Que por Resolución N° 39/10 de la entonces SECRETARIA DE LA GESTIÓN PÚBLICA de la JEFATURA DE GABINETE DE MINISTROS sustituida por el Anexo I de la Resolución N° 166 de fecha 14 de agosto de 2015 de la ex SECRETARÍA DE GABINETE DE LA JEFATURA DE GABINETE DE MINISTROS se dispuso que la asignación del grado escalafonario podrá formalizarse una vez efectuada la designación, a través del acto administrativo previsto en la jurisdicción o entidad descentralizada en cuya dotación se integre el cargo, para la asignación de grado para el personal del régimen de carrera, con retroactividad a la fecha de designación.

Que por último la Decisión Administrativa N° 449 del 7 de mayo de 2021, incorporó y asignó los cargos vacantes detallados en el ANEXO I (IF-2021-32327012-APN-DNGIYPS#JGM), con el fin de proceder a la designación de personal en la planta permanente en las distintas Jurisdicciones y Entidades de la Administración Pública Nacional, atento los procesos de selección de personal oportunamente sustanciados y a realizarse, con carácter de excepción al artículo 7° de la Ley N° 27.591.

Que en el proceso de selección citado precedentemente no hubo impugnación alguna, así como tampoco fue recurrido el orden de mérito definitivo.

Que dichas designaciones no implican la asignación de recurso extraordinario alguno.

Que la OFICINA NACIONAL DE EMPLEO PÚBLICO de la JEFATURA DE GABINETE DE MINISTROS y la DIRECCIÓN GENERAL DE ASUNTOS JURÍDICOS del MINISTERIO DE SALUD han tomado la intervención que les compete.

Que la presente medida se dicta de conformidad con lo dispuesto por la Ley de Ministerios Nº 22.520, texto ordenado por Decreto Nº 438/92, y sus modificatorias y por el artículo 3 del Decreto Nº 355 del 22 de mayo de 2017 y su modificatorio Decreto Nº 859 de fecha 26 de septiembre de 2018.

Por ello,

LA MINISTRA DE SALUD
RESUELVE:

ARTÍCULO 1º - Desígnanse en la planta permanente a las personas que se detallan en el Anexo I (IF-2021-119533252-APN-DACMYSG#ANLIS) y en el Anexo II (IF-2021-117433407-APN-DACMYSG#ANLIS), que forman parte integrante de la presente Resolución en el Agrupamiento y Nivel del SISTEMA NACIONAL DE EMPLEO PÚBLICO (SINEP), homologado por el Decreto Nº 2098/08 sus modificatorios y complementarios, en el cargo concursado en el Instituto o dependencia de la ADMINISTRACIÓN NACIONAL DE LABORATORIOS E INSTITUTOS DE SALUD "DR. CARLOS G. MALBRÁN" (ANLIS), organismo descentralizado que funciona en la órbita del MINISTERIO DE SALUD, que en cada caso se indica.

ARTÍCULO 2º - El gasto que demande el cumplimiento de la presente medida será atendido con cargo a las partidas específicas del presupuesto vigente de la Jurisdicción 80 - Entidad 906 – ADMINISTRACIÓN NACIONAL DE LABORATORIOS E INSTITUTOS DE SALUD "DR. CARLOS G. MALBRÁN" (ANLIS), organismo descentralizado que funciona en la órbita de la del MINISTERIO DE SALUD.

ARTÍCULO 3º - Comuníquese, dése a la DIRECCIÓN NACIONAL DEL REGISTRO OFICIAL para su publicación y archívese.

Carla Vizzotti

NOTA: El/los Anexo/s que integra/n este(a) Resolución se publican en la edición web del BORA -www.boletinoficial.gob.ar-

e. 15/02/2022 N° 7001/22 v. 15/02/2022

MINISTERIO DE SEGURIDAD

Resolución 75/2022

RESOL-2022-75-APN-MSG

Ciudad de Buenos Aires, 10/02/2022

VISTO el Expediente N° EX-2022-01773043- -APN-UGA#MSG del registro del MINISTERIO DE SEGURIDAD, la Ley de Ministerios Nº 22.520 (t.o. Decreto N° 438 del 12 de marzo de 1992) y sus modificatorias, la Ley de Seguridad Interior N° 24.059, la Decisión Administrativa N° 335 del 6 de marzo de 2020, y,

CONSIDERANDO:

Que la Ley Nº 22.520 de Ministerios (T.O Decreto N° 438/92) y sus modificatorias asignan al MINISTERIO DE SEGURIDAD la facultad de entender en la determinación de la política criminal y en la elaboración de planes

y programas para su aplicación, así como para la prevención del delito; procurando garantizar el derecho a la seguridad de los habitantes del país a través de la prevención del delito, la investigación del crimen organizado, la respuesta efectiva ante el delito complejo y el cuidado de todas las personas que habitan la República Argentina.

Que mediante Resolución Nº 977/2019 se aprobó el Plan Federal de Prevención de Delitos Tecnológicos y Ciberdelitos, que establece los lineamientos y prioridades de las políticas públicas relacionadas con las responsabilidades referentes al ciberespacio y su impacto en la Seguridad Nacional, llevando adelante las acciones de fomento de capacidades, entre otros, sobre la base de la coordinación y cooperación entre los organismos del sector público, 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 REPÚBLICA ARGENTINA ha adherido.

Que asimismo, la Resolución N° 829/2019 del 24 de mayo de 2019 de la SECRETARÍA DE GOBIERNO DE MODERNIZACIÓN de la JEFATURA DE GABINETE DE MINISTROS aprueba la ESTRATEGIA NACIONAL DE CIBERSEGURIDAD cuya finalidad es brindar un contexto seguro para el aprovechamiento del Ciberespacio por parte de los ciudadanos y organizaciones públicas y privadas, desarrollando de forma coherente y estructurada, acciones de prevención, detección, respuesta y recuperación frente a las ciberamenazas, conjuntamente con el desarrollo de un marco normativo acorde.

Que la esencia global del ciberespacio ofrece innumerables posibilidades en vista al desarrollo humano, conllevando en las mismas oportunidades, riesgos y amenazas a los usuarios, ya sean individuales o colectivos, y a la seguridad integral de las actividades de las naciones. Los riesgos intentan ser aprovechados tanto por las organizaciones criminales trasnacionales, nacionales como por delincuentes individuales.

Que esta situación se ha magnificado durante los años 2020 y 2021 producto de los cambios sociales y culturales que fueron ocurriendo en la sociedad a partir del brote infeccioso por Coronavirus (COVID-19) y las distintas medidas que los gobiernos, empresas y ciudadanos debieron adoptar para prevenir y dar una respuesta a la pandemia, tratando de disminuir el impacto a sus responsabilidades laborales como sociales.

Que la delincuencia, en forma individual u operando en forma organizada bajo esquemas criminales complejos, utilizaron a su favor la transnacionalidad que implica el ciberespacio generándose un crecimiento exponencial de los ciberdelitos. En tal sentido, los vacíos y atrasos legales de las diferentes jurisdicciones, la dificultad que provino de la ampliación de servicios digitales aumentando la superficie de ataque en todos los sectores que debieron adaptarse a la nueva normalidad, la escasa oferta de formación sobre investigación de delitos de altas tecnologías, entre otros factores, incrementaron la cantidad de hechos y, por ende, de víctimas a nivel global.

Que el Comité Interamericano contra el Terrorismo (CICTE) de la Organización de Estados Americanos -OEA- lleva adelante el programa de ciberseguridad por el cual brinda apoyo en el desarrollo e implementación de políticas y estrategias en la materia, el fortalecimiento de capacidades y la generación de conocimiento y difusión sobre el tema.

Que el “Reporte de Ciberseguridad 2020. Riesgos, avances y el camino a seguir en América Latina y el Caribe”, elaborado por el BANCO INTERAMERICANO DE DESARROLLO -BID- y la OEA sostiene que “EL INFORME DE CIBERCRIMEN THREATMETRIX” identificó a América Latina como un foco para el fraude en la creación de cuentas, con alrededor del 20% del volumen total mundial de nuevos usuarios.

Que, además, en el informe precitado se aplica el “Modelo de Madurez de la Capacidad de la Ciberseguridad para las Naciones” creado por el CENTRO GLOBAL DE CAPACIDAD EN SEGURIDAD CIBERNÉTICA (GCSCC,) por sus siglas en inglés) de la Universidad de Oxford en consulta con más de 200 expertos internacionales provenientes de gobiernos, la sociedad civil y la academia, que tiene por objeto evaluar el nivel de madurez de las capacidades en ciberseguridad de un país y tiene 5 etapas, a saber: Inicial, Formativa, Consolidada, Estratégica y Dinámica. De la observación de los indicadores propuestos se evidencia la necesidad que existe en el país de profundizar en políticas públicas y acciones que fortalezcan la seguridad de los habitantes en el ciberespacio.

Que a partir del mejoramiento continuo y las lecciones aprendidas, derivadas de la realidad antes descripta, se hace indispensable la revisión y actualización del “Plan Federal de Prevención de Delitos Tecnológicos (2019 - 2023)” que fuera aprobado por Resolución del Ministerio de Seguridad N° 977/2019.

Que resulta oportuno ampliar su vigencia hasta el año 2024 en pos de dar continuidad a las acciones emprendidas en el marco del mismo, pero a su vez, modificar determinadas líneas de acción político-estratégicas en pos de brindar respuestas adecuadas a una nueva realidad mundial a partir de la irrupción de la pandemia provocada por el virus COVID-19.

Que la actualización y reformulación del Plan Federal permite trazar los lineamientos estratégicos transversales a la temática mencionada, teniendo como objetivo central incrementar la protección de los ciudadanos y ciudadanas contra la delincuencia. La finalidad de las acciones a llevar adelante podrá ser cumplimentada en la medida que se procure reducir las amenazas existentes, fortalecer la ciberseguridad, capacitar y concientizar sobre nuevas

modalidades de los cibercriminales, incrementar las herramientas de investigación sobre los ciberdelitos y delitos tecnológicos, mitigar las consecuencias de los incidentes a través de estos medios.

Que por su parte, resulta necesario reforzar la visión integral de la medida en pos de otorgarle una mayor transversalidad y en orden a ello, se propicia asignar a la UNIDAD DE GABINETE DE ASESORES, a través de la instancia que su Titular disponga, la facultad de coordinar la política estratégica ínsita en los lineamientos del Plan.

Que lo anteriormente expuesto, es sin perjuicio de las áreas con funciones operativas, a las que se instruye a colaborar en lo que resulte necesario a los efectos de cumplir con los objetivos estratégicos planteados.

Que por su parte, es fundamental lograr una mayor articulación federal para dar una respuesta efectiva contra las diversas modalidades delictivas locales.

Que la SECRETARÍA DE SEGURIDAD Y POLÍTICA CRIMINAL a través de sus áreas técnicas competentes ha tomado intervención, dando conformidad a la presente medida.

Que la DIRECCIÓN GENERAL DE ASUNTOS JURÍDICOS de este ministerio ha tomado la intervención que le corresponde.

Que la presente medida se dicta en virtud del artículo 22 bis de la Ley de Ministerios Nº 22.520 (T.O Decreto N° 438/92) y sus modificatorias.

Por ello,

EL MINISTRO DE SEGURIDAD
RESUELVE:

ARTÍCULO 1°. – Aprúebase la actualización del “PLAN FEDERAL DE PREVENCIÓN DE DELITOS TECNOLÓGICOS Y CIBERDELITOS (2021 - 2024)” que, como Anexo (IF-2022-05822603-APN-UGA#MSG), forma parte integrante de la presente medida.

ARTÍCULO 2°. – Déjase establecido que la UNIDAD DE GABINETE DE ASESORES, a través de las instancias que su Titular disponga, llevará adelante la coordinación de la política estratégica del “PLAN FEDERAL DE PREVENCIÓN DE DELITOS TECNOLÓGICOS Y CIBERDELITOS (2021 - 2024)” y para tales fines articulará todas las acciones y medios necesarios a fin de lograr una implementación transversal de los lineamientos formulados.

ARTÍCULO 3°. – Instrúyase a las áreas con competencia en la materia del Ministerio y de las Fuerzas de Policiales y de Seguridad, a colaborar y participar en aquellas acciones y medidas que resulten necesarias para lograr la sinergia necesaria que conlleva el cometido previsto en el Plan.

ARTICULO 4°.- Invítase a las provincias, a la Ciudad Autónoma de Buenos Aires y a los municipios a adherir al “PLAN FEDERAL DE PREVENCIÓN DE DELITOS TECNOLÓGICOS Y CIBERDELITOS (2021– 2024)”.

ARTÍCULO 5°. – Deróguese la Resolución Nº 977/2019.

ARTÍCULO 6º.- Comuníquese, publíquese, dese a la DIRECCIÓN NACIONAL DEL REGISTRO OFICIAL y archívese.

Aníbal Domingo Fernández

NOTA: El/los Anexo/s que integra/n este(a) Resolución se publican en la edición web del BORA -www.boletinoficial.gob.ar-

e. 15/02/2022 N° 7159/22 v. 15/02/2022

MINISTERIO DE SEGURIDAD

Resolución 86/2022

RESOL-2022-86-APN-MSG

Ciudad de Buenos Aires, 11/02/2022

Visto el expediente EX-2022-01780105- -APN-UGA#MSG del registro del MINISTERIO DE SEGURIDAD, la Ley de Ministerios Nº 22.520 (t.o. Decreto N° 438 del 12 de marzo de 1992) y sus modificatorias, la Ley de Seguridad Interior N° 24.059, la Decisión Administrativa N° 335 del 6 de marzo de 2020 y la Resolución Nº 75 de fecha 10 de febrero de 2022 de este Ministerio de Seguridad (Plan Federal de Prevención de Delitos Tecnológicos y Ciberdelitos), y

CONSIDERANDO

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

modalidades de los cibercriminales, incrementar las herramientas de investigación sobre los ciberdelitos y delitos tecnológicos, mitigar las consecuencias de los incidentes a través de estos medios.

Que por su parte, resulta necesario reforzar la visión integral de la medida en pos de otorgarle una mayor transversalidad y en orden a ello, se propicia asignar a la UNIDAD DE GABINETE DE ASESORES, a través de la instancia que su Titular disponga, la facultad de coordinar la política estratégica ínsita en los lineamientos del Plan.

Que lo anteriormente expuesto, es sin perjuicio de las áreas con funciones operativas, a las que se instruye a colaborar en lo que resulte necesario a los efectos de cumplir con los objetivos estratégicos planteados.

Que por su parte, es fundamental lograr una mayor articulación federal para dar una respuesta efectiva contra las diversas modalidades delictivas locales.

Que la SECRETARÍA DE SEGURIDAD Y POLÍTICA CRIMINAL a través de sus áreas técnicas competentes ha tomado intervención, dando conformidad a la presente medida.

Que la DIRECCIÓN GENERAL DE ASUNTOS JURÍDICOS de este ministerio ha tomado la intervención que le corresponde.

Que la presente medida se dicta en virtud del artículo 22 bis de la Ley de Ministerios Nº 22.520 (T.O Decreto N° 438/92) y sus modificatorias.

Por ello,

EL MINISTRO DE SEGURIDAD
RESUELVE:

ARTÍCULO 1°. – Aprúebase la actualización del “PLAN FEDERAL DE PREVENCIÓN DE DELITOS TECNOLÓGICOS Y CIBERDELITOS (2021 - 2024)” que, como Anexo (IF-2022-05822603-APN-UGA#MSG), forma parte integrante de la presente medida.

ARTÍCULO 2°. – Déjase establecido que la UNIDAD DE GABINETE DE ASESORES, a través de las instancias que su Titular disponga, llevará adelante la coordinación de la política estratégica del “PLAN FEDERAL DE PREVENCIÓN DE DELITOS TECNOLÓGICOS Y CIBERDELITOS (2021 - 2024)” y para tales fines articulará todas las acciones y medios necesarios a fin de lograr una implementación transversal de los lineamientos formulados.

ARTÍCULO 3°. – Instrúyase a las áreas con competencia en la materia del Ministerio y de las Fuerzas de Policiales y de Seguridad, a colaborar y participar en aquellas acciones y medidas que resulten necesarias para lograr la sinergia necesaria que conlleva el cometido previsto en el Plan.

ARTICULO 4°.- Invítase a las provincias, a la Ciudad Autónoma de Buenos Aires y a los municipios a adherir al “PLAN FEDERAL DE PREVENCIÓN DE DELITOS TECNOLÓGICOS Y CIBERDELITOS (2021– 2024)”.

ARTÍCULO 5°. – Deróguese la Resolución Nº 977/2019.

ARTÍCULO 6º.- Comuníquese, publíquese, dese a la DIRECCIÓN NACIONAL DEL REGISTRO OFICIAL y archívese.

Aníbal Domingo Fernández

NOTA: El/los Anexo/s que integra/n este(a) Resolución se publican en la edición web del BORA -www.boletinoficial.gob.ar-

e. 15/02/2022 N° 7159/22 v. 15/02/2022

MINISTERIO DE SEGURIDAD

Resolución 86/2022

RESOL-2022-86-APN-MSG

Ciudad de Buenos Aires, 11/02/2022

Visto el expediente EX-2022-01780105- -APN-UGA#MSG del registro del MINISTERIO DE SEGURIDAD, la Ley de Ministerios Nº 22.520 (t.o. Decreto N° 438 del 12 de marzo de 1992) y sus modificatorias, la Ley de Seguridad Interior N° 24.059, la Decisión Administrativa N° 335 del 6 de marzo de 2020 y la Resolución Nº 75 de fecha 10 de febrero de 2022 de este Ministerio de Seguridad (Plan Federal de Prevención de Delitos Tecnológicos y Ciberdelitos), y

CONSIDERANDO

Que la Ley N° 22.520 de Ministerios (T.O Decreto N° 438/92) y sus modificatorias asignan al MINISTERIO DE SEGURIDAD la facultad de entender en la determinación de la política criminal y en la elaboración de planes y programas para su aplicación, así como para la prevención del delito; procurando garantizar el derecho a la seguridad de los habitantes del país a través de la prevención del delito, la investigación del crimen organizado, la respuesta efectiva ante el delito complejo y el cuidado de todas las personas que habitan la República Argentina;

Que la Ley Nº 24.059 establece las bases jurídicas, orgánicas y funcionales del sistema de planificación, coordinación, control y apoyo del esfuerzo nacional de policía tendiente a garantizar la seguridad interior.

Que el artículo 2° de la ley precitada define a la seguridad interior como "la situación de hecho basada en el derecho en la cual se encuentran resguardadas la libertad, la vida y el patrimonio de los habitantes, sus derechos y garantías y la plena vigencia de las instituciones del sistema representativo, republicano y federal que establece la Constitución Nacional" y el artículo 8° asigna el ejercicio de la conducción política del esfuerzo nacional de policía al MINISTERIO DE SEGURIDAD.

Que en virtud del artículo 8º de la Ley Nº 24.059 de Seguridad Interior se establece en cabeza del MINISTRO DE SEGURIDAD por delegación del PRESIDENTE DE LA NACIÓN, además de las competencias que le son otorgadas en la Ley de Ministerios Nº 22.520, la facultad de ejercer la conducción política del esfuerzo nacional de policía; la coordinación del accionar de los referidos cuerpos y fuerzas entre sí y con los cuerpos policiales provinciales y la dirección superior de los cuerpos policiales y fuerzas de seguridad del Estado nacional a los fines derivados de la seguridad interior.

Que, asimismo, para el cumplimiento de sus objetivos, la precitada Ley le asignó la facultad de formular las políticas correspondientes al ámbito de la seguridad interior, y elaborar la doctrina y planes y conducir las acciones tendientes a garantizar un adecuado nivel de seguridad interior, con el asesoramiento del Consejo de Seguridad Interior.

Que, por su parte, también le otorgó la facultad de dirigir y coordinar la actividad de los órganos de información e inteligencia de la Policía Federal Argentina y de la Policía de Seguridad Aeroportuaria; como también de los pertenecientes a Gendarmería Nacional Argentina y Prefectura Naval Argentina, en estos últimos casos exclusivamente a los efectos concernientes a la seguridad interior.

Que en lo que a la presente medida concierne, resulta fundamental señalar que la Ley Nº 24.059 en el artículo 8º ya citado, facultó al MINISTERIO DE SEGURIDAD a entender en la determinación, entre otros aspectos allí citados, de la capacitación de la Policía Federal Argentina y Policía de Seguridad Aeroportuaria; e intervenir en dichos aspectos con relación a Gendarmería Nacional y Prefectura Naval Argentina, en estos últimos casos exclusivamente a los fines establecidos en la mencionada Ley.

Que la Policía Federal Argentina tiene por función prevenir los delitos de competencia de la justicia federal, así como practicar las diligencias para asegurar su prueba, descubrir a los autores y partícipes, y entregarlos a la Justicia, con los deberes y atribuciones que a la policía confiere el Código de Procedimientos en lo Criminal (art. 3°, Dto. Ley Nº 333/1958).

Por su parte, la Ley de Seguridad Aeroportuaria N° 26.102 y sus modificatorias, establece que corresponde a la Policía de Seguridad Aeroportuaria prevenir delitos e infracciones en el ámbito aeroportuario, llevando a cabo las acciones tendientes a impedirlos, evitarlos, obstaculizarlos o limitarlos (arts. 12° y 13º).

Que Ley de Gendarmería Nacional Argentina N° 19.349 y sus modificatorias determina que dicha fuerza de seguridad tiene la función de prevenir delitos e infracciones, poseyendo, para ello, funciones de policía de prevención en su respectiva jurisdicción (arts. 2° y 3º)

Que la Ley General de la Prefectura Naval Argentina N° 18.398 y sus modificatorias, prescribe que tiene por función prevenir la comisión de delitos y contravenciones (art. 5°, inc. c], ap. 3°)

Que como se ha previsto en el Anexo del "Plan Federal de Prevención de Delitos Tecnológicos (2021 - 2024)" aprobado mediante la Resolución Nº 75 de fecha 10 de febrero de 2022 el "ciberdelito", se encuentra comprendido por los delitos ciberasistidos, entendido como aquellas conductas que ya se encuentra tipificadas en nuestro ordenamiento y cuya planificación, organización, ejecución o resultado se encuentran utilizando el ciberespacio para lograr su fin ilícito, y los delitos ciberdependientes, como aquellos delitos realizados únicamente por medio y/o a través de las tecnologías de la información y comunicación (TIC´s) haciendo que éstos necesiten del ciberespacio para su existencia.

Que lo ciberdelitos mencionados, son una manifestación delictiva en expansión que afecta cada día a más cantidad de personas físicas y jurídicas, economías, sistemas, servicios, infraestructuras críticas, y en consecuencia es necesario generar mecanismos coordinados y proactivos para la investigación por parte de las fuerzas policiales y de seguridad federales.

Que la UNODOC - Oficina de las Naciones Unidas contra la Droga y el Delito, establece que La ciberdelincuencia es un acto que infringe la ley y que se comete usando las tecnologías de la información y la comunicación (TIC) para atacar las redes, sistemas, datos, sitios web y la tecnología o para facilitar un delito. Asimismo, indica que, la ciberdelincuencia se diferencia de los delitos comunes en que «no tiene barreras físicas o geográficas» [y se puede cometer con menos esfuerzo y más facilidad y velocidad que los delitos comunes

Qué asimismo, la Agencia de la Unión Europea para la Cooperación Policial (EUROPOL) considera que el ciberdelito es todo delito que solo se puede cometer usando computadoras, redes computarizadas u otras formas de tecnologías de la información y comunicación y delitos propiciados por los medios informáticos (es decir, delitos comunes facilitados por Internet y las tecnologías digitales). Indicando, de igual manera, que la distinción principal entre estas categorías de ciberdelincuencia es el papel de las TIC en el delito, ya sea como el objetivo del delito o como parte del modus operandi.

Que con fecha 4 de junio de 2008, se dictó la ley Nº 26.388 de delitos informáticos (modificatoria del Código Penal) a fin de incorporar las modalidades delictivas vinculadas con los Delitos Tecnológicos y Ciberdelitos.

Que la norma citada tipifica como delitos e incorpora al Código Penal varias conductas relacionadas con el uso de las nuevas tecnologías que, de acuerdo a la doctrina especializada en la materia pueden clasificarse en: a) Daño informático, agregándose en el artículo 183 del CP como segundo párrafo; b) Fraude informático, incorporando el inciso 16) al artículo 173 del CP; c) Alteración de pruebas, sustituyendo el artículo 255 del CP; d) Pornografía infantil, sustituyendo el artículo 128 del CP; e) Delitos contra la privacidad: en primer lugar, la ley 26388 modifica el epígrafe del Capítulo III, del Título V, del Libro II del CP por el siguiente: "Violación de Secretos y de la Privacidad"; f) Delitos contra la seguridad pública e interrupción de las comunicaciones: en relación con este delito se sustituye el artículo 197 del CP; g) Falsificación de documentos electrónicos: en este caso se incorporan como últimos párrafos del artículo 77 del CP (conf. (FERNÁNDEZ DELPECH, H. Manual de Derecho Informático – Ed. Abeledo Perrot – Bs. As. 2014 páginas 197/213).

Que la Ley N° 27.411, publicada en el Boletín Oficial con fecha 15 de diciembre de 2017, aprobó el CONVENIO SOBRE CIBERCRIMINALIDAD del CONSEJO DE EUROPA previamente citado, adoptado en la Ciudad de BUDAPEST, HUNGRÍA, el 23 de noviembre de 2001, el cual tiene por objeto la prevención de los actos atentatorios de la confidencialidad, la integridad y la disponibilidad de los sistemas informáticos, de las redes y de los datos, así como el uso fraudulento de tales sistemas, redes y datos, asegurando la incriminación de dichos comportamientos, y la atribución de poderes suficientes para permitir una lucha eficaz contra estas infracciones penales, facilitando su detección. Además, busca garantizar un equilibrio adecuado respeto de los derechos fundamentales del hombre, como los garantizados en el Pacto internacional relativo a los derechos civiles y políticos de las Naciones Unidas (1966), así como en otros convenios internacionales aplicables en materia de derechos del hombre, que reafirman el derecho de no ser perseguido por su opinión, el derecho a la libertad de expresión, incluida la libertad de buscar, obtener y comunicar informaciones e ideas de toda naturaleza, sin consideración de fronteras, así como el derecho al respeto de la vida privada.

Que se pueden identificar distintos tipos de ciberdelincuentes, entre los cuales 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 complejas asociadas con el fin 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 y continua a través de múltiples vectores de ataque, y de forma sostenible en el tiempo, un objetivo estratégico determinado sea este una empresa, una infraestructura crítica o un Estado.

Que las personas que incurren en este tipo de conductas presuntamente delictivas utilizan, entre otros artefactos, software malicioso con el que infectan equipos sin el conocimiento de sus usuarios, pudiendo retransmitir toda clase de amenazas digitales que pueden tener por misión obtener el control remoto ilícito de los dispositivos, pueden robar contraseñas y deshabilitar la protección antivirus; pueden crear "puertas traseras" a los efectos de acceder sin autorización a la propiedad y la información de los usuarios; pueden utilizar vulnerabilidades de los sistemas o componentes del mismo para lograr su acceso ilegal, pueden crear y utilizar foros en línea para comerciar con artículos ilícitos así como con acciones de piratería informática; así como realizar actividades de lavado de dinero y cometer fraudes en línea; entre otros muchos fines ilícitos.

Que a nivel internacional se observa que la ciberdelincuencia y los delitos tecnológicos cobran mayor relevancia y en consecuencia organismos internacionales, regionales y los países adoptan medidas para prevenirlo e investigarlo.

Que INTERPOL ha expresado la necesidad de dejar de identificar al ciberespacio como un espacio no tangible, porque todas las consecuencias repercuten en aspectos económicos, sociales, psicológicos de las víctimas, y en su realidad, en sus decisiones, en sus patrimonios y familias.

Que, en ese orden de ideas, la Alta Representante de la ORGANIZACIÓN DE LAS NACIONES UNIDAS (ONU) para Asuntos de Desarme, Izumi Nakamitsu, durante una reunión informal del Consejo de Seguridad en mayo del año 2020 ha señalado sobre el crecimiento exponencial de la ciberdelincuencia detectándosek, un aumento del 600 % en los correos electrónicos maliciosos durante la crisis y ataques contra organizaciones sanitarias e instalaciones de investigación médica en distintos países.

Que asimismo en Abril del año 2021, los Estados Miembros de la ORGANIZACIÓN DE LAS NACIONES UNIDAS (ONU) presentaron, a través del informe de la Reunión de Grupos de Expertos encargado de realizar un estudio exhaustivo del delito cibernético, una serie de recomendaciones y conclusiones entre las que se encuentran: "…g) Los países deberían destinar recursos a generar los conocimientos especializados necesarios para investigar la ciberdelincuencia y establecer alianzas que se valgan de mecanismos de cooperación para obtener pruebas vitales; h) Los Estados Miembros deberían seguir esforzándose por crear y apoyar dependencias, órganos y estructuras especializados en ciberdelincuencia en las fuerzas del orden, el ministerio público y la judicatura, dotándolos de los conocimientos especializados y el equipo necesarios para hacer frente a los retos que plantean esos delitos y para reunir, compartir y utilizar pruebas electrónicas en las actuaciones penales; (…) s) Los Estados deberían reforzar las actividades de investigación y aplicación de la ley relacionadas con los actos de asociación, complicidad y preparación para cometer delitos cibernéticos con miras a afrontar eficazmente toda la cadena de la ciberdelincuencia; t) Los Estados deberían seguir reforzando la creación de capacidad y mejorando la capacidad de las autoridades judiciales y las fuerzas del orden para investigar y perseguir los delitos cibernéticos. En las actividades de creación de capacidad se debería hacer hincapié en los problemas cada vez mayores que plantean la computación en la nube, la web oscura y otras tecnologías emergentes. También se alienta a los Estados a que presten asistencia para el fomento de la capacidad a los países en desarrollo".

Que, a nivel internacional, varias naciones e instituciones intergubernamentales llevan adelante mecanismos de coordinación para denunciar e investigar presuntas actividades delictivas facilitadas por Internet.

Que a modo de ejemplo de lo establecido en el acápite anterior se puede enunciar que EUROPOL creó en el año 2013 el Centro Europeo de Ciberdelincuencia (C3) a los efectos de reforzar la respuesta policial a la ciberdelincuencia y, en el año 2014, creó el Grupo de trabajo conjunto de acción contra el Ciberdelito (J – CAT) que tiene por objeto impulsar acciones coordinadas abordando los delitos ciberdependientes, fraudes de pago trasnacional, explotación sexual infantil en línea y facilitadores cibernéticos de otros delitos; en la órbita del Buró Federal de Investigaciones funciona el Centro de Denuncias de Delitos en Internet (IC3 por su sigla en Inglés) que tiene por función investigar presuntos delitos; Que en el año 2020 INTERPOL mostró un aumento alarmante de los ciberataques durante la epidemia de COVID-19, indicando Jürgen Stock, Secretario General de INTERPOL, que a partir del Covid – 19, los ciberdelincuentes crearon nuevos ataques e intensificando su ejecución a un ritmo alarmante, aprovechándose del miedo y la incertidumbre provocados por la inestabilidad de la situación socioeconómica generada.

Asimismo, durante el mes de octubre de 2021, la Oficina Federal para la Seguridad en la Tecnología de la Información (BSI) de Alemania, el organismo gubernamental responsable de la seguridad de las tecnologías de la información, ha advertido de que se ha alcanzado el nivel de alarma máximo en algunas áreas, ya que los ciberdelincuentes son cada vez más profesionales en sus en sus métodos, mientras que la sociedad está cada vez más conectada digitalmente, razón por la cual considera que Alemania está bajo una amenaza de ciberataques de "tensa a crítica"

Que en la órbita de este Ministerio se dictaron diversas reglamentaciones, así puede mencionarse la Resolución Nº 1107-E/2017 mediante la cual se creó el Comité de Respuesta de Incidentes de Seguridad Informática del MINISTERIO DE SEGURIDAD (CSIRT), cuyo objetivo principal era la coordinación de las actuaciones centralizadas ante usos nocivos y/o ilícitos de las infraestructuras tecnológicas, las redes y los sistemas de información y de telecomunicaciones del Ministerio y sus órganos dependientes

Que asimismo por Resolución Nº 977/2019 se aprobó el Plan Federal de Prevención de Delitos Tecnológicos y Ciberdelitos, que establece los lineamientos y prioridades de las políticas públicas relacionadas con las responsabilidades referentes al ciberespacio y su impacto en la Seguridad Nacional, llevando adelante las acciones de fomento de capacidades, entre otros, sobre la base de la coordinación y cooperación entre los organismos del sector público, 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 REPÚBLICA ARGENTINA ha adherido.

Que por Disposición Nº 655/2020, de la Subsecretaria de Investigación Criminal y Cooperación Judicial del MINISTERIO DE SEGURIDAD se creó, en el ámbito de la Dirección de Investigaciones del Ciberdelito, la Comisión Asesora en Materia de Lucha Contra el Ciberdelito con carácter ad honorem, para el seguimiento de la implementación de las iniciativas incorporadas al Plan Federal de Prevención de Delitos Tecnológicos y Ciberdelitos (2019 – 2023).

Que el Plan aprobado mediante la Resolución Nº 977/19 fue actualizado por Resolución de este Ministerio de Seguridad Nº 75/2022, extendiéndose su vigencia hasta el 2024.

Que los desafíos que se plantean a nivel mundial requieren acciones focalizadas y sostenidas, orientadas estratégicamente a afrontar las problemáticas inherentes a las conductas ilícitas relacionadas con los delitos informáticos de manera integral y con un fuerte sentido preventivo.

Que, por su parte, se pone de manifiesto especialmente la necesidad de contar con recursos humanos especializados, entrenados y capaces de brindar respuestas adecuadas y eficientes, así como también la infraestructura tecnológica necesaria para afrontar los flagelos descriptos.

Que, en orden a ello, resulta necesario poner a disposición de las fuerzas policiales y de seguridad federales herramientas de formación, capacitación e investigación en la materia, de manera tal que las brechas existentes entre el accionar ilícito y las respuestas por parte del Estado en cuanto a garantizar la seguridad interior.

Que en orden a lo expuesto, se propicia la creación del "PROGRAMA DE FORTALECIMIENTO EN CIBERSEGURIDAD Y EN INVESTIGACION DEL CIBERCRIMEN (ForCIC)" cuyo objetivo es coordinar, asistir y brindar asesoramiento en técnicas investigativas en materia de ciberdelitos y/o delitos con presencia de la tecnología y/o utilización de tecnologías.

Que participará en la ejecución del mencionado Programa el personal de las fuerzas policiales y de seguridad federales que a tal efecto se asigne, que se encuentren capacitados o se capaciten al efecto, en la investigación criminal de estas modalidades delictivas.

Que a fin de llevar adelante los cometidos del Programa se instruye a las áreas que pudieran tener injerencia en la materia conforme las competencias asignadas normativamente, a colaborar y a facilitar todas las instancias necesarias para el fortalecimiento de la presente iniciativa.

Que asimismo, con el propósito de garantizar la mirada integral y una marcada impronta federal a la medida, se invitará a las autoridades competentes de las provincias y de la Ciudad Autónoma de Buenos Aires a participar de las acciones que se lleven adelante incluyendo, pero no limitándose, a la realización de capacitaciones y otras acciones formativas que resulten necesarias.

Que la presente medida se dicta en uso de las atribuciones conferidas por los artículos 4°, inciso b, apartado 9° y 22° bis de la Ley Nº 22.520 de Ministerios (t.o 1992) y sus modificatorias.

Por ello,

EL MINISTRO DE SEGURIDAD
RESUELVE:

ARTÍCULO 1°. Créase en el ámbito de la UNIDAD DE GABINETE DE ASESORES del MINISTERIO DE SEGURIDAD, el "PROGRAMA DE FORTALECIMIENTO EN CIBERSEGURIDAD Y EN INVESTIGACION DEL CIBERCRIMEN (ForCIC)" que tendrá como objetivo coordinar, asistir y brindar asesoramiento en técnicas de seguridad de las infraestructuras digitales y en técnicas de investigación en materia de ciberdelitos y delitos con presencia de la tecnología y/o utilización de tecnologías.

ARTÍCULO 2°. Los lineamientos, normas aclaratorias y la evaluación estratégica del "PROGRAMA DE FORTALECIMIENTO EN CIBERSEGURIDAD Y EN INVESTIGACION DEL CIBERCRIMEN (ForCIC)" estará a cargo de la UNIDAD DE GABINETE DE ASESORES del MINISTERIO DE SEGURIDAD.

ARTÍCULO 3°. Apruébanse los objetivos y acciones del "PROGRAMA DE FORTALECIMIENTO EN CIBERSEGURIDAD Y EN INVESTIGACION DEL CIBERCRIMEN (ForCIC)" establecidas en el Anexo Único (IF-2022-05822510-APN-UGA#MSG) que forma parte integrante de la presente Resolución.

ARTÍCULO 4°. El "PROGRAMA DE FORTALECIMIENTO EN CIBERSEGURIDAD Y EN INVESTIGACION DEL CIBERCRIMEN (ForCIC)" estará a cargo de un Responsable que reportará en forma directa al Titular de la UNIDAD DE GABINETE DE ASESORES del MINISTERIO DE SEGURIDAD y será designado a propuesta de dicho funcionario.

ARTÍCULO 5°. Déjese establecido que las acciones derivadas del COMITÉ DE RESPUESTA DE INCIDENTES DE SEGURIDAD INFORMÁTICA (CSIRT) y de la COMISIÓN ASESORA EN MATERIA DE LUCHA CONTRA EL CIBERDELITO de este Ministerio o aquellas instancias que en el futuro las reemplacen, se enmarcan dentro del programa que se aprueba por la presente Resolución y sujetas a la coordinación del Responsable de Programa.

ARTICULO 6°. Instrúyase a las unidades orgánicas de este Ministerio y a las fuerzas policiales y de seguridad nacionales que tengan o pudieran tener injerencia en la materia, conforme las competencias asignadas normativamente, a prestar colaboración y a facilitar las instancias necesarias para el fortalecimiento del Programa y el adecuado cumplimiento de sus objetivos.

ARTICULO 7°. Invítase a las policías provinciales y de la Ciudad Autónoma de Buenos Aires a participar del presente Programa a través de su adhesión.

Artículo 8°. Instrúyese a la SECRETARÍA DE COORDINACIÓN, BIENESTAR, CONTROL Y TRANSPARENCIA INSTITUCIONAL a arbitrar los medios necesarios para atender los gastos que demande la ejecución del programa que se aprueba por la presente Resolución.

ARTICULO 9º. La presente medida entrará en vigor a partir de su publicación en el Boletín Oficial de la República Argentina.

ARTICULO 10. Comuníquese, publíquese, dese a la DIRECCIÓN NACIONAL DE REGISTRO OFICIAL y archívese.

Aníbal Domingo Fernández

NOTA: El/los Anexo/s que integra/n este(a) Resolución se publican en la edición web del BORA -www.boletinoficial.gob.ar-

e. 15/02/2022 N° 7209/22 v. 15/02/2022

MINISTERIO DE TRABAJO, EMPLEO Y SEGURIDAD SOCIAL

Resolución 100/2022

RESOL-2022-100-APN-MT

Ciudad de Buenos Aires, 10/02/2022

VISTO el EX-2022-09959846- -APN-DGD#MT, el Decreto N° 2136 de fecha 30 de diciembre de 1974, la Resolución del MINISTERIO DE TRABAJO, EMPLEO Y SEGURIDAD SOCIAL N° 897 de fecha 7 de septiembre de 2015, modificada por la Resolución del entonces MINISTERIO DE SALUD Y DESARROLLO SOCIAL Nº 164 de fecha 7 de marzo de 2019, y

CONSIDERANDO

Que el Decreto N° 2136/74 fue dictado de conformidad con lo dispuesto por el artículo 62 de la entonces vigente Ley N° 18.037 (T.O. 1974), norma por la cual se autorizaba al PODER EJECUTIVO NACIONAL a establecer regímenes que adecuaran los límites de edad y de años de servicio en relación con aquellas actividades que implicaran la realización de tareas penosas, riesgosas o determinantes de vejez o agotamiento prematuro.

Que, en ese marco, el Decreto N° 2136/74 estableció, en su artículo 1°, el derecho a la jubilación ordinaria con CINCUENTA (50) años de edad y VEINTICINCO (25) años de servicios para el personal que se desempeñe habitual y directamente en las siguientes actividades: a) en la exploración petrolífera o gasífera llevada a cabo en campaña y b) en tareas desempeñadas en boca de pozo y afectadas a la perforación, terminación, mantenimiento y reparación de pozos petrolíferos o gasíferos.

Que el MINISTERIO DE TRABAJO, EMPLEO Y SEGURIDAD SOCIAL emitió la Resolución Nº 897/15, en el entendimiento de considerar necesario y conveniente especificar las actividades y tareas que implican los procesos productivos de trabajo enunciados en el decreto arriba citado, y que, por tanto, quedan comprendidas en las disposiciones del referido régimen diferencial, y, asimismo, aclarar en forma precisa sus alcances, con las limitaciones y exclusiones que la propia norma establece.

Que, con posterioridad, mediante la Resolución del entonces MINISTERIO DE SALUD Y DESARROLLO SOCIAL Nº 164/19, se introdujeron modificaciones a la Resolución mencionada en el párrafo anterior con el objeto de contribuir al esclarecimiento y correcta aplicación del régimen diferencial, especialmente respecto de las tareas llevadas a cabo por el personal de apoyo y el que desarrolla actividades auxiliares o complementarias.

Que, es importante señalar que para que una tarea pueda ser encuadrada en el régimen del Decreto Nº 2136/74 debe reunir un conjunto de requisitos en forma concurrente, relativos a las características de las mismas, su vinculación y afectación directa con los procesos de explotación y exploración petrolífera y gasífera, el carácter penoso, riesgo o causante de envejecimiento prematuro y el lugar de desempeño.

Que a fin de brindar mayor certeza respecto de las tareas comprendidas en el régimen, se ha elaborado un nomenclador, de carácter enunciativo, con la familia de puestos comprendidos en el régimen diferencial del Decreto N° 2136/74, normas complementarias y aclaratorias, sin perjuicio de lo que en cada caso surja de los procesos de probatoria y verificación a cargo de la ADMINISTRACIÓN NACIONAL DE LA SEGURIDAD SOCIAL (ANSES), en el marco de sus competencias.

Que también, resulta necesario establecer procedimientos adecuados que permitan colectar elementos de probanza complementaria o supletoria de carácter fidedigno a fin de coadyuvar al análisis y encuadre legal de las

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 “PROGRAMA DE FORTALECIMIENTO EN CIBERSEGURIDAD Y EN INVESTIGACION DEL CIBERCRIMEN (ForCIC)” EX-2022-01780105- -APN-UGA#MSG

ANEXO ÚNICO

ARTÍCULO 1°: El “PROGRAMA DE FORTALECIMIENTO EN CIBERSEGURIDAD Y EN INVESTIGACION DEL CIBERCRIMEN (ForCIC)” tiene como objetivos los siguientes:

a) Incrementar las capacidades de prevención, detección y análisis de incidentes cibernéticos.

b) Incrementar las capacidades de prevención, detección e investigación del ciberdelito.

c) Incrementar la capacidad de respuesta en el marco de las actividades de investigación de las áreas específicas de ciberdelito dependientes de las fuerzas de seguridad y policiales.

d) Elaborar métricas específicas de la situación de ciberseguridad que puedan afectar las infraestructuras internas de la jurisdicción, así como las que pudieran ser de impacto en la seguridad nacional.

e) Elaborar métricas específicas de delitos ciberdependientes y ciberasistidos, de todo el Territorio Nacional.

f) Coordinar, asistir y/o brindar asesoramiento técnico para la realización de las investigaciones que, por su especificidad, complejidad y/o urgencia, le fueran requeridas.

g) Ejecutar todas las acciones conducentes y tendientes a la mejora y perfeccionamiento de las tareas de investigación de ciberdelitos y optimización de la ciberseguridad.

h) Instrumentar mecanismos de comunicación y concientización acerca de la temática referida a los incidentes cibernéticos y del ciberdelito en el ámbito nacional e internacional.

ARTÍCULO 2°: Para el cumplimiento de sus objetivos el “PROGRAMA DE FORTALECIMIENTO EN CIBERSEGURIDAD Y EN INVESTIGACION DEL CIBERCRIMEN (ForCIC)” llevará adelante las siguientes acciones:

a) Crear el “CENTRO DE INVESTIGACIÓN DE CIBERDELITOS DE ALTA TECNOLOGÍA (CICAT)” para la capacitación, prevención, análisis e investigación de ciberdelitos, el que abarcará áreas específicas de abordaje tales como: forencia digital; unidades regionales federales; entre otras.

b) Reorganizar y adecuar el funcionamiento del COMITÉ DE RESPUESTAS DE INCIDENTES DE SEGURIDAD INFORMÁTICA (CSIRT) para la prevención, detección y análisis de ataques e incidentes cibernéticos.

c) Crear el COMITÉ DE PRIORIZACIÓN DE RESPUESTA A INCIDENTES CIBERNÉTICOS (CoPRIC).

d) Poner en funcionamiento la Comisión Asesora en Materia de Lucha contra el Ciberdelito.

e) Fortalecer las capacidades de las áreas formativas en materia de ciberseguridad e investigaciones del ciberdelito del Ministerio de Seguridad y las Fuerzas Policiales y de Seguridad federales, provinciales y de la Ciudad Autónoma de Buenos Aires que se adhieran.

f) Impulsar Acuerdos de Colaboración y Cooperación con el sector público y/o privado, nacional e internacional.

g) Instar todas aquellas acciones y medidas que resulten necesarias a los efectos del cumplimiento de los objetivos del programa ForCIC.

José Lucas Gaincerain
Titular

Unidad Gabinete de Asesores
Ministerio de Seguridad