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 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 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 13°).

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 3°)

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