“PLAN FEDERAL DE PREVENCIÓN DE DELITOS TECNOLÓGICOS Y CIBERDELITOS (2019-2023)”

INTRODUCCIÓN

Los ciudadanos y visitantes del Territorio Nacional utilizan el ciberespacio para relacionarse, para informarse, para expresarse, para investigar y desarrollar productos, para crear obras artísticas, para comerciar, para brindar servicios, y otras tantas tareas que son parte de su vida social y laboral.

La esencia global del ciberespacio, ofrece innumerables posibilidades en vista al desarrollo humano, conllevando en las mismas oportunidades, nuevos riesgos y amenazas a las garantías constitucionales de los usuarios, a las organizaciones, a la seguridad integral de las actividades de las naciones. Las amenazas están evolucionando, así como los delincuentes individuales, las organizaciones criminales nacionales y transnacionales, y otros actores malintencionados mudan sus actividades al mundo digital.

Los delincuentes asi como las organizaciones criminales, los grupos terroristas, los delitos basados en entidades bancarias y financieras que pueden ser partícipes de financiamiento al terrorismo, el lavado de activos y el narcotráfico, la venta ilegal de armas, la trata de personas, los delitos contra la integridad sexual, entre otros, encuentran en las nuevas tecnologías y en el ciberespacio los canales necesarios para anonimizarse, organizarse, buscar sus víctimas y llevar adelante sus acciones.

Consciente de la situación nacional e internacional del ciberdelito, mediante la Decisión Administrativa Nª 299/2018, se creó en el MINISTERIO DE SEGURIDAD DE LA NACIÓN, la DIRECCIÓN DE INVESTIGACIÓN DEL CIBERDELITO dependiente de la DIRECCIÓN NACIONAL DE INVESTIGACIONES de la SECRETARIA DE SEGURIDAD. Asimismo, se han creado áreas específicas en la temática, en la Policía Federal Argentina, en la Gendarmería Nacional Argentina, en la Prefectura Nacional Argentina y en la Policía de Seguridad Aeroportuaria, tendientes a atender la problemática especializada en las amenazas que atenten contra los individuos y organizaciones en general, pero también con unidades específicas de atención y contención en aquellos que involucren a menores de edad.

Considerando el avance y cantidad de hechos delictivos que utilizan las tecnologías como medio o como fin de sus objetivos a atacar y que los despliegues de estos actos delictivos poseen carácter trasnacional, evolucionando constantemente, es que desde el Ministerio de Seguridad consideramos que es necesario elaborar un **“PLAN FEDERAL DE PREVENCIÓN DE DELITOS TECNOLÓGICOS Y CIBERDELITOS”**

El presente, nos permitirá trazar un curso de accion tendiente a la protección de los ciudadanos y organizaciones de estos actores malintencionados, coadyuve a reducir las amenazas, alertar de nuevas modalidades de los cibercriminales, investigar los delitos cibernéticos o que se cometan a través de medios cibernéticos y disminuir las consecuencias de los incidentes a través de medios cibernéticos. De esta forma poder articular y acrecentar una respuesta federal efectiva, cuando corresponda, contra los cibercriminales.

Este Plan Federal, que se encuentra en su totalidad alineado a la "**Estrategia Nacional de Ciberseguridad**" aprobada por **Resolución 829/2019 de la Secretaría de Gobierno de Modernización de la Jefatura de Gabinete de Ministros**, establece nuestra visión de metas, objetivos y prioridades para ejecutar con éxito toda la gama de responsabilidades referente al ciberespacio y su impacto en la Seguridad Nacional, dejando expresa constancia de que estas acciones se llevarán a cabo sobre la base de la coordinación y cooperación entre las Administraciones Públicas, los Poderes, el sector privado, las organizaciones no gubernamentales y las entidades académicas. Todo ello en el marco del respeto a los principios recogidos en la Constitución Nacional y a las disposiciones de los tratados y acuerdos internacionales a los que la Republica Argentina ha adherido.

A los fines del presente documento debe entenderse como "Ciberdelito" a delitos realizados por a través de las tecnologías de la información y comunicación (TIC´s) en el ciberespacio. Asimismo, debe entenderse como "Delitos Tecnológicos" aquellos delitos cuya planificación, organización, ejecución o resultado se encuentra expuesta en el ciberespacio o en elementos tecnológicos que pueden ayudar tanto en la investigación de delitos tradicionales como en ciberdelitos.

ESTADO DE SITUACION

En la actualidad contamos en el Ministerio con diversas areas que se abocan a la tarea de prevención, detección, investigación y asistencia en caso de ciberdelitos y delitos tecnológicos, dado soporte a los requerimientos judiciales y a las víctimas. Estas acciones se encuentran limitadas por diferentes razones como ser:

Necesidad de coordinación y nivelación de todas las areas competentes en las fuerzas de seguridad: el avance en la creación de areas tanto en el Ministerio como en cada fuerza conllevó a estructuras de trabajo que fueron creciendo acorde a las posibilidades y experiencias de cada fuerza. Para optimizar el funcionamiento, lograr una métrica estandarizada e incorporar los hallazgos de nuevas problemáticas y resoluciones en pos de la mejora continua, es necesario una mayor nivelación, articulación y coordinación con patrones de trabajo y areas comunes en cada fuerza federal.

Necesidad de incremento de personal idoneo y herramientas tecnológicas en las áreas: el volumen de casos de ciberdelitos y análisis tanto de investigaciones, análisis y de forensia de equipamientos resulta en la necesidad de dotar de mayor personal con los conocimientos necesarios para cumplir las tareas. Asimismo, incorporar tecnologías que permitan un más rápido accionar y que permitan la agilización de los análisis tanto investigativos como forenses.

Necesidad de normativa específica: algunos de los delitos considerados no federales, en el avance de las investigaciones demuestran una articulación delictiva con individuos, victimarios y víctimas, que se encuentran en diferentes jurisdicciones territoriales. Esto conlleva a la necesidad de normativa que permita un avance coordinado nación-provincias que facilite la cooperación federal en la materia asi como la utilización de nuevas herramientas y técnicas en la investigacion y detención de los delincuentes.

Necesidad de fortalecimiento de la prevención: uno de los factores principales del incremento del delito en el ciberespacio es la falta de concientización y conocimiento de estos delitos por parte de la sociedad. Por ello es necesario incursionar desde el Ministerio y las Fuerzas Federales en planes de proximidad de concientización a la población en general, principalmente en menores en edades escolares y en segmentos de adultos mayores a los fines de que tomen las precauciones para tratar de evitar de ser víctimas de los delincuentes. Asimismo, producir material para alertar y prevenir tanto por medios de difusión tradicionales como digitales, contemplando la producción de material para ser utilizados en escuelas, colegios, universidades y material específico para el sector privado.

Necesidad de incremento de cooperación público-privado: el Ministerio de Seguridad a través de la Dirección de Investigaciones del Ciberdelito de la Direccion Nacional de Investigaciones, viene desarrollando mesas de cooperación público-privada con la participación de más de 45 responsables de seguridad de la información y sistemas de diferentes empresas de diversos sectores productivos. La necesidad de cooperar y colaborar en el marco de la detección e investigacion del ciberdelito y basado en que las infraestructuras de información son basados en empresas del sector privado, genera la necesidad de un incremento en acciones determina la necesidad de la creación de un Foro de cooperación público-privado que nos permita trazar proyectos de generación de confianza y colaboración a largo plazo.

Necesidad de incremento de cooperación internacional: tanto en las investigaciones como en la prevención reviste de suma importancia la cooperación que desde otros estados y organizaciones puedan brindar para un más rápido y eficaz procedimiento. Si bien en la actualidad contamos con canales de comunicación en cada institución para estos fines, los mismo deben ser fortalecidos y agilizados siempre en respeto del marco legal, a los fines de obtener los alertas e información en tiempo y forma que sirvan para las causas en curso. Es necesario pues incrementar y fortalecer los vínculos transnacionales que permitan un mayor acercamiento a los organismos competentes en cada estado logrando una mayor posibilidad de cooperación y colaboración.

Necesidad de mejoras y nuevas propuestas: uno de los puntos más críticos de las nuevas tecnologías es el amplio espectro de posibilidades para los delincuentes, quienes no dejan de probar cada nuevo vector, servicio, dispositivo o tecnología que aparece para intentar cometer algún delito. Por ellos es necesario fortalecer los conocimientos e incrementar los aportes tanto tecnológicos como metodológicos a través de la confirmación de grupos de especialistas en diferentes aspectos y problemáticas del ciberespacio que coadyuven a construir y ampliar la superficie de atención y monitoreo de posibles incidentes asi como el tratamiento de nuevas metodologías de investigación.

OBJETIVOS GENERALES

- Contar al año 2023 con el personal idóneo, tecnología y normativa necesaria para combatir los delitos realizados a través de las tecnologías de la información y comunicación (TIC) en todo el Territorio Nacional.

- Encontrarnos al año 2023 con el conocimiento de métricas nacionales y equipos de respuesta a lo largo del territorio federal.

CAPITULO I

PRINCIPIOS RECTORES

PLAN FEDERAL DE PREVENCIÓN DE DELITOS TECNOLÓGICOS Y CIBERDELITOS", se basa en los siguientes Principios Rectores:

- **DERECHOS Y LIBERTADES INDIVIDUALES:** las acciones en materia investigación y lucha contra el ciberdelito contemplará el respeto por los derechos y libertades individuales, establecidas en la Constitución Nacional y en los Tratados Internacionales en los que la República Argentina es parte.

- **CONDUCCIÓN Y ARTICULACION**: el Ministerio de Seguridad de la Nación asume la conducción y propondrá las tareas a proyectar y articular con los pares provinciales, el sector privado, las universidades, la sociedad civil, los pares internacionales y organismos multinacionales, las acciones de fortalecimiento de capacidades para la atención, detección, investigación y persecución de criminales que utilicen el ciberespacio para actos ilícitos.

- **FORTALECIMIENTO DE CAPACIDADES**: incrementar la dotación de personal especializado en la problemática y mantener actualizado el conocimiento sobre las modalidades y técnicas que utilizan los criminales es uno de los principales retos a encarar debido a que el principal recurso en la prevención y lucha contra el ciberdelito es el conocimiento y ética del personal involucrado.

- **PREVENCION**: la proactividad en esta materia incluye desde la construcción de ejercicios prácticos hasta la concientización de los diferentes comunidades, grupos y sectores que pueden ser objeto de maniobras criminales. Por ello, contamos con la articulación con organizaciones públicas y privadas, académicas y organizaciones no gubernamentales para difundir buenas prácticas y acciones responsables para generar un ciberespacio seguro.

- **INTEGRACION INTERNACIONAL**: mancomunar esfuerzos y conocimientos con fuerzas, agencias y organizaciones internacionales debido a que el ciberespacio no reconoce fronteras físicas y la transnacionalidad de las amenazas cibernéticas demandan de la cooperación global y regional.

- **RESPONSABILIDAD COMPARTIDA**: las infraestructuras de comunicación, los servicios y diversas aplicaciones que se utilizan, en su gran mayoría, son provenientes del

Sector Privado. Por ello el esfuerzo nacional de lucha contra el ciberdelito incluye la cooperación público-privada que permita la cooperación, colaboración y generación de confianza a través de acciones concretas.

CAPITULO II

METAS ESTRATÉGICAS Y ESPECIFICAS

Meta 1) Coordinacion Federal de Lucha contra el Ciberdelito.

Acciones generales:

- Creación del **Centro de Atención y Respuesta al Ciberdelito (CARC-247)**, el mismo brindará atención las 24 horas todos los días del año, con recursos humanos provenientes de las diferentes fuerzas que integran el esfuerzo nacional de lucha contra el ciberdelito, sumado a la atención telefónica a través del número 134.
- Creación del plan de **articulación** con las fuerzas locales para la **creación y fortalecimiento** de áreas específicas en las tareas de lucha contra el ciberdelito.
- Generación de la **base de conocimiento** federal para el intercambio de incidentes, técnicas, amenazas y demás información que permita el accionar conjunto contra los delincuentes.
- Creación del **Sistema Federal de Ciberdelitos**, la cual será nutrida con la información provista por las fuerzas federales, fuerzas provinciales y autoridades locales competentes. con el fin de recabar información de delitos y posibles delitos cometidos a través de las tecnologías de información y las comunicaciones.

Meta 2) Fortalecimiento en capacitación.

Acciones generales:

- Desarrollo de cursos, talleres y ejercicios destinado a las fuerzas de seguridad con el fin de generar una actualización en **conocimientos** en las capacidades de respuesta y profundizar una **dinámica operativa federal**.
- Elaboración y actualización de **protocolos** en técnicas de detección, investigación, preservación de pruebas, cadena de custodia y forense.
- Incremento de las actividades transversales de **formación** incluyendo al sector académico, la vinculación científica y el fortalecimiento de las capacidades tecnológicas.
- Promocionar e incentivar el interés en materia de la lucha contra el ciberdelito en jóvenes adolescentes que estén cursando ciclos lectivos, a través de disertaciones y competencias, para **generar personal calificado** que pueda desarrollarse en el sector público y privado.

Meta 3) Actualización del marco normativo.

Acciones generales:

- Promover en coordinación con los organismos de competencia, propuestas de actualización del marco jurídico tomando en cuenta la necesidad de principios comunes mínimos con la comunidad internacional y las garantías constitucionales, de acuerdo a las **lecciones aprendidas** sobre las nuevas amenazas y actos delictivo
- Fortalecimiento de las normas, **estandarización de procesos, procedimientos y protocolos** vinculados a la investigación, tratamiento de prueba, cadena de custodia entre otros, en materia de ciberdelito.

Meta 4) Incremento de las capacidades forenses.

Acciones generales:

- Incrementar las capacidades del personal afectado a análisis forenses de equipos encontrados en escenas de crímenes como ser dispositivos móviles, routers, cámaras, y todo aquel dispositivo que pudiera ayudar en la investigación de un delito, creando a tal fin el **Curso de generación de Expertos Forenses Digitales**.
- Creación del **Registro de Expertos Forenses Digitales** del Ministerio de Seguridad, integrado por especialistas calificados de todas las fuerzas federales, que hayan aprobado las capacitaciones requeridas.
- **Ampliación y articulación** del parque de equipos afectados a los análisis forenses de dispositivos digitales.

Meta 5) Cooperación Internacional.

Acciones generales:

- Ampliar el desarrollo de acuerdos a nivel regional e internacional **incrementando la colaboración**, de acuerdo a la normativa vigente, con naciones y organizaciones internacionales que trabajen en la prevención y respuesta a ciberdelito.
- Fortalecer la **presencia y participación** nacional en entrenamientos, talleres y ejercicios internacionales.

Meta 6) Protección de la niñez.

Acciones generales:

- Incrementar las alianzas y esfuerzos para la detección e investigación de los delitos cometidos a través de las redes sociales, en particular los dirigidos contra la **infancia y la integridad sexual de los menores**.
- Generación de contenidos orientativos para la detección y denuncia de los mayores que **acosen** a través de las redes a menores o distribuyan material, penado por Ley, con contenidos de menores.

Meta 7) Acción de concientización y prevención.

Acciones generales

- Brindar disertaciones y material a los **diferentes sectores y a la comunidad** con el fin de que conozcan los riegos que acarrean las nuevas tecnologías y cómo prevenir ser víctimas de los criminales
- Difundir la información de cómo proceder en caso de ser víctima de delito cibernético y **como realizar la denuncia** correspondiente según el caso de delito de que se trate.
- Profundizar las acciones de prevención a través de la **detección temprana** de delitos de acción pública cometidos por medios cibernéticos.

Meta 8) Cooperación Público Privado.

Acciones generales

- Incrementar la colaboración con los **proveedores de servicios y empresas** de las tecnologías de la información y las comunicaciones.
- Fomentar y potenciar las **capacidades tecnológicas** precisas para disponer de soluciones confiables que permitan responder adecuadamente frente a las diferentes amenazas, fomentando las actividades de investigación, desarrollo e innovación (I+D+i).

Meta 9) Comisión Asesora

Acciones generales:

- Creación de la Comisión Asesora en materia de lucha contra el ciberdelito la cual será conformada por especialistas con perfiles **intra, inter y multidisciplinarios** que nos permitirá estar actualizados y en concordancia con los avances en la materia. Los participantes de la misma serán en carácter Ad-Honorem

República Argentina - Poder Ejecutivo Nacional
2019 - Año de la Exportación

Hoja Adicional de Firmas
Anexo

Número: IF-2019-94761790-APN-DIC#MSG

CIUDAD DE BUENOS AIRES
Lunes 21 de Octubre de 2019

Referencia: EX-2018-68075998- -APN-DIC#MSG - PLAN FEDERAL DE PREVENCIÓN DE DELITOS TECNOLÓGICOS Y CIBERDELITOS (2019 - 2023)

El documento fue importado por el sistema GEDO con un total de 11 pagina/s.

Digitally signed by GESTION DOCUMENTAL ELECTRONICA - GDE
Date: 2019.10.21 14:21:15 -03:00

Pablo Lazaro
Director
Dirección de Investigaciones del Ciberdelito
Ministerio de Seguridad

Digitally signed by GESTION DOCUMENTAL ELECTRONICA - GDE
Date: 2019.10.21 14:21:16 -03:00