República Argentina - Poder Ejecutivo Nacional
Las Malvinas son argentinas

Informe

Número: IF-2022-05822603-APN-UGA#MSG

CIUDAD DE BUENOS AIRES
Miércoles 19 de Enero de 2022

Referencia: ANEXO ÚNICO PLAN FEDERAL PRESO EX-2022-01773043- -APN-UGA#MSG

ANEXO ÚNICO

ACTUALIZACION DEL

“PLAN FEDERAL DE PREVENCIÓN

DE DELITOS TECNOLÓGICOS Y CIBERDELITOS (2021-2024)”

Diagnóstico

Desde los últimos años de la década del 70 del siglo pasado hasta la actualidad, las sociedades dieron paso a una nueva forma de comunicación e interrelación basada principalmente en el progreso tecnológico y con ella en la inmediatez, el acceso a la información. En este proceso la digitalización tiene un rol clave en el desarrollo social modificando las relaciones interpersonales, la forma en la que se educa, se aprende, se brinda y se recibe entretenimiento, se produce, se brinda servicios.

Estas transformaciones también afectaron a la forma en que el delito se relaciona con el ciberespacio, por un lado, se utilizan las nuevas tecnologías como herramientas para cometer delitos clásicos (por ejemplo, fraudes) y por el otro estas nuevas tecnologías dieron paso a nuevas manifestaciones delictivas (por ejemplo, ransomware). De esta manera se pueden identificar distintos tipos de ciberdelincuentes. Entre ellos se pueden reconocer a personas que no forman parte de ninguna estructura asociada a la criminalidad organizada y cometen ilícitos con beneficios solo para sí mismo mientras que, por otra parte, encontramos ciberdelincuentes que forman parte de organizaciones criminales asociadas con el objeto de obtener un rédito económico, político o geopolítico, siendo un caso de estos los grupos que utilizan amenazas persistentes avanzadas (Advanced Persistent Threads – APT) con el objeto y la capacidad de atacar de forma avanzada, a través de múltiples vectores de ataque, y de forma sostenible en el tiempo, un objetivo determinado sea este una empresa, una infraestructura critica o un Estado.

Pero, sin duda alguna, la tecnología tiene incursión transversal a los delitos tipificados en el Código Penal Argentino.

Como hemos señalado, el panorama de la ciberseguridad se ha visto comprometido y complejizado a partir de la irrupción de la pandemia COVID -19, que ha profundizado los riesgos del ciberespacio y claro ejemplo son los ataques producidos a diferentes entidades del Gobierno Nacional que han tomado estado público.

Tal es así que, a nivel mundial, se observó un aumento de las estafas por internet, el phishing, el vishing, smishing, infiltraciones, exposición de información y bases de datos sensibles, un aumento considerable en BEC´s (por sus siglas en ingles Business Email Compromise) y ransomware, así como la utilización de todo tipo de malware y campañas de desinformación, particularmente sobre la problemática de salud que nos encontrábamos atravesando y en campañas de asistencia social del Gobierno Nacional.

De este modo, encontramos que el desafío de los Estados en la actualidad, y en particular de nuestro país, radica en preservar los derechos y garantías de todos los habitantes, trabajando de una manera federal, multiagencia e interpoderes, desde las perspectivas de distintas disciplinas y con participación de la sociedad civil, la academia, así como el sector privado.

A los efectos de dar respuesta a la situación descripta se han identificado diferentes áreas prioritarias para ser abordadas:

a) **coordinación federal y multiagencia**: Para abordar el desafío planteado es necesario la articulación entre los tres (3) poderos del Estado (ejecutivo, legislativo y judicial), tanto a nivel central como con las 23 jurisdicciones provinciales y la Ciudad Autónoma de Buenos Aires.

b) **fortalecer los recursos humanos del Estado Nacional y las herramientas tecnológicas**: Las constantes innovaciones que se han llevado a cabo a partir del uso de las nuevas tecnologías requiere que el Estado Nacional arbitre los medios para que los recursos humanos y materiales con los que se debe contar estén a la altura del desafío que debe afrontar siendo aprovechados en su totalidad.

c) **creación y actualización normativa**: La evolución constante del fenómeno hace que se deba evaluar la actualización, así como la creación de nueva normativa relacionada a un mejor entendimiento de la investigación del delito por medios cibernéticos, que atienda tanto la calidad del proceso como los tiempos de respuesta.

d) **acciones de campaña de prevención del ciberdelito**: En el marco de garantizar a los habitantes de nuestro país un adecuado nivel de seguridad es importante que se realicen distintas acciones de comunicación y sensibilización, que ayuden a reducir y alertar la comisión de delitos.

e) **crear equipos de respuesta específicamente capacitados**: Ciertos delitos en crecimiento deben contar con una respuesta del personal entrenado para su investigación y análisis, siguiendo metodologías modernas y agiles en forma innovadora, y contando con áreas altamente equipadas para dar respuesta efectiva en tiempo y forma a la alta demanda judicial, tanto en lo investigativo como en lo forense.

f) **incremento de cooperación público-privado**: A los efectos de prevenir e investigar los delitos asociados a las nuevas tecnologías, la cooperación entre el Estado Nacional, la ciudadanía en general, las organizaciones de la sociedad civil y las empresas privadas se vuelve cada día más relevante y fundamental.

g) **incremento y profundización de la cooperación internacional**: La cooperación internacional se torna

indispensable a los efectos de la prevención e investigación de los delitos y amenazas vinculados al ciberespacio dado que aumentan las capacidades de los Estados para afrontar la problemática.

h) **profundizar las acciones preventivas**: Las acciones de prevención que las fuerzas de ley deben llevar adelante en el marco de sus competencias formalmente establecidas, deben ser fortalecidas y ampliadas acorde al Código Penal, con el fin de proteger a la ciudadanía frente al amplio abanico de ciberdelitos existentes, en consonancia con el punto d) del presente y las detecciones tempranas de vulnerabilidades.

i) **Acciones interministeriales de abordaje de los incidentes prioritarios**: Generación de una instancia gubernamental que tome intervención ante un incidente o vulneración cibernética que afecte la seguridad publica en el ámbito de la Administración Pública Nacional.

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 Republica Argentina es parte, leyes nacionales y demás legislación vigente.

CONDUCCION Y ARTICULACION: el Ministerio de Seguridad de la Nación asume la conducción y propondrá las tareas a proyectar y articular con los pares provinciales, los pares internacionales, las universidades, la sociedad civil y el sector privado, las acciones de fortalecimiento de capacidades para la prevención e investigación de ilícitos en el ciberespacio.

PREVENCIÓN: El Ministerio de Seguridad impulsa en materia de ciberseguridad y ciberdelitos una acción multiagencia, con fuerte participación de la ciudadanía en general, con el objeto de evitar que los distintos tipos de delitos asociados al ciberespacio ocurran.

EFICIENCIA: El Ministerio de Seguridad busca que, todas las acciones en materia de prevención e investigación, sean realizadas bajo parámetros de optimización de recursos y por ende de eficiencia.

Objetivos

Tal como fue mencionado en la Resolución del Ministerio de Seguridad N° 977/2019, y persistiendo la necesidad de llevar acabo las acciones, siendo estas intensificadas por la necesaria hiperconectividad que generó la pandemia, extendemos al 2024 el Plan Federal y ampliamos algunos objetivos específicos acorde a las lecciones aprendidas.

Objetivo General

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

Líneas de acción

1) Coordinación y fortalecimiento Federal frente al ciberdelito

a) Elaborar y actualizar anualmente un diagnóstico sobre la situación del fenómeno del ciberdelito en Argentina.

b) Crear un centro de investigación en la materia compuesto por las fuerzas federales para la investigación de delitos de alta tecnología.

c) Crear un Tablero Federal de Alerta Temprana en materia de ciberdelitos, el cual será nutrido 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.

d) Generar una instancia en la que las fuerzas federales y provinciales compartan experiencias de buenas prácticas y experiencias en investigación de ciberdelitos.

e) Coordinar actuaciones centralizadas para el estudio y reducción de vulnerabilidades y amenazas informáticas ante usos ilícitos o perjudiciales de las infraestructuras tecnológicas.

f) Formular una propuesta para la creación de una instancia gubernamental que tome intervención ante un incidente o vulneración cibernética que afecte la seguridad publica en el ámbito de la Administración Pública Nacional.

g) Impulsar el desarrollo de métricas que permitan determinar el nivel de seguridad y su evolución en el tiempo.

2) Fortalecimiento en la capacitación especifica

a) Desarrollo de cursos, talleres y ejercicios destinados al personal de las fuerzas federales policiales y de seguridad, con el fin de generar una actualización en conocimientos en las capacidades de respuesta y profundizar una dinámica operativa federal, invitando a participar a los Ministerios Públicos Fiscales.

b) Elaboración y actualización de protocolos en técnicas de detección, investigación, preservación de pruebas, cadena de custodia y forense.

c) Incremento de las actividades transversales de formación en ciberseguridad e investigación del ciberdelito incluyendo al sector académico, la vinculación científica y el fortalecimiento de las capacidades tecnológicas.

3) Actualización del marco normativo

a) Promover en coordinación con los organismos de competencia, propuestas de actualización del marco jurídico tomando en cuenta la necesidad de estándares mínimos comunes con la comunidad internacional y las garantías constitucionales, de acuerdo con las lecciones aprendidas sobre las nuevas amenazas y actos delictivos.

b) Fortalecimiento de las normas, estandarización de procesos, procedimientos y protocolos vinculados a la ciberseguridad y a la investigación, tratamiento de prueba, cadena de custodia entre otros, en materia de ciberdelito.

c) Impulsar y colaborar en el desarrollo de normativa sobre infraestructura crítica.

4) Incremento de las capacidades forenses

a) Incrementar la cantidad de personal calificado a los efectos de la realización de tareas forenses.

b) Incrementar las capacidades del personal afectado a análisis forenses de equipos y dispositivos encontrados en

escenas de crímenes que pudiera ayudar en la investigación de un delito, creando a tal fin el Curso de generación de Expertos Forenses Digitales.

c) Ampliación y gestión del parque de equipos afectados a los análisis forenses de dispositivos digitales, aumentando su cantidad y variedad.

5) Cooperación Internacional

a) 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 al ciberdelito.

b) Fortalecer la presencia y participación nacional en entrenamientos, talleres y ejercicios internacionales.

6) Protección de la niñez

a) Incrementar las alianzas y esfuerzos para la detección e investigación de los delitos cometidos a través de las redes sociales u otro canal informático, en particular los dirigidos contra la infancia y la integridad sexual de los menores.

b) Generación de contenidos orientativos para la detección y denuncia para quienes acosen a través de las redes sociales u otro canal informático, a menores o distribuyan material, penado por Ley, con contenidos de menores.

c) Fortalecer la infraestructura técnico-operativa del área.

7) Acciones de prevención del ciberdelito

a) Producir y 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.

b) 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.

c) Impulsar iniciativas con los organismos correspondientes tendientes a la ciudadanía digital.

8) Cooperación Multisectorial

a) Incrementar la colaboración Público-Privada, con especial foco con el sector financiero y con los proveedores de servicios y empresas de las tecnologías de la información y las comunicaciones.

b) Incrementar la colaboración con la Sociedad Civil y las instituciones educativas.

c) Fomentar y potenciar las capacidades tecnológicas precisas para disponer de soluciones confiables que permitan responder adecuadamente frente a las diferentes amenazas, focalizando en las actividades de investigación, desarrollo e innovación (I+D+i).

José Lucas Gaincerain
Titular
Unidad Gabinete de Asesores
Ministerio de Seguridad

Digitally signed by Gestion Documental Electronica
Date: 2022.01.19 16:57:41 -03:00