemas de seguridad tradicionales, explotando vulnerabilidades conocidas o descubriendo desconocidas, como utilizándose para conocer patrones de comportamiento de usuarios e identificar el mejor momento en el que realizar una acción delictiva con las mayores garantías de éxito, o suplantando personalidades mediante generación de audios, vídeos y textos falsos en acciones de desinformación.

4.13. Dispositivos electrónicos y terminales telefónicos

El uso masivo de estas herramientas provoca la generación, transmisión y almacenamiento de una cantidad de información difícilmente gestionable a efectos operativos por las FCS, tanto en lo que respecta a su interceptación legal y acceso físico, como en lo relativo al posterior análisis forense en la persecución de actividades delictivas.

4.14. Identidad digital

Es necesario impulsar la regulación de la identidad digital que permita la posibilidad de la autenticación y la firma a una persona en los casos y con las garantías previstas por el ordenamiento jurídico, y en especial con el Reglamento (UE) nº 910/2014, del Parlamento Europeo y del Consejo de 23 de julio de 2014 relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior.

Asimismo, establecer un sistema seguro y fiable de identificación en la red, persiguiendo la suplantación de identidades.

5. CAPACIDADES DISPONIBLES EN EL MINISTERIO DEL INTERIOR

El Ministerio del Interior es el departamento gubernamental responsable de la propuesta y ejecución de las políticas de seguridad ciudadana, siendo el encargado de garantizar la protección de las personas y bienes y la seguridad de los ciudadanos.

Misión y funciones que también se desarrollan en el ciberespacio, en particular en las actuaciones relativas a la prevención y en la lucha contra la cibercriminalidad, la protección de infraestructuras críticas y servicios esenciales.

Toda estrategia de ciberseguridad abarca cinco vectores de actuación: **detección, prevención, protección, respuesta y persecución**, sin poder obviarse la adecuada atención a las víctimas que el Estado debe proporcionar.

En este sentido, no hay que olvidar que en España el Ministerio del Interior es el único departamento presente en todo el ciclo de la ciberseguridad, puesto que la persecución de aquellas conductas reprochables penalmente es competencia de dicho Ministerio a través de la acción de las FCSE, labor que se desarrolla bajo la dependencia y dirección de la Administración de Justicia.

Por este motivo, desde el momento en que se comete un ciberdelito se convierte en una cuestión que es susceptible de ser judicializada, y por tanto el resto de actuaciones estarían totalmente condicionadas a la labor de la Policía Judicial.

Además, para el desarrollo del presente Plan, este Ministerio cuenta con una inmejorable posición de cara a continuar siendo una referencia en materia de prevención e investigación de la cibercriminalidad, a través de las capacidades de los siguientes organismos:

- La **Policía Nacional y la Guardia Civil** a través de sus unidades altamente especializadas en la prevención e investigación de la cibercriminalidad.
- **El Gabinete de Coordinación y Estudios** es el órgano de apoyo y asesoramiento a través del cual la persona titular de la Secretaría de Estado de Seguridad ejerce su función de coordinación y supervisión, de todas las actividades que tiene

encomendadas la Secretaría de Estado en relación con la protección de las infraestructuras críticas en el territorio nacional, en colaboración con otros departamentos ministeriales, a través del **Centro Nacional de Protección de Infraestructuras Críticas (CNPIC)**. Así mismo, ejerce, a través de la **Oficina de Coordinación de Ciberseguridad (OCC)**, las funciones de punto de contacto nacional de coordinación operativa para el intercambio de información con la Comisión Europea y los Estados miembros, en el marco de lo establecido por la Directiva 2013/40/UE de 12 de agosto de 2013, relativa a los ataques contra los sistemas de información, y actúa como canal específico de comunicación entre los Centros de Respuesta a Incidentes Cibernéticos (CSIRT) nacionales de referencia y la Secretaría de Estado de Seguridad, desempeñando la coordinación técnica en materia de ciberseguridad entre dicha Secretaría de Estado y sus organismos dependientes, sin perjuicio de las competencias atribuidas a otros ministerios.

- El **Centro de Inteligencia contra el Terrorismo y el Crimen Organizado (CITCO)** es el órgano de la Secretaría de Estado de Seguridad que impulsa y coordina la integración y valoración de cuantas informaciones y análisis operativos dispongan las FCS en materia de terrorismo, crimen organizado y radicalismo violento, para la elaboración de inteligencia criminal estratégica, y establece los criterios de actuación y coordinación operativa de los órganos u organismos actuantes en los supuestos de concurrencia en las investigaciones. Igualmente le corresponde el diseño de estrategias nacionales específicas contra estas amenazas y su financiación, coordinando y verificando su desarrollo y ejecución.

- Por su parte, la **Subdirección General de Sistemas de Información y Comunicaciones para la Seguridad (SGSICS)**, como departamento tecnológico de referencia de la Secretaría de Estado, cuenta con capacidades, infraestructura y personal cualificado en áreas específicas de seguridad en las TIC, redes y sistemas.

  Asimismo, esta Subdirección General, teniendo en cuenta las propuestas de las Direcciones Generales de la Policía Nacional y de la Guardia Civil, planificará, coordinará y, en su caso, gestionará las inversiones en sistemas de información y comunicaciones. De igual forma será la encargada de proponer a la persona titular de la Secretaría de Estado de Seguridad los planes y programas que afecten a los sistemas de información y comunicaciones en el ámbito de la seguridad, así como su coordinación, supervisión de su ejecución, evaluación y análisis de sus costes, promoviendo 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 FCSE.

6. PRINCIPIOS RECTORES Y OBJETIVOS DEL PLAN ESTRATÉGICO

Este Plan, junto a las actuaciones que permitirán su desarrollo, se rige por los siguientes principios:

1. Focalización en la **prevención.**
2. **Cooperación** entre las diferentes FCS y **colaboración** estrecha con los operadores jurídicos, en el ámbito nacional e internacional.
3. **Disponibilidad** de capacidades suficientes y adecuadas para articular respuestas adaptadas a las diferentes modalidades delictivas.
4. **Colaboración** con la industria y con todos los operadores relevantes en materia de ciberseguridad en el sector público y privado, tanto en el ámbito nacional como internacional.
5. **Respeto** escrupuloso a la libertad, a la privacidad y demás derechos fundamentales.

El presente Plan, de acuerdo con lo establecido en la Estrategia Nacional de Ciberseguridad, tiene como **objetivo principal:**

> ***Potenciar las capacidades del Ministerio del Interior para detectar, prevenir, proteger, responder y perseguir la cibercriminalidad, de modo que permita la convergencia entre los ámbitos cibernético y físico, generando un impulso operativo y técnico eficaz que garantice la protección de los derechos y libertades y la seguridad ciudadana.***

Este objetivo principal se llevará a cabo a través del logro de los siguientes **objetivos específicos**:

- **Objetivo I**: promover la cultura de prevención de la cibercriminalidad entre la ciudadanía y la empresa.
- **Objetivo II:** impulsar la formación y la especialización de los miembros de las FCSE en materia de ciberseguridad y cibercriminalidad.
- **Objetivo III:** proteger los sistemas de información y telecomunicaciones utilizados por el Ministerio del Interior.
- **Objetivo IV:** incrementar y mejorar el uso y disposición de las herramientas tecnológicas e implementar I+D+i.
- **Objetivo V:** gestionar adecuadamente la información disponible en el ciberespacio.
- **Objetivo VI:** promover un marco legal e institucional que dé solución a los desafíos que surjan relacionados con la ciberseguridad y la cibercriminalidad.

- **Objetivo VII:** impulsar la coordinación a nivel nacional e internacional y favorecer la colaboración entre el sector público y privado.

7. EJES ESTRATÉGICOS Y LÍNEAS DE ACCIÓN

Los **ejes estratégicos** y las **líneas de acción** para la consecución del **objetivo general** y los **objetivos específicos** del Plan, son los siguientes:

EJE ESTRATÉGICO I: CULTURA DE PREVENCIÓN DE LA CIBERCRIMINALIDAD

OBJETIVO: ***fomentar el conocimiento y la información entre los ciudadanos y el sector empresarial para incrementar la prevención y la autoprotección en el uso del ciberespacio.***

Este eje estratégico responde al Objetivo Específico I del Plan.

- **LÍNEA DE ACCIÓN 1.1: elaborar un Plan Permanente de Divulgación para la Prevención contra la Cibercriminalidad (PPDPC).**
- **Resultados esperados:** diseñar y poner en marcha un mecanismo integral de difusión de contenidos de interés en materia de ciberseguridad focalizado en la prevención de la cibercriminalidad, identificando destinatarios y herramientas de elaboración y difusión de contenido de calidad, con la colaboración de los CSIRT nacionales de referencia.

- **LÍNEA DE ACCIÓN 1.2: promover el desarrollo de campañas específicas de información y divulgación sobre determinadas tipologías de delitos cometidos a través de la red.**
- **Resultados esperados:** diseñar y poner en marcha, con el apoyo de lo avanzado en el desarrollo del PPDPC, campañas específicas de difusión de contenidos acerca de aquellas modalidades delictivas que presentan una mayor incidencia en un marco temporal determinado.

- **LÍNEA DE ACCIÓN 1.3: impulsar campañas de sensibilización y actuación sobre la prevención de la cibercriminalidad en empresas, en especial PYMES y MICROPYMES.**
- **Resultados esperados:** llevar a cabo, con el apoyo de lo avanzado en el desarrollo del PPDPC, acciones que permitan identificar inquietudes, amenazas y problemática actual presente en el sector empresarial, aportando las medidas más eficaces para la prevención y mitigación de los delitos con mayor incidencia en este ámbito.

- **LÍNEA DE ACCIÓN 1.4: renovar y actualizar los planes dirigidos a concienciar acerca de los riesgos que presenta el uso del ciberespacio en los centros educativos, en centros sociales (mayores, personas sin recursos, etc.) y en otros colectivos vulnerables cibernéticamente que se detecten.**
- **Resultados esperados:** adecuar a la actual realidad delincuencial los planes específicos de la Secretaría de Estado de Seguridad u otras herramientas semejantes (tales como el Plan Director para la Convivencia y Mejora de la Seguridad en los Centros Educativos y sus Entornos y el Plan Mayor Seguridad, etc.). De tal manera que la ciberseguridad se perciba como un elemento esencial a tener en cuenta por los ciudadanos.

EJE ESTRATÉGICO II: POTENCIACIÓN DE CAPACIDADES

OBJETIVO*: **incrementar las capacidades operativas y técnicas de las unidades policiales y las competencias y habilidades de sus integrantes***.

Este eje estratégico responde a los Objetivos Específicos II, III y IV del Plan.

- **LÍNEA DE ACCIÓN 2.1: diseñar e implementar en las FCSE un sistema transversal de enseñanza en materia de ciberseguridad y cibercriminalidad.**
- **Resultados esperados:** elaborar y ejecutar acciones formativas de carácter generalista en materia de ciberseguridad y cibercriminalidad en todos los ámbitos formativos de las FCSE, estableciendo vínculos con otras iniciativas formativas de la Administración.

- **LÍNEA DE ACCIÓN 2.2: incrementar la formación especializada para los integrantes de las unidades tecnológicas de las FCSE.**
- **Resultados esperados:** poner en marcha un conjunto de acciones formativas dirigidas a disponer de funcionarios con un elevado conocimiento técnico en materias de ciberseguridad y cibercriminalidad, garantizando la especialización en técnicas delictivas con mayor incidencia y velando por la continua actualización de los funcionarios.

- **LÍNEA DE ACCIÓN 2.3: favorecer la captación y/o retención del talento en las unidades tecnológicas de las FCSE.**
- **Resultados esperados:** identificar y subsanar aquellas deficiencias, bien sean estructurales o coyunturales, que impidan disponer de profesionales con las habilidades necesarias.

- **LÍNEA DE ACCIÓN 2.4: impulsar el empleo de herramientas tecnológicas que faciliten la actividad operativa de los investigadores y el avance en I+D+i en el Ministerio del Interior.**
- **Resultados esperados:** identificar, evaluar y adquirir las herramientas más adecuadas que permitan a los funcionarios especializados en tareas operativas o de I+D+i disponer de los recursos técnicos necesarios para desarrollar sus funciones.

- **LÍNEA DE ACCIÓN 2.5: potenciar las actuaciones en el ámbito de la informática forense.**
- **Resultados esperados:** garantizar que las FCSE dispongan de medios y capacidades adecuadas en materia de análisis y conservación de evidencias digitales, reforzando y potenciando aquellos aspectos necesarios para disponer de laboratorios forenses eficaces capaces de atender la demanda de dictámenes relacionadas con el uso de las TIC en actividades criminales.

- **LÍNEA DE ACCIÓN 2.6: potenciar los sistemas de alerta temprana de amenazas y su correcta valoración.**
- **Resultados esperados:** potenciar la cibervigilancia y la monitorización de amenazas en el ciberespacio, así como fomentar la ciberresiliencia en activos estratégicos.

- **LÍNEA DE ACCIÓN 2.7: potenciar la seguridad de los sistemas de información del Ministerio del Interior.**
- **Resultados esperados:** reforzar los mecanismos y garantizar las inversiones que permitan el cumplimiento de las políticas de seguridad de la información, en especial velando por el cumplimiento del Esquema Nacional de Seguridad, el Esquema Nacional de Interoperabilidad y la normativa de protección de información clasificada.

- **LÍNEA DE ACCIÓN 2.8: reducir la "cifra negra u oculta" sobre la cibercriminalidad mediante el establecimiento de un marco favorable para las comunicaciones y denuncias de los usuarios.**
- **Resultados esperados:** poner en práctica iniciativas que permitan conocer la incidencia delictiva real de la cibercriminalidad, fomentando canales ágiles de comunicación y denuncia con las FCSE e identificando aquellas deficiencias de carácter técnico o legal que impiden avanzar en este sentido.

- **LÍNEA DE ACCIÓN 2.9: optimizar el uso de los recursos tecnológicos existentes en las FCSE.**
- **Resultados esperados:** garantizar el uso eficiente y compartido de los recursos técnicos disponibles del Ministerio Interior por todos sus organismos con competencia en ciberseguridad, evitando duplicidades y creando sinergias para su correcta utilización.

- **LÍNEA DE ACCIÓN 2.10: potenciar las capacidades de las unidades periféricas de las FCSE en la lucha contra la cibercriminalidad.**
- **Resultados esperados:** incrementar las capacidades de las unidades periféricas de las FCSE, de modo que aquellas investigaciones que requieran una menor complejidad puedan ser atendidas eficientemente.

EJE ESTRATÉGICO III: GENERACIÓN DE CIBERINTELIGENCIA

OBJETIVO: ***recoger, elaborar, tratar, analizar y difundir información para generar inteligencia en la lucha contra la cibercriminalidad.***

Este eje estratégico responde al Objetivo Específico V del Plan.

- **LÍNEA DE ACCIÓN 3.1: impulsar la captación de informaciones de interés operativo en materia de cibercriminalidad para su incorporación a la estructura de inteligencia.**
- **Resultados esperados:** identificar y explotar fuentes de información de interés en la materia mediante la implantación o refuerzo de canales con la ciudadanía, así como mediante la colaboración público-privada.

- **LÍNEA DE ACCIÓN 3.2: identificar y explotar fuentes de información cualificada, en especial con técnicos especializados e investigadores.**
- **Resultados esperados:** detectar y fomentar la colaboración de especialistas e investigadores en ciberseguridad con las FCSE, de modo que permita disponer de conocimientos técnicos avanzados en materia de vulnerabilidades, tácticas, técnicas y procedimientos asociados a la cibercriminalidad.

- **LÍNEA DE ACCIÓN 3.3: fomentar sinergias e impulsar el uso adecuado de los mecanismos existentes que permitan compartir la inteligencia en la lucha contra la cibercriminalidad entre las FCSE.**
- **Resultados esperados:** llevar a cabo acciones que permitan fijar conceptos, criterios, procedimientos y mecanismos que permitan al Ministerio del Interior

disponer de un modelo avanzado de ciberinteligencia en coordinación con otros cuerpos policiales y los CSIRT.

- **LÍNEA DE ACCIÓN 3.4: potenciar e impulsar el intercambio de inteligencia sobre la lucha contra la cibercriminalidad entre agencias policiales internacionales.**
- **Resultados esperados:** reforzar la cooperación con agencias internacionales de cara a fomentar el intercambio de ciberinteligencia, a través de los mecanismos existentes, así como explorando nuevas posibilidades que maximicen esta línea de acción. Haciendo partícipes a otras policías de las informaciones que afecten a su territorio de actuación.

- **LÍNEA DE ACCIÓN 3.5: reforzar las capacidades actuales de obtención, tratamiento y análisis operativo de información en las FCSE.**
- **Resultados esperados:** evaluar las herramientas y capacidades disponibles, implantando aquellas que permitan una mejor gestión del ciclo de la inteligencia de las FCSE, en especial en aquello referente al tratamiento y análisis de inteligencia operativa**.**

- **LÍNEA DE ACCIÓN 3.6: incrementar las capacidades actuales de obtención, tratamiento y análisis estratégico de información en el Ministerio del Interior.**
- **Resultados esperados:** evaluar las herramientas y capacidades disponibles, implantando aquellas que permitan un mejor tratamiento y análisis de la inteligencia estratégica como elemento fundamental en la prevención y anticipación de amenazas, con especial atención al Sistema Estadístico de Criminalidad (SEC).
- **LÍNEA DE ACCIÓN 3.7: potenciar las actuaciones de unidades especializadas en materia de ciberinteligencia.**
- **Resultados esperados:** evaluar, y en su caso implementar, estructuras organizativas en los organismos dependientes del Ministerio del Interior cuyo cometido sea la obtención y el tratamiento de información disponible en el ciberespacio, de modo que la prevención y anticipación sea el eje principal de actuación en materia de ciberseguridad y lucha contra la cibercriminalidad.

EJE ESTRATÉGICO IV: COORDINACIÓN NACIONAL Y COOPERACIÓN INTERNACIONAL

OBJETIVO*: impulsar la coordinación nacional y la cooperación internacional en la lucha contra la cibercriminalidad.*

Este eje estratégico responde al Objetivo Específico VII del Plan.

- **LÍNEA DE ACCIÓN 4.1: consolidar la presencia del Ministerio del Interior en el Sistema Nacional de Ciberseguridad.**
- **Resultados esperados:** fortalecer la presencia activa del Ministerio del Interior en el Sistema Nacional de Ciberseguridad como departamento ministerial presente en todos los estadios del ciclo de la ciberseguridad.
- **LÍNEA DE ACCIÓN 4.2: impulsar y fomentar la coordinación entre las FCS en la lucha contra la cibercriminalidad.**
- **Resultados esperados:** definir mecanismos de trabajo que logren una adecuada coordinación técnica y operativa de las FCS, potenciando capacidades de organismos coordinadores.
- **LÍNEA DE ACCIÓN 4.3: impulsar la actuación coordinada del Ministerio del Interior con el resto de las administraciones públicas en ciberseguridad, en la lucha contra la cibercriminalidad y la desinformación.**
- **Resultados esperados:** coordinarse de forma óptima con organismos públicos con competencias en estas materias, en el marco general establecido por la Estrategia de Seguridad Nacional y la Estrategia Nacional de Ciberseguridad, de forma especial con los CSIRT nacionales de referencia.
- **LÍNEA DE ACCIÓN 4.4: potenciar la presencia del Ministerio del Interior en las organizaciones, conferencias y foros internacionales, en los que la cibercriminalidad forma parte sustancial de sus agendas de trabajo.**
- **Resultados esperados:** participar en las reuniones, grupos de trabajo y foros internacionales cuya principal finalidad sea combatir la cibercriminalidad y asegurar la homogeneización de su regulación.
- **LÍNEA DE ACCIÓN 4.5: impulsar la participación de las FCSE en los organismos supranacionales de lucha contra la cibercriminalidad.**
- **Resultados esperados:** coordinar adecuadamente la presencia de los organismos dependiente del Ministerio del Interior con competencia en ciberseguridad y lucha contra la cibercriminalidad tanto a nivel comunitario como internacional.

- **LÍNEA DE ACCIÓN 4.6: promover el intercambio de metodologías y buenas prácticas entre agencias policiales de distintos países.**

  Resultados esperados: reforzar los lazos con otros países mediante la firma de acuerdos de colaboración que permitan compartir buenas prácticas y modelos policiales de cara a afrontar la cibercriminalidad.

- **LÍNEA DE ACCIÓN 4.7: impulsar los mecanismos de colaboración entre las autoridades judiciales y el Ministerio del Interior.**
- **Resultados esperados:** potenciar la colaboración con las autoridades judiciales, de modo que se logre la mejora del marco general en el que se desarrollan las investigaciones sobre cibercriminalidad, así como poner en marcha acciones de colaboración en materia formativa para los miembros de las FCSE.
- **LÍNEA DE ACCIÓN 4.8: impulsar los mecanismos de colaboración entre el Ministerio Fiscal y el Ministerio del Interior.**
- **Resultados esperados:** incrementar el marco de colaboración en el ámbito de las investigaciones en la lucha contra la cibercriminalidad y potenciar las acciones formativas dirigidas a las FCSE con la Fiscalía General del Estado, y en especial con la Fiscalía especializada en materia de criminalidad informática. Asimismo se debe potenciar el traslado de información, la colaboración y apoyo mutuo en los aspectos técnicos y jurídicos relacionados con las investigaciones en curso.
- **LÍNEA DE ACCIÓN 4.9: fomentar relaciones con el Consejo General de la Abogacía Española.**
- **Resultados esperados:** impulsar la colaboración del Ministerio del Interior con el Consejo General de la Abogacía española, de cara a poner en práctica acciones formativas, de análisis o de otra índole en materia de lucha contra la cibercriminalidad.
- **LÍNEA DE ACCIÓN 4.10: establecer procedimientos que permitan la coordinación técnica de las investigaciones que afecten a incidentes sufridos por operadores de servicios esenciales.**
- **Resultados esperados:** desarrollar en coordinación con Autoridades Judiciales, Ministerio Fiscal, las unidades de Policía Judicial, las autoridades sectoriales competentes y los CSIRT, los mecanismos de coordinación en materia de incidentes de ciberseguridad de gran alcance notificados por operadores de servicios esenciales a la autoridad competente, conforme lo establecido en el

Real Decreto-ley 12/2018, el Real Decreto 43/2021 y la Guía Nacional de Notificación y Gestión de Ciberincidentes.

- **LÍNEA DE ACCIÓN 4.11: desarrollar un entorno digital apropiado para el intercambio de comunicaciones entre la Administración de Justicia y los servicios policiales.**
- **Resultados esperados:** identificar y subsanar las deficiencias en materia de mecanismos de comunicación de las unidades policiales con órganos dependientes de la Administración de Justicia, en especial agilizando el flujo de atestados, oficios u otras comunicaciones, de forma segura. Para los equipos que contengan cifra se tendrá en cuenta lo establecido por el Centro Criptológico Nacional (CCN).

EJE ESTRATÉGICO V: CONTRIBUIR A LA DISPONIBILIDAD DE UN MARCO NORMATIVO ADECUADO

OBJETIVO: ***impulsar la actualización de la legislación, mediante el traslado de las oportunas propuestas que favorezcan la adaptación o creación de instrumentos jurídicos, administrativos, penales y procesales, en función de la demanda que se origine en la lucha contra la cibercriminalidad.***

Este eje estratégico responde al Objetivo Específico VI del Plan.

- **LÍNEA DE ACCIÓN 5.1: facilitar la actualización del marco jurídico nacional en el ámbito de la ciberseguridad y la cibercriminalidad.**
- **Resultados esperados:** contribuir activamente a que el legislador disponga de información acerca de la realidad y evolución de la cibercriminalidad de cada momento, evaluando la tipificación de nuevas conductas delictivas o eliminando otras de cara a adaptar la legislación a las TIC derivadas de estas.
- **LÍNEA DE ACCIÓN 5.2: impulsar la adecuación de la legislación a las necesidades actuales en informática forense y evidencias judiciales.**
- **Resultados esperados:** impulsar iniciativas, tanto a nivel nacional como europeo, que permitan avanzar en materia de evidencias electrónicas (*e-evidence*), así como en la estandarización de productos de *software* comerciales y procedimientos apoyados en éstos para dar seguridad jurídica a la actuación policial. Estas acciones han de realizarse, en todo caso, en las condiciones y con los requisitos necesarios para garantizar su plena validez y eficacia como medio de prueba en el proceso penal.
- **LÍNEA DE ACCIÓN 5.3: promover la armonización legislativa internacional en la lucha contra los paraísos cibercriminales.**

- **Resultados esperados:** impulsar acciones que promuevan un marco normativo internacional que impida la existencia de territorios en los que la cibercriminalidad quede impune.

- **LÍNEA DE ACCIÓN 5.4: poner en marcha instrumentos legales para garantizar la ciberseguridad de los operadores críticos y los operadores de servicios esenciales.**

- **Resultados esperados:** desarrollar, en el marco de la implantación de la Directiva 1148/2016, normas u otro tipo de herramientas que permitan avanzar en la protección de los servicios esenciales, velando en especial por la puesta en marcha de esquemas de certificación y mecanismos de notificación de incidentes.

- **LÍNEA DE ACCIÓN 5.5: promover un marco jurídico que regule la figura de operador de seguridad en el ámbito de la ciberseguridad.**

- **Resultados esperados:** impulsar la regulación jurídica de la figura profesional de operador de seguridad en sus diferentes modalidades, de modo que se garantice la disposición de perfiles laborales cualificados en determinados ámbitos sectoriales, así como su correspondiente habilitación por el Ministerio del Interior.

- **LÍNEA DE ACCIÓN 5.6: avanzar en el marco normativo de protección a las víctimas de los ciberdelitos.**

- **Resultados esperados:** adecuar el marco normativo de asistencia, protección y reparación a las víctimas de ciberdelitos a la nueva realidad delincuencial, especialmente en acciones cometidas a gran escala con un número masivo de víctimas localizadas en varios países.

- **LÍNEA DE ACCIÓN 5.7: reforzar la colaboración nacional e internacional para la correcta actualización y normalización del marco jurídico que permita responder con eficacia a la cibercriminalidad.**

- **Resultados esperados:** velar por una correcta armonización normativa, participando en iniciativas o foros que promuevan la normalización internacional.

- **LÍNEA DE ACCIÓN 5.8: adecuar la normativa para el control de los criptoactivos en actividades criminales.**

- **Resultados esperados:** identificar y poner en práctica mecanismos que permitan a las FCS disponer de un mayor control y seguimiento sobre posibles

conductas delictivas asociadas a nuevas modalidades de pago basadas en criptografía, impulsando mecanismos y normativas que regulen la incautación, decomiso y conversión de criptoactivos.

- **LÍNEA DE ACCIÓN 5.9: contribuir a la adaptación de la Directiva 1148/2016 al ordenamiento jurídico español, así como a las futuras modificaciones que se desarrollen.**
- **Resultados esperados:** garantizar la correcta puesta en funcionamiento del Real Decreto 43/2021, así como participar en la futura transposición de la Directiva NIS 2.0.
- **LÍNEA DE ACCIÓN 5.10: actualizar y adecuar la normativa sobre protección de infraestructuras críticas, al objeto de garantizar la integralidad de la seguridad.**
- **Resultados esperados:** actualización y adecuación de la Ley 8/2011 y el Real Decreto-ley 704/2011 de cara a disponer de una normativa actualizada que permita incrementar la protección de los activos lógicos implicados en la protección de infraestructuras críticas.
- **LÍNEA DE ACCIÓN 5.11: potenciar la figura del agente encubierto informático en las FCS.**
- **Resultados esperados:** desarrollar herramientas normativas, procedimientos y mecanismos de trabajo que permitan agilizar la puesta en marcha y ejercicio de esta figura esencial en las investigaciones en el ciberespacio.

EJE ESTRATÉGICO VI: COLABORACIÓN PÚBLICO-PRIVADA

OBJETIVO: ***potenciar en el ámbito de la ciberseguridad y la cibercriminalidad la colaboración público-privada.***

Este eje estratégico responde al Objetivo Específico VII del Plan.

- **LÍNEA DE ACCIÓN 6.1: impulsar la colaboración con actores relevantes en el ámbito de la industria de la ciberseguridad.**
- **Resultados esperados:** fortalecer el contacto del Ministerio del Interior con la industria del sector mediante la presencia en el Foro Nacional de Ciberseguridad, así como promover modelos de colaboración y cooperación sectoriales de cara a prevenir y responder ante la cibercriminalidad.
- **LÍNEA DE ACCIÓN 6.2: impulsar la colaboración con universidades, escuelas y otros centros de formación e investigación de interés.**

- **Resultados esperados:** definir modelos de colaboración con universidades, escuelas y otros centros de formación e investigación de interés en materia de cibercriminalidad.

- **LÍNEA DE ACCIÓN 6.3: fomentar la confianza con el sector privado.**
- **Resultados esperados:** definir modelos de colaboración público-privada, forma jurídica y nivel o niveles de relaciones, canales de comunicación, e instrumentos que garanticen la continuidad y eficacia de las colaboraciones.

- **LÍNEA DE ACCIÓN 6.4: potenciar la colaboración en materia de ciberseguridad con los operadores críticos y los operadores de servicios esenciales.**
- **Resultados esperados:** reforzar el modelo de colaboración entre el Ministerio del Interior y los operadores críticos y operadores de servicios esenciales con la finalidad de generar sinergias que potencien la resiliencia del modelo del Sistema de Protección de las Infraestructuras Críticas en España.

- **LÍNEA DE ACCIÓN 6.5: incrementar los mecanismos de colaboración de las FCS con las distintas empresas y departamentos de seguridad privada en la lucha contra la cibercriminalidad.**
- **Resultados esperados:** ampliar y profundizar en el contacto con operadores de seguridad privada, de modo que se potencien foros u otros canales de intercambio de información que incrementen la implicación de la seguridad privada en la lucha contra la cibercriminalidad.

- **LÍNEA DE ACCIÓN 6.6: fomentar la colaboración con los proveedores de servicios digitales y prestadores de servicios de la sociedad de la información y comercio electrónico.**
- **Resultados esperados:** desarrollar mecanismos de trabajo específicos con estas entidades, de modo que los mismos permitan agilizar la obtención de datos, la colaboración y la puesta en marcha de acciones conjuntas en el marco de la lucha contra la cibercriminalidad.

8. GOBERNANZA DEL PLAN

8.1 Dirección y coordinación del Plan

La persona titular de la Secretaría de Estado de Seguridad, bajo la superior dirección del Ministro del Interior, es el responsable de la dirección, impulso y seguimiento de las líneas de acción y las actuaciones previstas en este Plan.

La coordinación de las actuaciones previstas en el presente Plan será ejercida por el Gabinete de Coordinación y Estudios, a través de la **Oficina de Coordinación de Ciberseguridad** (OCC) –en colaboración con el CITCO en el ámbito de sus competencias–, que realizará la asignación de las responsabilidades del cumplimiento de este Plan y el seguimiento de su ejecución.

8.2 Comisión de seguimiento

Para el seguimiento estratégico, la evaluación periódica del desarrollo y ejecución de las actuaciones previstas en el Plan, y su adecuación al logro de los objetivos marcados, existirá una **Comisión de Seguimiento del Plan**, presidida por la persona titular de la Secretaría de Estado de Seguridad, que se reunirá al menos una vez al semestre, y de la que formarán parte los Directores del Gabinete de Coordinación y Estudios y del CITCO, el Subdirector General de la SGSICS, los Jefes de la OCC y del CNPIC; y dos miembros designados, respectivamente, por la Policía Nacional y la Guardia Civil.

Asimismo, podrán asistir dos representantes designados, respectivamente, por el Consejo General del Poder Judicial y por la Fiscalía General del Estado, un responsable por cada Cuerpo de Policía autonómico, y un representante por cada una de las organizaciones o entes públicos o privados que se determinen.

8.3 Mesa permanente de coordinación

A los fines referidos de coordinación operativa y de inteligencia disponible, y de seguimiento de la ejecución de los ejes estratégicos y sus respectivas líneas de acción, se constituirá una **Mesa Permanente de Coordinación**, que se reunirá al menos una vez al trimestre o a iniciativa del Director del Gabinete de Coordinación y Estudios, en la que participarán los siguientes organismos: Gabinete de Coordinación y Estudios, a través de la OCC y del CNPIC, CITCO, SGSICS y FCSE, así como en su caso representantes de las organizaciones o entes públicos o privados cuando se determine.

8.4 Planes de acción operativos

En el plazo máximo de cuatro meses a partir de la publicación de este Plan Estratégico, Policía Nacional, Guardia Civil, CITCO, SGSICS, CNPIC, OCC, presentarán a la Secretaría de Estado de Seguridad, para su aprobación, una propuesta de su correspondiente **Plan de Acción Operativo**, teniendo en cuenta las **Líneas de Acción** contenidas en los diferentes **Ejes Estratégicos de este Plan** que le sean de aplicación, dejando el desarrollo posterior a cada organismo implicado.

Cada organismo priorizará las medidas previstas contenidas en sus respectivas propuestas, con indicación de:

- Su prioridad justificada.

- Objetivos a alcanzar y resultados esperados.
- Modelo de gobernanza.
- Recursos (humanos, económicos y de infraestructura) empleados y necesarios.
- Plazo de ejecución.
- Indicadores y métricas de cumplimiento.

8.5 Informe de desarrollo y ejecución del Plan

Con carácter anual, el Gabinete de Coordinación y Estudios, a través de la OCC, y en colaboración con el CITCO, presentará al titular de la Secretaría de Estado de Seguridad un informe del cumplimiento de las Líneas de Acción consignadas en el presente Plan.

9. RECURSOS HUMANOS Y ECONÓMICOS NECESARIOS PARA LA EJECUCIÓN DEL PLAN.

Las medidas y actuaciones contempladas en el presente Plan contarán en el ámbito de la Secretaría de Estado de Seguridad con una dotación económica de **1.000.000 de euros** para el año presupuestario de 2021.

Cada uno de los organismos referenciados en el punto 8.4 elaborará una relación priorizada de inversiones y adquisición de las capacidades necesarias para ejecutar durante la vigencia de este Plan, así como un estudio de las necesidades de recursos humanos que remitirán a la Secretaría de Estado de Seguridad en el plazo de cuatro meses desde la publicación del Plan.

La SGSICS, teniendo en cuenta las propuestas de las Direcciones Generales de la Policía Nacional y de la Guardia Civil, planificará, coordinará y, en su caso, gestionará las inversiones en sistemas de información y comunicaciones. De igual forma será la encargada de proponer a la persona titular de la Secretaría de Estado de Seguridad los planes y programas que afecten a los sistemas de información y comunicaciones en el ámbito de la seguridad, así como su coordinación, supervisión de su ejecución, evaluación y análisis de sus costes, promoviendo 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 FCSE.

10. VIGENCIA Y ACTUALIZACIÓN DEL PLAN

El Plan Estratégico contra la Cibercriminalidad será aprobado mediante la oportuna Instrucción del Secretario de Estado de Seguridad y tendrá un periodo de vigencia de cuatro años desde su aprobación, sin perjuicio de que las circunstancias aconsejen

anticipar su revisión, correspondiendo al Ministerio del Interior la coordinación de estas actuaciones en el marco de la Estrategia Nacional de Ciberseguridad.

ANEXO I. DEFINICIÓN DE CONCEPTOS

Amenaza híbrida:

Acciones coordinadas y sincronizadas dirigidas a atacar de manera deliberada las vulnerabilidades sistémicas de los estados democráticos y las instituciones, a través de una amplia gama de medios, tales como acciones militares tradicionales, ciberataques, operaciones de manipulación de la información, o elementos de presión económica.

Ciberataque:

Acción producida en el ciberespacio que compromete la disponibilidad, integridad y confidencialidad de la información de una organización mediante el acceso no autorizado, la modificación, la degradación o la destrucción de las redes y los sistemas de información o las infraestructuras que los soportan.

Cibercriminalidad:

La ENCS-2019, da la definición de "*El término cibercriminalidad hace referencia al conjunto de actividades ilícitas cometidas en el ciberespacio que tienen por objeto los elementos, sistemas informáticos o cualesquiera otros bienes jurídicos, siempre que en su planificación, desarrollo y ejecución resulte determinante la utilización de herramientas tecnológicas; en función de la naturaleza del hecho punible en sí, de la autoría, de su motivación, o de los daños infligidos, se podrá hablar así de ciberterrorismo, de ciberdelito, o en su caso, de hacktivismo*".

Continúa esa Estrategia indicando que *"son tres los ámbitos en los que se desenvuelve la lucha contra la cibercriminalidad: el ciberespacio como objetivo directo de los hechos delictivos, o de la amenaza; el ciberespacio como medio clave para su comisión; y el ciberespacio como medio u objeto directo de investigación de cualquier tipo de hecho ilícito".*

Ciberdelito:

En este sentido, se entienden todos aquellos delitos que para su comisión el autor o autores se valen del empleo de las TIC.

Ciberseguridad:

Conjunto de herramientas, políticas, conceptos de seguridad, medidas de seguridad, directrices, enfoques de gestión de riesgos, acciones de formación, buenas prácticas, aseguramiento y tecnologías que se pueden utilizar para proteger el entorno cibernético, la organización y los activos de los usuarios. Los objetivos generales de seguridad comprenden la disponibilidad, integridad, que puede incluir autenticidad y no repudio, y la confidencialidad. (ITU-T Recommendation Rec. ITU-T X.1205; 2008).

Ciberterrorismo:

Se encuadra como un tipo cualificado de ciberdelito atendiendo al Código Penal, que referencia estos como; "*Delitos informáticos previstos en los art. 197 bis y ter y 264 a 264 quater de la Ley Orgánica 10/1995 del Código Penal, cuando dichos delitos se cometan con las finalidades previstas en el artículo 573.1 del mismo texto".*

Para definir aquellos conceptos que no figuran ya descritos en textos legales o normas y recomendaciones ampliamente aceptadas, es preciso tomar como referencia **la Guía Nacional de Notificación y Gestión de Ciberincidentes (GNNGC),** en su Anexo 5.

Cifra negra u oculta:

El número de delitos cometidos, pero desconocidos por la administración de justicia y las FCS al no ser objeto de denuncia, lo que impide su prevención y persecución, así como el auxilio a la víctima.

CSIRT:

Los equipos de respuesta a incidentes que analizan riesgos y supervisan incidentes a escala nacional, difunden alertas sobre ellos y aportan soluciones para mitigar sus efectos. El término CSIRT es el usado comúnmente en Europa en lugar del término protegido CERT (*Computer Emergency Response Team*), registrado en EE.UU.

Desinformación:

La Comunicación sobre la lucha contra la desinformación en línea, COM (2018) 236, de la Comisión Europea define la desinformación como la información verificablemente falsa o engañosa que se crea, presenta y divulga con fines lucrativos o para engañar deliberadamente a la población, y que puede causar un perjuicio público, e incluye en este perjuicio público las amenazas a los procesos democráticos y a bienes públicos tales como la salud, el medio ambiente o la seguridad, entre otros.

Conforme a la normativa actual española en materia penal, estas conductas no siempre son delictivas, tan solo algunas de sus manifestaciones, en consonancia con lo recogido en la Constitución Española en su artículo 20, que reconoce el derecho a comunicar o recibir información veraz por cualquier medio de difusión.

Identidad digital:

El conjunto de datos que permiten establecer la identidad de una persona física o jurídica, o de una persona física que representa a una persona jurídica mediante un proceso electrónico que posibilita su identificación y la integridad de los mismos en formato electrónico.

ANEXO II. MARCO NORMATIVO DE REFERENCIA

Normativa nacional

- **Constitución Española** de 1978.
- **Real Decreto de 14 de septiembre de 1882** por el que se aprueba la **Ley de Enjuiciamiento Criminal**. Modificado por la Ley Orgánica 13/2015, de 5 de octubre, de modificación de la Ley de Enjuiciamiento Criminal para el fortalecimiento de las garantías procesales y la regulación de las medidas de investigación tecnológica y la Ley 41/2015, de 5 de octubre, de modificación de la Ley de Enjuiciamiento Criminal para la agilización de la justicia penal y el fortalecimiento de las garantías procesales.
- **Ley Orgánica 6/1985**, de 1 de julio, del Poder Judicial.
- **Ley Orgánica 10/1995**, de 23 de noviembre, del Código Penal. Modificada por la Ley Orgánica 5/2010, de 22 de junio; Ley Orgánica 1/2015, de 30 de marzo; Ley Orgánica 2/2015, en materia de delitos de terrorismo y Ley Orgánica 1/2019, de 20 de febrero para transponer Directivas de la Unión Europea en los ámbitos financiero y de terrorismo, y abordar cuestiones de índole internacional.
- **Ley Orgánica 5/2000**, de 12 de enero, reguladora de la responsabilidad penal de los menores.
- **Ley Orgánica 3/2018**, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.
- **Ley 50/1981**, de 30 de diciembre, por la que se regula el Estatuto Orgánico del Ministerio Fiscal.
- **Ley 34/2002**, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico.
- **Ley 25/2007**, de 18 de octubre, de conservación de datos relativos a las comunicaciones electrónicas y a las redes públicas de comunicaciones.
- **Ley 5/2014**, de 4 de abril, de Seguridad Privada.
- **Ley 9/2014**, de 9 de mayo, General de Telecomunicaciones.
- **Ley 23/2014**, de 20 de noviembre, de reconocimiento mutuo de resoluciones penales en la Unión Europea.
- **Ley 4/2015**, de 27 de abril, del Estatuto de la víctima del delito.
- **Ley 36/2015**, de 28 de septiembre, de Seguridad Nacional.
- **Real Decreto-ley 12/2018**, de 7 de septiembre, de seguridad de las redes y sistemas de información.
- **Real Decreto 769/1987**, de 19 de junio, sobre regulación de la Policía Judicial.
- **Real Decreto 3/2010**, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica.
- **Real Decreto 4/2010,** de 8 de enero, por el que se regula el Esquema Nacional de Interoperabilidad en el ámbito de la Administración Electrónica.

- **Real Decreto 1008/2017**, de 1 de diciembre, por el que se aprueba la Estrategia de Seguridad Nacional 2017.
- **Real Decreto 734/2020**, de 4 de agosto, por el que se desarrolla la estructura orgánica básica del Ministerio del Interior.
- **Real Decreto 43/2021**, de 26 de enero, por el que se desarrolla el Real Decreto-ley 12/2018, de 7 de septiembre, de seguridad de las redes y sistemas de información.
- **Orden INT/28/2013**, de 18 de enero, por la que se desarrolla la estructura orgánica y funciones de los Servicios Centrales y Periféricos de la Dirección General de la Policía.
- **Orden PRE/422/2013**, de 15 de marzo, por la que se desarrolla la estructura orgánica de los Servicios Centrales de la Dirección General de la Guardia Civil.
- **Orden PCI/161/2019**, de 21 de febrero, Estrategia Nacional contra el Crimen Organizado y la Delincuencia Grave 2019-2023.
- **Orden PCI/179/2019**, de 22 de febrero, Estrategia Nacional Contra el Terrorismo 2019.
- **Orden PCI/487/2019**, de 26 de abril, por la que se publica la Estrategia Nacional de Ciberseguridad 2019, aprobada por el Consejo de Seguridad Nacional.
- **Orden PCI/489/2019**, de 26 de abril, por la que se publica la Estrategia de Seguridad Aeroespacial Nacional, aprobada por el Consejo de Seguridad Nacional.
- **Orden PCM/1030/2020**, de 30 de octubre, por la que se publica el Procedimiento de actuación contra la desinformación aprobado por el Consejo de Seguridad Nacional.

Normativa internacional

- **Convenio nº 108 del Consejo de Europa para la Protección de las Personas** con respecto al tratamiento automatizado de los datos de carácter personal (1981).
- **Convenio del Consejo de Europa sobre Ciberdelincuencia**, hecho en Budapest el 23 de noviembre de 2001, ratificado por España en el año 2010. Instrumento de Ratificación del Convenio publicado en el BOE de 17 de septiembre de 2010.
- **Protocolo adicional al Convenio sobre la Ciberdelincuencia**, relativo a la penalización de actos de índole racista o xenófoba cometidos por medio de sistemas informáticos, hecho en Estrasburgo el 28 de enero de 2003 y ratificado por España en el año 2014. Instrumento de ratificación del Convenio publicado en el BOE de 30 de enero de 2015.
- **Convenio del Consejo de Europa para la protección de los niños contra la explotación y el abuso infantil**, hecho en Lanzarote el 27 de octubre de 2007, ratificado por España en el año 2010. Instrumento de ratificación del Convenio publicado en el BOE de 12 de noviembre de 2010.

- **Protocolo Facultativo de la Convención de Derechos del Niño,** relativo a la venta de niños, la prostitución infantil y la utilización de niños en la pornografía, hecho en Nueva York el 25 de mayo de 2000, ratificado por España, el 5 de diciembre de 2001.
- **Directiva 95/46/ CE** del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos.
- **Directiva 2002/58/CE** del Parlamento Europeo y del Consejo, de 12 de julio de 2002, relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas.
- **Directiva 2008/919/JAI** del Consejo sobre prevención del terrorismo.
- **Directiva 2011/93/UE** del Parlamento y del Consejo, relativa a la lucha contra los abusos sexuales y la explotación sexual de los menores y la pornografía infantil.
- **Directiva 2013/40/UE** del Parlamento Europeo y del Consejo, de 12 de agosto de 2013, relativa a los ataques contra los sistemas de información.
- **Directiva (UE) 2016/1148** del Parlamento Europeo y del Consejo**,** de 6 de julio de 2016, relativa a las medidas destinadas a garantizar un elevado nivel común de seguridad de las redes y sistemas de información en la Unión.
- **Directiva (UE) 2018/843**, de 30 de mayo, relativa a la prevención de la utilización del sistema financiero para el blanqueo de capitales y la financiación del terrorismo.
- **Directiva (UE) 2019/713** de 17 de abril sobre fraude y falsificación de medios de pago distintos del efectivo (pendiente incorporación al ordenamiento jurídico nacional).
- **Reglamento (UE) 2016/679** del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos).
- **Directiva (UE) 2016/680** del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por parte de las autoridades competentes para fines de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales, y a la libre circulación de dichos datos y por la que se deroga la Decisión Marco 2008/977/JAI del Consejo.
- **Estrategia Europea de Ciberseguridad** del Consejo de la UE, de 20 noviembre de 2017.
- **Plan de Acción contra la Desinformación**, de 5 de diciembre de 2018 de la Comisión Europea.
- **Estrategia de la UE para una Unión de la Seguridad para el período 2020-2025** de la Comisión Europea, de 24 de julio de 2020.
- **Estrategia de Ciberseguridad Europea para el Decenio Digital** de la Comisión Europea, de 12 de diciembre de 2020.

PÁGINA INTENCIONADAMENTE EN BLANCO

PLAN ESTRATÉGICO CONTRA LA CIBERCRIMINALIDAD

GOBIERNO DE ESPAÑA
MINISTERIO DEL INTERIOR