República Argentina - Poder Ejecutivo Nacional
AÑO DE LA RECONSTRUCCIÓN DE LA NACIÓN ARGENTINA

Anexo

Número: IF-2025-04008168-APN-DCYAC#MSG

CIUDAD DE BUENOS AIRES
Lunes 13 de Enero de 2025

Referencia: ANEXO - PLAN FEDERAL DE PREVENCIÓN DE CIBERDELITOS Y GESTIÓN ESTRATÉGICA DE LA CIBERSEGURIDAD (2025 - 2027) - EX-2024-142626534- -APN-DCYAC#MSG

PLAN FEDERAL DE PREVENCIÓN DE CIBERDELITOS Y GESTIÓN ESTRATÉGICA DE LA CIBERSEGURIDAD (2025 - 2027)

Introducción

En esta era digital en la cual nos encontramos inmersos, el ciberespacio se consolidó como una infraestructura esencial para el desarrollo económico, social y político de las naciones. Desde la gestión de servicios públicos hasta la operación de infraestructuras críticas que pasan por la comunicación interpersonal y las transacciones comerciales, la tecnología y redes digitales son la columna vertebral de la vida moderna. Sin embargo, este avance tecnológico también trajo aparejado un aumento exponencial del ciberdelito y las amenazas cibernéticas.

Las amenazas en el ciberespacio son diversas y sofisticadas, abarcan desde ataques de *ransomware*, que paralizan sistemas críticos, hasta campañas de *phishing* que buscan robar información personal y financiera. Los actores detrás de estas amenazas varían desde ciberdelincuentes individuales y organizaciones criminales hasta actores estatales y grupos patrocinados por estados que buscan ventajas estratégicas y económicas. La naturaleza transnacional del cibercrimen complica aún más la respuesta y coordinación de esfuerzos, ya que los ataques pueden originarse desde cualquier lugar del mundo y causar un impacto global.

Uno de los mayores desafíos en materia de lucha contra la ciberdelincuencia y ciberseguridad es la rápida evolución de las técnicas, tácticas y procedimientos de los atacantes. Es por este motivo que las amenazas se vuelven cada vez más complejas y difíciles de detectar y los ataques son cada vez más dirigidos y específicos paraaprovechar vulnerabilidades tanto tecnológicas como humanas. Además, la proliferación de dispositivos conectados a Internet, conocidos como el Internet de las Cosas (IoT), amplió enormemente la superficie de ataque, ofreciendo nuevas oportunidades para los ciberdelincuentes.

A nivel global, los gobiernos, empresas y organizaciones internacionales se encuentran redoblando sus esfuerzos para fortalecer la ciberseguridad. En tal sentido, se encuentran desarrollando y actualizando marcos normativos,

fomentando la cooperación internacional y promoviendo la colaboración público-privada para crear un ciberespacio más seguro, tales como el Segundo Protocolo adicional al Convenio sobre la Ciberdelincuencia, relativo a la cooperación reforzada y la divulgación de pruebas electrónicas, o las negociaciones en curso para adoptar una nueva Convención de Naciones Unidad sobre Ciberdelincuencia. Iniciativas como el Reglamento General de Protección de Datos (GDPR) en la Unión Europea establecieron nuevos estándares para la protección de datos y la privacidad, mientras que organizaciones como la OTAN e INTERPOL se encuentran ampliando permanentemente sus capacidades para combatir el cibercrimen y proteger infraestructuras críticas.

La educación y la toma de conciencia también juegan un papel crucial en la lucha contra la ciberdelincuencia y la ciberseguridad. Las campañas de concientización pública y la formación continua de profesionales de TI son esenciales para mitigar el riesgo de ataques cibernéticos. Las empresas se encuentran invirtiendo en tecnologías avanzadas de ciberseguridad, como la inteligencia artificial y el machine learning, para detectar y responder a las amenazas en tiempo real.

Es por este y otros tantos motivos, que tanto la lucha contra el cibercrimen como el fortalecimiento de la ciberseguridad, deben constituirse como un asunto de Estado, debido al papel preponderante que las tecnologías de la información y comunicación tienen en el desarrollo de nuestras vidas y el complejo entramado de relaciones socioculturales que nos rodean.

En este contexto, el Plan Federal de Prevención de Ciberdelitos y Gestión Estratégica de la Ciberseguridad se presenta como una iniciativa estratégica fundamental para enfrentar los desafíos actuales y futuros en esos temas, garantizando la protección de los derechos y libertades individuales en el ciberespacio. Este plan busca coordinar esfuerzos a nivel federal, mejorar las capacidades de respuesta y prevención y fomentar una cultura de ciberseguridad entre todos los actores involucrados.

El éxito en la lucha contra el cibercrimen depende de la colaboración y el compromiso de múltiples partes interesadas, entre ellas, el sector público y privado, las instituciones académicas, la sociedad civil y los usuarios individuales. Sólo a través de un enfoque integral y coordinado se podrá construir un entorno digital seguro, confiable y resiliente capaz de soportar las crecientes amenazas del ciberespacio y proteger a la sociedad en su conjunto.

Estado de situación

En la actualidad, el Ministerio de Seguridad por intermedio de la Dirección de Ciberdelito y Asuntos Cibernéticos diseña y lleva adelante la coordinación estratégica de las fuerzas policiales y de seguridad en materia de lucha contra la ciberdelincuencia, quienes por medio de diversas áreas se abocan a las tareas de prevención, detección, investigación y asistencia en caso de ciberdelitos y delitos asistidos tecnológicamente y brindan soporte a los diferentes requerimientos judiciales y asistencia a las víctimas. Estas acciones se encuentran limitadas por diferentes razones, por cuanto para dar acabada respuesta a la situación planteada se identificaron múltiples aspectos que requieren un abordaje integral y prioritario, entre los que se encuentran:

1. **Reconocer el ciberdelito y el fortalecimiento de la ciberseguridad como asuntos de Estado**: para diseñar una estrategia integral de lucha contra la ciberdelincuencia resulta imperioso reconocer el impacto de este tipo de actividades criminales en nuestra sociedad y su incidencia en la seguridad nacional. Por tal motivo, su abordaje requiere una activa articulación de los tres (3) poderes del Estado (ejecutivo, legislativo y judicial), donde deben participar tanto el nivel central como la Ciudad Autónoma de Buenos Aires y las 23 jurisdicciones provinciales.

2. **Evaluar el grado de madurez en materia de lucha contra la ciberdelincuencia:** a fin de establecer un marco metodológico de lucha contra el ciberdelito que resulte eficaz y sustentable en el tiempo resulta necesario realizar una profunda evaluación sobre el estado en que se encuentra la infraestructura tecnológica, la capacitación del personal y los procedimientos internos vinculados con esta temática. A tal efecto, resultará necesario establecer una serie de indicadores y métricas de desempeño que nos permita medir la eficiencia del esfuerzo realizado, identificar oportunidades de mejora continua e implementar acciones de corrección de forma temprana.
3. **Fortalecer los recursos humanos y herramientas tecnológicas**: así como los delitos asistidos tecnológicamente mutan y se complejizan a lo largo del tiempo, el Estado Nacional debe arbitrar los medios necesarios para promover el fortalecimiento de las capacidades en materia de investigación y lucha contra el ciberdelito respecto de los recursos humanos empeñados en estas complejas actividades que fomentan, sobre todo, el uso de herramientas tecnológicas altamente especializadas para la obtención y análisis de evidencias almacenadas electrónicamente, como así también la investigación, desarrollo e innovación.
4. **Fomentar la especialización de los equipos de respuesta**: debido al amplio espectro que abarca la prevención e investigación del ciberdelito, resulta necesario contar con equipos de respuesta altamente especializados en diferentes temáticas sobre la base de una sólida formación técnica profesional y la adopción de metodologías alineadas con reglas de buena práctica y estándares internacionales. Del mismo modo, para apuntalar las investigaciones y evacuar los diferentes requerimientos judiciales, se deberá contar con equipamiento de vanguardia tanto para el análisis forense digital como para la correlación de eventos e integración de diferentes fuentes de datos.
5. **Adecuar y actualizar la normativa vigente**: el ciberdelito como fenómeno criminal evoluciona permanentemente, esta situación propicia una profunda evaluación sobre la adecuación y actualización del marco normativo, como así también considerar la incorporación de herramientas especiales de investigación, prevención y lucha contra delitos complejos en el marco de esta temática altamente especializada.
6. **Promover una conducta preventiva y proactiva**: en este aspecto, resulta crucial la implementación de campañas de comunicación y sensibilización que permitan a la población en general mantenerse alerta sobre los riesgos cibernéticos y prácticas seguras en línea a fin de reducir la incidencia de este tipo de delitos en la sociedad. Del mismo modo, los integrantes de las fuerzas federales policiales y de seguridad deberán contar con las capacidades necesarias para la detección temprana y prevención de delitos ciberasistidos.
7. **Incrementar la cooperación asimétrica**: la lucha contra la ciberdelincuencia requiere que todas las partes interesadas colaboren activamente, es en este sentido que la cooperación entre el Estado Nacional, la ciudadanía en general, la academia, las organizaciones de la sociedad civil y las empresas privadas toma un rol preponderante. A tal efecto, se desarrollaron diferentes actividades mediante la conformación de mesas de trabajo especializadas en diferentes temáticas.
8. **Ampliar y profundizar la cooperación internacional**: debido a la supraterritorialidad que caracteriza las actividades criminales en el ciberespacio, la cooperación internacional toma un rol preponderante en materia de prevención e investigación de los ciberdelitos y amenazas cibernéticas. Para el desarrollo de esta capacidad, resulta fundamental incrementar y fortalecer los vínculos entre los Estados mediante los mecanismos de cooperación existentes y la consignación de acuerdos específicos de entendimiento entre diferentes agencias con la finalidad de afrontar este fenómeno delictivo.

Principios rectores

DERECHOS Y LIBERTADES INDIVIDUALES: las acciones en materia de investigación y lucha contra el ciberdelito contemplaran el respeto por los derechos y libertades individuales establecidas en la Constitución Nacional, en los Tratados Internacionales en los que la República Argentina es parte, leyes nacionales y demás legislación vigente. Este principio garantiza que las medidas de seguridad no comprometan la privacidad y las libertades civiles.

CONDUCCION Y LIDERAZGO: el Ministerio de Seguridad de la Nación asume la conducción y propondrá las tareas a proyectar y articular con los pares provinciales e internacionales y organismos multinacionales, las universidades, la sociedad civil y el sector privado;y las acciones de fortalecimiento de capacidades para la prevención e investigación en materia de lucha contra la ciberdelincuencia. La coordinación interinstitucional y la cooperación internacional son claves para enfrentar los ciberdelitos de manera efectiva y enfrentar amenazas transnacionales.

PROACTIVIDAD Y PREVENCIÓN INTEGRAL: consiste en la realización de diferentes actividades que permitan diseñar una estrategia proactiva en la materia a fin de identificar de forma temprana diferentes actividades criminales relacionadas con delitos ciberasistidos, como así también la concientización de aquellas comunidades, grupos y sectores que puedan ser objeto de maniobras criminales. A tal efecto, resulta necesario articular estas acciones preventivas de forma conjunta con organizaciones públicas y privadas, académicas y organizaciones no gubernamentales para difundir buenas prácticas y acciones que fomenten una robusta cultura de ciberseguridad.

EFICACIA Y EFICIENCIA: El Ministerio de Seguridad busca que todas las acciones y medidas implementadas para combatir la ciberdelincuencia sean efectivas en la prevención, detección, respuesta e investigación de aquellos incidentes cibernéticos que aquejan a la comunidad e instituciones en general. En tal sentido, se debe maximizar el uso de los recursos disponibles tanto humanos como tecnológicos, de manera óptima y sostenible. Esto incluye la evaluación y medición del impacto, la innovación y adopción de tecnologías avanzadas, como así también la capacitación del personal. La colaboración y coordinación entre múltiples partes interesadas y la gestión de riesgos son esenciales para maximizar la resiliencia y garantizar la sostenibilidad.

Objetivos

Acorde lo establecido en la Resolución del Ministerio de Seguridad N° 977/2019, y persistiendo la necesidad de llevar a cabo diferentes acciones en materia de lucha contra la ciberdelincuencia y garantizar la ciberseguridad de los habitantes de la Nación Argentina, resulta oportuno desarrollar hasta el año 2027 el Plan Federal cuyo marco metodológico, diseño e implementación se encuentra alineado con la “Segunda Estrategia Nacional de Ciberseguridad” aprobada por Resolución 44/2023 de la Secretaría de Innovación Pública de la Jefatura de Gabinete de Ministros.

Objetivo general

Garantizar, en la medida de lo técnico y jurídicamente posible, el uso seguro del ciberespacio para protegerp los derechos y garantías reconocidos en la normativa vigente para los habitantes de la República Argentina.

Objetivos específicos

1. **Coordinación Federal en materia de lucha contra el ciberdelito**

a. Realizar un análisis integral del ciberdelito como fenómeno criminal y su impacto en nuestro país, elaborar y actualizar métricas que permitan identificar técnicas, tácticas y procedimientos utilizados por los cibercriminales con la finalidad de diseñar una estrategia sostenible en el tiempo y efectiva en el marco de la lucha contra esta modalidad delictiva.
b. Fortalecer la estructura orgánica y funcional del Centro de Sinergia Cibernética de las fuerzas policiales y de seguridad federales (CS5) a fin de dar acabada respuesta en materia de prevención e investigación de delitos asistidos tecnológicamente, como así también análisis forense digital.
c. Diseñar e implementar una plataforma que permita visibilizar y categorizar la incidencia de la actividad criminal en materia de ciberdelitos que será sustentada mediante información provista por las fuerzas federales, provinciales y autoridades locales competentes propiciando la conformación de una red nacional de lucha contra la ciberdelincuencia.
d. Promover la creación de grupos de trabajo especializados en diferentes temáticas, conformados por profesionales de las fuerzas policiales y de seguridad federales con la finalidad de aunar criterios y metodologías sobre la base de su experiencia operativa en materia de investigación de ciberdelitos alineados con reglas de buenas prácticas y estándares nacionales e internacionales con amplia injerencia en la temática.
e. Realizar las coordinaciones pertinentes a fin de promover el estudio, reporte y mitigación de vulnerabilidades y amenazas informáticas ante la presencia de usos ilícitos o perjudiciales de las infraestructuras tecnológicas que gestionenestos incidentes de forma conjunta con aquellas agencias competentes en la materia.
f. Participar activamente en el Comité de Ciberseguridad para, así, poner a disposición aquellos recursos humanos y tecnológicos disponibles para intervenir ante un incidente o vulneración cibernética que afecte la seguridad publica en el ámbito de la Administración Pública Nacional.
g. Fomentar el desarrollo de indicadores y métricas de desempeño que permitan determinar el grado de madurez en materia de lucha contra la ciberdelincuencia y el fortalecimiento de la seguridad de la información con la finalidad de la mejora continua y promover una cultura sostenible en el tiempo respecto de estos ejes temáticos.

2. **Fortalecimiento y capacitación altamente especializada**

a. Planificar y desarrollar cursos, talleres y ejercicios destinados al personal de las fuerzas policiales y de seguridad federales que realicen la integración de los planes anuales de capacitación con el fin de generar una actualización de sus conocimientos e incrementar sus capacidades operativas en materia de respuesta y lucha contra la ciberdelincuencia.
b. Elaborar y actualizar aquellos protocolos específicos sobre técnicas de prevención e investigación de los delitos ciberasistidos, preservación y manejo de evidencias digitales, cadena de custodia, trazabilidad de criptoactivos y análisis forense digital en sus diferentes especialidades.
c. Incrementar el desarrollo de actividades transversales de formación en materia de ciberseguridad e investigación del ciberdelito que incluyan diferentes partes interesadas, entre ellas el sector académico y la vinculación científica con la finalidad de promover el fortalecimiento de las capacidades tecnológicas.
d. Realizar un amplio abordaje sobre múltiples tecnologías emergentes, en especial aquellas cuyo impacto disruptivo en materia de ciberdelincuencia y ciberseguridad impliquen un desafío desde el punto de vista investigativo como, por ejemplo, inteligencia artificial, internet de las cosas y criptoactivos, entre otras.
e. Promocionar e incentivar el interés en materia de la lucha contra el ciberdelito en jóvenes que estén

cursando ciclos lectivos, a través de disertaciones y talleres prácticos que les permitan medir sus habilidades técnicas, para generar personal calificado que pueda desarrollarse en el sector público y privado.

3. **Actualización del marco normativo**

a. Promover en coordinación con los organismos de competencia propuestas de actualización del marco jurídico vigente sobre la base del respeto a las garantías constitucionales y haciendo especial énfasis en la necesidad de alinear nuestra normativa con aquellos estándares mínimos adoptados por la comunidad internacional en tenor de las lecciones aprendidas sobre las nuevas amenazas y actos delictivos que se desarrollan en el ciberespacio.
b. Fortalecimiento de las normas, estandarización de procesos, procedimientos y protocolos vinculados a la ciberseguridad y la investigación del ciberdelito como fenómeno criminal, tratamiento y manejo de evidencias almacenadas electrónicamente y cadena de custodia, entre otros.
c. Impulsar y colaborar activamente en el desarrollo e implementación de políticas, estándares y procedimientos vinculados con la ciberseguridad de las infraestructuras críticas.

4. **Incremento de las capacidades en materia de análisis forense digital**

a. Fomentar la capacitación como una de las principales directrices para incrementar la cantidad de personal especializado en materia de análisis forense digital.
b. Promover el desarrollo de las capacidades del personal que se encuentra encargado del manejo y gestión de evidencias almacenadas electrónicamente distinguiendo, especialmente, los roles y funciones que deberá cumplir ya sea como primer interviniente en la escena del crimen o bien como experto en análisis de evidencias digitales.
c. Coordinar la integración de los planes anuales de capacitación de las fuerzas federales de seguridad en materia de análisis forense digital mediante el diseño de programas educativos que permitan brindar certificaciones en materia de análisis forense digital en diferentes temáticas y niveles de especialización.
d. Gestionar los activos informáticos empleados en las diferentes actividades y tareas que demanda el análisis forense digital con la finalidad de proponer una estrategia eficiente de crecimiento y fortalecimiento de las capacidades tecnológicas.
e. Diseñar indicadores y métricas de desempeño que permitan evaluar el tipo y cantidad de intervenciones en materia de análisis forense digital que categoricen estas actividades según la naturaleza de los dispositivos analizados y los resultados obtenidos, todo ello con la finalidad de la mejora continua y una gestión eficiente de los recursos humanos y materiales empeñados.

5. **Cooperación Internacional**

a. Ampliar el desarrollo de acuerdos a nivel regional e internacional que incrementen la colaboración, de acuerdo a la normativa vigente, con naciones y organizaciones internacionales cuyo esfuerzo se encuentre abocado a la prevención, respuesta e investigación en materia de ciberdelitos.
b. Fortalecer la presencia y la participación nacional e internacional en entrenamientos, talleres y ejercicios vinculados con el ciberdelito como fenómeno criminal y la gestión de incidentes de seguridad.
c. Posicionar a nuestro país como referente en materia de lucha contra la ciberdelincuencia y desarrollo de políticas de ciberseguridad que promuevan la cooperación internacional como eje principal de este nuevo paradigma.

6. **Protección de la niñez**

a. Incrementar las alianzas y esfuerzos para la detección e investigación de los delitos cometidos por medio de las tecnologías de la comunicación e información, en particular, aquellos dirigidos contra la infancia e integridad sexual de las niñas, niños y adolescentes.
b. Sensibilizar a la sociedad mediante contenidos orientativos para la detección y denuncia contra aquellos adultos que acosen a través de redes sociales u otro canal informático a menores, como así también aquellos que almacenen, compartan o distribuyan contenido de abuso sexual infantil.
c. Fortalecer las capacidades de respuesta y asistencia a la víctima en este tipo de delitos, mediante la permanente actualización de la infraestructura técnico-operativa de aquellas áreas de las fuerzas federales de seguridad que posean injerencia alguna en la materia.

7. **Acciones de concientización y prevención del ciberdelito**

a. Diseñar diferentes capacitaciones, piezas comunicativas y material destinado a sensibilizar a los diferentes sectores y a la comunidad en general con el fin de que conozcan los riegos que acarrean las nuevas tecnologías y cómo prevenirse ante la posibilidad de ser víctimas de los cibercriminales.
b. Difundir información acerca de cómo proceder en caso de ser víctimas de un delito ciberasistido y cómo realizar la denuncia correspondiente según el tipo de delito de que se trate y que promueva la utilización de la línea 134 como principal forma de asistencia.
c. Fortalecer el esfuerzo en materia de prevención de delitos asistidos tecnológicamente que se desarrollan en el ciberespacio mediante el diseño de lineamientos estratégicos que permitan adoptar una actitud proactiva por parte de las fuerzas federales de seguridad.
d. Promover el desarrollo de iniciativas de manera conjunta con aquellos organismos correspondientes a fin de evaluar la implementación de la ciudadanía digital.

8. **Cooperación Multisectorial**

a. Incrementar la colaboración Público-Privada haciendo hincapié en el sector financiero, como así también los proveedores de servicios y empresas vinculadas con las tecnologías de la información y las comunicaciones.
b. Establecer como prioritario el nexo con los proveedores de servicios de activos virtuales en atención a la preponderancia que este tipo de tecnología posee a nivel global.
c. Promover la colaboración con diferentes sociedades civiles e instituciones educativas.
d. Fomentar y potenciar las capacidades tecnológicas en materia de investigación, desarrollo e innovación con la finalidad de incrementar las capacidades en materia de análisis forense digital.

Digitally signed by GESTION DOCUMENTAL ELECTRONICA - GDE
Date: 2025.01.13 11:19:40 -03:00

Santiago Gonzalez Bellengeri
Director
Dirección de Ciberdelito y Asuntos Cibernéticos
Ministerio de Seguridad

Digitally signed by GESTION DOCUMENTAL ELECTRONICA - GDE
Date: 2025.01.13 11:19:41 -03:00