ADENDA TC 33

AMPLIACIÓN

Plan Estratégico Contra la Cibercriminalidad

MARCO NORMATIVO

Con una **vigencia de 4 años** se **aprueba el Plan Estratégico contra la Cibercriminalidad** regulado en la **ISES 1/2021.**

La lucha contra la **cibercriminalidad supone uno de los pilares fundamentales en los que se sustenta el concepto y la dimensión de la ciberseguridad** y así lo recoge la **Estrategia Nacional de Ciberseguridad 2019 aprobada en la Orden PCI/487** que destaca como el segundo de sus objetivos generales alcanzar y proporcionar un uso seguro y fiable del ciberespacio frente a su uso ilícito o malicioso, al considerar la cibercriminalidad como un problema de seguridad ciudadana de primer orden por ser una de las amenazas más extendidas.

Respondiendo a ese objetivo general, la Estrategia Nacional de Ciberseguridad 2019 define la cibercriminalidad como el **conjunto de las actividades ilícitas cometidas en el ciberespacio que tienen por objeto los elementos, sistemas informáticos o cualesquiera otros bienes jurídicos, utilizando para ello herramientas tecnológicas. Y para hacer frente a la misma establece una serie de medidas específicas contempladas en su Línea de Acción 3: "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"**.

OBJETIVOS

El Plan valora las tendencias y los retos actuales que supone la cibercriminalidad, planteando 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.

LÍNEAS DE ACCIÓN

Para la consecución de estos objetivos el Plan contempla seis ejes estratégicos que, a su vez, se desglosan en **cuarenta y nueve líneas de acción**.

1. Eje I: CULTURA DE PREVENCIÓN DE LA CIBERCRIMINALIDAD, que responde al Objetivo I

   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.

   LÍNEA DE ACCIÓN 1.1: elaborar un Plan Permanente de Divulgación para la Prevención contra la Cibercriminalidad (PPDPC).

   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.

   LÍNEA DE ACCIÓN 1.3: impulsar campañas de sensibilización y actuación sobre la prevención de la cibercriminalidad en empresas, en especial PYMES y MICROPYMES.

   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.

2. Eje II: POTENCIACIÓN DE CAPACIDADES, que responde a los Objetivos II, III y IV

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

LÍNEA DE ACCIÓN 2.1: diseñar e implementar en las FCSE un sistema transversal de enseñanza en materia de ciberseguridad y cibercriminalidad

LÍNEA DE ACCIÓN 2.2: incrementar la formación especializada para los integrantes de las unidades tecnológicas de las FCSE.

LÍNEA DE ACCIÓN 2.3: favorecer la captación y/o retención del talento en las unidades tecnológicas de las FCSE.

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.

LÍNEA DE ACCIÓN 2.5: potenciar las actuaciones en el ámbito de la informática forense.

LÍNEA DE ACCIÓN 2.6: potenciar los sistemas de alerta temprana de amenazas y su correcta valoración.

LÍNEA DE ACCIÓN 2.7: potenciar la seguridad de los sistemas de información del Ministerio del Interior.

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.

LÍNEA DE ACCIÓN 2.9: optimizar el uso de los recursos tecnológicos existentes en las FCSE.

LÍNEA DE ACCIÓN 2.10: potenciar las capacidades de las unidades periféricas de las FCSE en la lucha contra la cibercriminalidad.

3. Eje III: GENERACIÓN DE CIBERINTELIGENCIA, que responde al Objetivo V

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

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.

LÍNEA DE ACCIÓN 3.2: identificar y explotar fuentes de información cualificada, en especial con técnicos especializados e investigadores.

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.

LÍNEA DE ACCIÓN 3.4: potenciar e impulsar el intercambio de inteligencia sobre la lucha contra la cibercriminalidad entre agencias policiales internacionales.

LÍNEA DE ACCIÓN 3.5: reforzar las capacidades actuales de obtención, tratamiento y análisis operativo de información en las FCSE.

LÍNEA DE ACCIÓN 3.6: incrementar las capacidades actuales de obtención, tratamiento y análisis estratégico de información en el Ministerio del Interior.

LÍNEA DE ACCIÓN 3.7: potenciar las actuaciones de unidades especializadas en materia de ciberinteligencia.

4. Eje IV: COORDINACIÓN NACIONAL Y COOPERACIÓN INTERNACIONAL, que responde al Objetivo VII

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

LÍNEA DE ACCIÓN 4.1: consolidar la presencia del Ministerio del Interior en el Sistema Nacional de Ciberseguridad.

LÍNEA DE ACCIÓN 4.2: impulsar y fomentar la coordinación entre las FCS en la lucha contra la cibercriminalidad.

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.

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.

LÍNEA DE ACCIÓN 4.5: impulsar la participación de las FCSE en los organismos supranacionales de lucha contra la cibercriminalidad.

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

LÍNEA DE ACCIÓN 4.7: impulsar los mecanismos de colaboración entre las autoridades judiciales y el Ministerio del Interior.

LÍNEA DE ACCIÓN 4.8: impulsar los mecanismos de colaboración entre el Ministerio Fiscal y el Ministerio del Interior.

LÍNEA DE ACCIÓN 4.9: fomentar relaciones con el Consejo General de la Abogacía Española.

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.

LÍNEA DE ACCIÓN 4.11: desarrollar un entorno digital apropiado para el intercambio de comunicaciones entre la Administración de Justicia y los servicios policiales.

5. Eje V: CONTRIBUIR A LA DISPONIBILIDAD DE UN MARCO NORMATIVO ADECUADO, que responde al Objetivo VI

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.

LÍNEA DE ACCIÓN 5.1: facilitar la actualización del marco jurídico nacional en el ámbito de la ciberseguridad y la cibercriminalidad.

LÍNEA DE ACCIÓN 5.2: impulsar la adecuación de la legislación a las necesidades actuales en informática forense y evidencias judiciales.

LÍNEA DE ACCIÓN 5.3: promover la armonización legislativa internacional en la lucha contra los paraísos cibercriminales.

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

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

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

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.

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

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.

LÍNEA DE ACCIÓN 5.10: actualizar y adecuar la normativa sobre protección de infraestructuras críticas, al objeto de garantizar la integralidad de la seguridad.

LÍNEA DE ACCIÓN 5.11: potenciar la figura del agente encubierto informático en las FCS.

6. Eje VI: COLABORACIÓN PÚBLICO-PRIVADA, que responde al Objetivo VII

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

LÍNEA DE ACCIÓN 6.1: impulsar la colaboración con actores relevantes en el ámbito de la industria de la ciberseguridad.

LÍNEA DE ACCIÓN 6.2: impulsar la colaboración con universidades, escuelas y otros centros de formación e investigación de interés.

LÍNEA DE ACCIÓN 6.3: fomentar la confianza con el sector privado.

LÍNEA DE ACCIÓN 6.4: potenciar la colaboración en materia de ciberseguridad con los operadores críticos y los operadores de servicios esenciales.

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.

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.

GOBERNANZA DEL PLAN

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 la **Dirección General 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.

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 el **titular de la Secretaría de Estado de Seguridad, que se reunirá al menos una vez al semestre, y de la que formarán parte el Director General del Gabinete de Coordinación y Estudios, el Director del CITCO, el Subdirector General de la Subdirección General de Sistemas de Información y Comunicaciones para la Seguridad, 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.**

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 General 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.**

DEFINICIÓN DE CONCEPTOS

El anexo I de Plan recoge los siguientes conceptos de interés:

- **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 Estrategia Nacional de Ciberseguridad de 2019 la define como el **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.

- **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.