PODER EJECUTIVO
MINISTERIO DE TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIÓN

RESOLUCIÓN MITIC Nº 346 -

POR LA CUAL SE APRUEBA E IMPLEMENTA EL REGLAMENTO DE REPORTE OBLIGATORIO DE INCIDENTES CIBERNÉTICOS POR PARTE DE LOS ORGANISMOS Y ENTIDADES DEL ESTADO (OEE), AL EL MINISTERIO DE TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIÓN.----------

Asunción, 04 *de agosto de 2020*

VISTO: *La necesidad de reglamentar el artículo 7, numerales 4, 5, 13 y 23 de la Ley N° 6207/2018 "QUE CREA EL MINISTERIO DE TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIÓN Y ESTABLECE SU CARTA ORGÁNICA", así como los artículos 43 y 44 del Decreto N° 2274/2019, reglamentario de dicha ley, en lo concerniente a las políticas y facultades del Ministerio de Tecnologías de la Información y Comunicación ("MITIC") en materia de Ciberseguridad;----------*

El Dictamen DGAJ N° 115/2020 de fecha 22 de julio de 2020, de la Dirección General de Asesoría Jurídica de la Institución;----------

El Memorándum DG N° 445/2020 de fecha 30 de junio de 2020, de la Dirección de Gabinete del Viceministerio de Tecnologías de la Información y Comunicación de la Institución, por el cual se solicita la aprobación del reglamento de reportes obligatorios de incidentes cibernéticos por parte de los Organismos y Entidades del Estado (OEE) ante el Ministerio de Tecnologías de la Información y Comunicación; mediante la emisión de la Resolución respectiva para el efecto; y,----------

CONSIDERANDO: *Que, por la misiva mencionada precedentemente, la Dirección de Gabinete del Viceministerio de Tecnologías de la Información y Comunicación de la Institución, remite la propuesta de reglamentación de reportes obligatorios de incidentes cibernéticos por parte de los OEE, presentada por la Dirección General de Ciberseguridad y Protección de la Información, por Memorándum CyPI-20200629 de fecha 29 de junio de 2020, el cual fuera elaborada en forma conjunta con la Dirección General de Asesoría Jurídica, en base a diversas reglamentaciones, normas y estándares internacionales, adaptadas al contexto nacional, a fin de dar cumplimiento a las atribuciones conferidas al MITIC en materia de Ciberseguridad, por Ley N° 6207/2018 y su Decreto Reglamentario N° 2274/2019.----------*

Que, la referida presentación cuenta con el parecer favorable del Viceministro de Tecnologías de la Información y Comunicación de la Institución.----------

Que, la actividad administrativa, como función del Estado, exige por su dinamismo y amplio espectro de acción, la tarea permanente de indagar y explorar las mejores y más eficientes modalidades de gestión. En ese sentido, las herramientas y aplicaciones tecnológicas que proporcionan las ciencias de la tecnología de la información y comunicación se presentan como alternativas de gestión extraordinarias, en sustitución de las formas de prestación de servicios tradicionales en ejercicio del poder público.----------

Que, por Ley N° 6207/2018 del 22 de octubre del 2018 se ha creado el Ministerio de Tecnologías de la Información y Comunicación como "...entidad técnica e instancia rectora, normativa, estratégica y de gestión especializadas, para la formulación de políticas e implementación de planes y proyectos en el ámbito de las Tecnologías de la Información y Comunicación en el sector público, y de la comunicación del Poder Ejecutivo tanto en su

PODER EJECUTIVO
MINISTERIO DE TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIÓN

RESOLUCIÓN MITIC Nº 346

POR LA CUAL SE APRUEBA E IMPLEMENTA EL REGLAMENTO DE REPORTE OBLIGATORIO DE INCIDENTES CIBERNÉTICOS POR PARTE DE LOS ORGANISMOS Y ENTIDADES DEL ESTADO (OEE), AL EL MINISTERIO DE TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIÓN.----------

aspecto social como educativos para la inclusión, apropiación e innovación en la creación, uso e implementación de las tecnologías".----------

Que, el citado cuerpo legal en su Artículo 7º dispone cuanto sigue: "Competencias. El Ministerio tendrá las siguientes competencias: numeral 4) Coordinar la ejecución de acciones conjuntas e integradas entre las distintas reparticiones públicas de actividades relacionadas con la integración de los servicios públicos, ciberseguridad , el desarrollo de la normalización y la sistematización y difusión de la información de acciones relacionadas con la gestión pública por medios electrónicos; numeral 5) Propiciar y emitir directrices para la optimización de los trámites y procesos, y la interoperabilidad entre los distintos Organismos y Entidades del Estado (OEE), a su vez diseñar, coordinar, y monitorear las políticas públicas, planes y estrategias a ser ejecutadas por los mismos, en el marco del Gobierno Electrónico y de Ciberseguridad (...), numeral 13) Dictar, asesorar y participar en la formulación de las políticas nacionales en todas aquellas materias relacionadas con la protección de la información personal y gubernamental; el uso de tecnologías en la educación, en materia de ciberseguridad, innovación productiva, economía digital y demás sectores convergentes de las Tecnologías de la Información y Comunicación (TIC) (...), así como el numeral 23) Ejercer como Autoridad de Ciberseguridad, y de prevención, gestión y control de incidentes cibernéticos que pongan en riesgo el ecosistema digital nacional".----

Que, en idéntico sentido, el Decreto N° 2274 del 6 de agosto de 2019 , por la cual se reglamenta la Ley N° 6207/2018, en su considerando, expresa cuanto sigue: "Que asimismo el Ministerio de Tecnologías de la Información y Comunicación, como Entidad de gestión especializada, es el eje articulador de los esfuerzos de la administración pública destinadas a la formulación e implementación de políticas públicas, planes, programas y proyectos relacionados con las tecnologías de la información y comunicación en el sector público, condicionada a asegurar la plena vigencia del principio de legalidad y seguridad jurídica, para cuyo efecto se requiere la correspondiente reglamentación".----------

*Que, el Decreto mencionado precedentemente, en su Capítulo IV "Ciberseguridad", artículo 43 dispone: "**Prevención y control en materia de ciberseguridad**. El MITIC implementará los mecanismos de monitoreo, gestión, coordinación y respuesta ante los incidentes cibernéticos y amenazas que pongan en riesgo el ecosistema digital nacional y fomentará las iniciativas que contribuyan a la prevención de los mismos, para lo cual establecerá los criterios de definición y clasificación de la infraestructura TIC crítica, designará los sistemas, procesos y tecnologías críticos y propondrá las políticas, estándares y directrices específicas para la protección y aseguramiento de los mismos".----------*

*Que, así también, en su artículo 44 establece cuanto sigue: "**Reporte de incidentes cibernéticos**. El MITIC es la autoridad de prevención, gestión y control en materia de ciberseguridad en resguardo del ecosistema digital nacional. Las Instituciones del sector público, están obligadas a comunicar y denunciar al MITIC todos los incidentes cibernéticos que pongan en riesgo el ecosistema digital nacional, siguiendo las directrices y procedimientos que serán reglamentados los por Resolución del Ministro, sin perjuicio del que el MITIC pueda actuar de oficio ante el conocimiento de un incidente. De igual forma*

PODER EJECUTIVO
MINISTERIO DE TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIÓN

RESOLUCIÓN MITIC Nº 346.-

POR LA CUAL SE APRUEBA E IMPLEMENTA EL REGLAMENTO DE REPORTE OBLIGATORIO DE INCIDENTES CIBERNÉTICOS POR PARTE DE LOS ORGANISMOS Y ENTIDADES DEL ESTADO (OEE), AL EL MINISTERIO DE TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIÓN.----------

el MITIC intervendrá en los incidentes cibernéticos que sean comunicados y denunciados por otros sectores del ecosistema digital nacional. Se considera incidente cibernético a todo evento contra un sistema de información que produce violación de una política de seguridad explícita o implícita, poniendo en riesgo la confidencialidad, integridad y disponibilidad del mismo".----------

Que, a su vez, el Plan Nacional de Ciberseguridad, aprobado mediante el Decreto Presidencial N° 7052/2017 de fecha 24 de abril de 2017, dispone entre sus principios orientadores la coordinación de esfuerzos, estableciendo así que, en el ámbito de ciberseguridad el intercambio de información es fundamental para evaluar y garantizar la respuesta y la recuperación ante intrusiones cibernéticas o ataques a diversos sistemas de información.----------

Que, la Dirección General de Asesoría Jurídica de la Institución se expidió en los términos del Dictamen Nº 115/2020 de fecha 22 de julio de 2020, manifestando cuanto sigue: "Por tanto, atendiendo a las atribuciones que competen a este Ministerio, esta Asesoría no encuentra objeciones a la emisión del Acto Administrativo otorgando lo solicitado, siendo ésta atribución expresa de la Máxima Autoridad Institucional, correspondiendo proseguir, salvo mejor parecer".----------

Que, de acuerdo a lo expuesto precedentemente, atendiendo al rol del MITIC, a través del CERT-PY dependiente de la Dirección General de Ciberseguridad y Protección de la Información del Viceministerio de Tecnologías de la Información y Comunicación, como autoridad de prevención, gestión y control en materia de seguridad de la información del sistema digital nacional, resulta necesario implementar las políticas y estrategias generales en materia de seguridad de la información, desarrollando para el efecto normas reglamentarias, que permitan hacerlas efectivas y ejercer el rol institucional en dicha área.-

Que, la Ley Nº 6.207/2018, en su artículo 8º, establece que el Ministro es la máxima autoridad institucional. En tal carácter es el responsable de la dirección y de la gestión especializada, técnica, financiera y administrativa de la Entidad, en el ámbito de sus atribuciones legales, asimismo, ejerce la representación legal del Ministerio.----------

Que, el Decreto Nº 475/2018 nombra al señor Alejandro Peralta Vierci como Ministro de Tecnologías de la Información y Comunicación (MITIC).----------

***POR TANTO,** en ejercicio de sus atribuciones legales, ----------*

EL MINISTRO DE TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIÓN,

R E S U E L V E:

Artículo 1º.- ***Aprobar e Implementar** el Reglamento de Reporte Obligatorio de Incidentes Cibernéticos por parte de los Organismos y Entidades del Estado (OEE), de conformidad con lo expuesto en el exordio de la presente Resolución, y que como Anexo forma parte integrante de la misma.----------*

PODER EJECUTIVO
MINISTERIO DE TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIÓN

RESOLUCIÓN MITIC Nº 346 -

POR LA CUAL SE APRUEBA E IMPLEMENTA EL REGLAMENTO DE REPORTE OBLIGATORIO DE INCIDENTES CIBERNÉTICOS POR PARTE DE LOS ORGANISMOS Y ENTIDADES DEL ESTADO (OEE), AL EL MINISTERIO DE TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIÓN.----------

Artículo 2º.- ***Establecer*** *la vigencia del reglamento aprobado en el Artículo 1°, a partir de la fecha de la presente Resolución.----------*

Artículo 3º.- ***Encomendar*** *al Viceministerio de Tecnologías de la Información y Comunicación de la Institución la socialización del reglamento aprobado conforme al Artículo 1° de la presente Resolución.------*

Artículo 4º.- ***La*** *presente Resolución será refrendada por el Secretario General de la Institución.----------*

Artículo 5º.- ***Comunicar*** *a quienes corresponda, y cumplido, archivar. ----------*

Rodrigo Sánchez Stark
Secretario General

Alejandro Peralta Vierci
Ministro

PODER EJECUTIVO
MINISTERIO DE TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIÓN

RESOLUCIÓN MITIC Nº 346.-

POR LA CUAL SE APRUEBA E IMPLEMENTA EL REGLAMENTO DE REPORTE OBLIGATORIO DE INCIDENTES CIBERNÉTICOS POR PARTE DE LOS ORGANISMOS Y ENTIDADES DEL ESTADO (OEE), AL EL MINISTERIO DE TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIÓN.----------

CAPÍTULO I

Generalidades

Artículo 1°. - Ámbito de Aplicación.

La presente Resolución será de aplicación obligatoria para los Organismos y Entidades del Estado ("OEE") comprendidos en el ámbito de aplicación establecido en el artículo 3° del Decreto 2274/2019.

Artículo 2°.- Definiciones:

a) ***Activos de información:*** *son los recursos utilizados por un sistema de seguridad de la información para que la organización funcione y consiga sus objetivos. Los mismos incluyen, pero no se limitan a: los archivos de la Institución, ya sea en formato electrónico o no; los sistemas, cuentas, equipos y redes en los que se almacenan, procesan y/o transmite la información institucional, así como también el conocimiento específico acerca de estos activos.*

b) ***Incidente Cibernético de Seguridad ("Incidente"):*** *es una violación o una amenaza inminente de violación a una política de seguridad de la información implícita o explícita, así como un hecho que comprometa la seguridad de un sistema (confidencialidad, integridad o disponibilidad).*

c) ***Disponibilidad****: se refiere al acceso a la información y los sistemas de tratamiento de la misma por parte de los usuarios autorizados cuando lo requieran.*

d) ***Integridad****: significa un mantenimiento de la exactitud y completitud de la información y sus métodos de proceso.*

e) ***Confidencialidad****: se refiere al acceso a la información por parte únicamente de quienes estén autorizados.*

f) ***Seguridad digital nacional****: situación de hecho aplicada al ámbito digital, en la cual el orden público está resguardado, así como la vida, la libertad y los derechos de las personas y entidades y sus bienes, en un marco de plena vigencia de las instituciones establecidas en la Constitución Nacional.*

Artículo 3°.- Dimensiones de la seguridad.

A fin de poder determinar el impacto que tendría sobre la organización un incidente que afectara a la seguridad de la información de los activos de información, y de poder establecer el nivel de criticidad, se tendrán en cuenta las siguientes dimensiones de la seguridad:

a) Disponibilidad

b) Integridad

c) Confidencialidad.

Artículo 4°.- Criterios para definición de niveles de criticidad de un incidente cibernético de seguridad.

De manera a establecer el nivel de criticidad de un determinado incidente cibernético de seguridad, cada dimensión de seguridad afectada se adscribirá a uno de los niveles bajo, medio o alto descritos en el presente artículo.

PODER EJECUTIVO
MINISTERIO DE TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIÓN

RESOLUCIÓN MITIC Nº 346 -

POR LA CUAL SE APRUEBA E IMPLEMENTA EL REGLAMENTO DE REPORTE OBLIGATORIO DE INCIDENTES CIBERNÉTICOS POR PARTE DE LOS ORGANISMOS Y ENTIDADES DEL ESTADO (OEE), AL EL MINISTERIO DE TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIÓN.----------

Una información o un servicio pueden verse afectados en una o más de sus dimensiones de seguridad. Si ninguna dimensión de seguridad se ve afectada, no se adscribirá a ningún nivel.

a) ***Nivel alto:*** *Se utilizará cuando las consecuencias de un incidente de seguridad que afecte a alguna de las dimensiones de seguridad y supongan un perjuicio muy grave o total para los objetivos misionales de la organización, sus activos críticos o los individuos afectados. Se entenderá por perjuicio muy grave o total:*

   1. *º La anulación de la capacidad de la organización para atender a alguna de sus obligaciones fundamentales y que éstas sigan desempeñándose.*
   2. *º El daño muy grave, e incluso irreparable, de los activos de la organización, sean estos financieros, de información, de imagen o de otra naturaleza.*
   3. *º El incumplimiento de alguna ley o regulación.*
   4. *º Causar un perjuicio grave a individuos, de difícil o imposible reparación.*
   5. *º Otros de naturaleza análoga.*

b) ***Nivel medio****: Se utilizará cuando las consecuencias de un incidente cibernético de seguridad que afecte a alguna de las dimensiones de seguridad supongan un perjuicio parcial sobre las funciones de la organización, sobre sus activos o sobre los individuos afectados. Se entenderá por perjuicio parcial:*

   1. *º La reducción parcial de la capacidad de la organización para atender eficazmente a sus obligaciones fundamentales, aunque estas sigan desempeñándose.*
   2. *º El daño parcial de los activos de la organización, así sean estos financieros, de información, de imagen u otra naturaleza.*
   3. *º Causar un perjuicio moderado a algún individuo.*
   4. *º Otros de naturaleza análoga.*

c) ***Nivel bajo****. Se utilizará cuando las consecuencias de un incidente cibernético de seguridad que afecte a alguna de las dimensiones de seguridad supongan un perjuicio mínimo o incluso nulo sobre las funciones de la organización, sobre sus activos o sobre los individuos afectados. Se entenderá por perjuicio mínimo:*

   1.º *Sin reducción de la capacidad de la organización para atender eficazmente con sus obligaciones corrientes, las cuales se siguen desempeñando normalmente.*
   2.º *Sin daño o con daño mínimo de activos de la organización, así sean estos financieros, de información, de imagen u otra naturaleza.*
   3.º *Sin perjuicio a individuos.*
   4.º *Otros de naturaleza análoga.*

Cuando un sistema maneje diferentes informaciones y/o preste diferentes servicios, el nivel del sistema en cada dimensión será el mayor de los establecidos para cada información y cada servicio.

PODER EJECUTIVO
MINISTERIO DE TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIÓN

RESOLUCIÓN MITIC Nº 346.-

POR LA CUAL SE APRUEBA E IMPLEMENTA EL REGLAMENTO DE REPORTE OBLIGATORIO DE INCIDENTES CIBERNÉTICOS POR PARTE DE LOS ORGANISMOS Y ENTIDADES DEL ESTADO (OEE), AL EL MINISTERIO DE TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIÓN.----------

El MITIC, además, evaluará los factores del incidente que sobrepasen el contexto interno de la institución, entre ellos, el potencial impacto e interdependencia con otros sectores y categorizará el incidente de acuerdo a ello.

CAPÍTULO II

Reportes de Incidentes

Artículo 5°.- Reporte obligatorio de los incidentes por parte de los OEE.

Los servidores públicos de los OEE deben comunicar al responsable de seguridad de la información designado dentro de su institución o en su defecto al Director de la UETIC, acerca de todos los incidentes cibernéticos de seguridad de información que les afecten, siguiendo las políticas y procedimientos de gestión de incidentes de su institución.

Asimismo, los OEE a través de sus responsables, comunicarán inmediatamente acerca del incidente al CERT-PY, dependiente de la Dirección General de Ciberseguridad y Protección de la Información del MITIC, acompañando toda la información necesaria para valorar su impacto, a fin de que se articulen desde el MITIC las gestiones adecuadas tendientes a lograr la solución del incidente declarado. Independientemente a que el evento haya sido subsanado o mitigado, éste debe ser comunicado, con fines de alerta temprana a terceros y/o acciones de coordinación adicionales.

Los OEE deberán cuidar que las medidas de mitigación y/o control del incidente no comprometan la evidencia o la información relevante para la investigación del mismo.

El MITIC desarrollará, habilitará y dará a conocer las herramientas y plataformas necesarias para facilitar a los denunciantes los procesos de notificación, comunicación e información de incidentes.

Artículo 6°.- Reportes complementarios.

Los responsables de seguridad de la información designados por cada OEE o en su defecto, el Director de la UETIC, deberán efectuar los reportes adicionales o complementarios que permitan al MITIC actualizar la información sobre el incidente, en caso de que se descubriera información adicional o diferente a la declarada inicialmente.

Igualmente, los OEE deberán informar, como mínimo, del estado en que se encuentren las acciones que hayan sido recomendadas por el MITIC, hasta su resolución, para un cierre apropiado.

Artículo 7°. - Adopción de medidas de seguridad

Los OEE son los responsables por la seguridad de los activos de información generada o en su poder. Los OEE tienen la obligación de adoptar medidas de seguridad eficientes a fin de proteger todos sus activos de información. Estas medidas de seguridad deberán estar alineadas a las directivas, estándares y normativas del MITIC, así como también a los riesgos y brechas identificados por cada OEE y la criticidad de cada activo.

Además, si como consecuencia de los incidentes denunciados surgen elementos que justifiquen la adopción de nuevas medidas de seguridad, sean estas recomendadas por parte del MITIC o identificadas internamente en el OEE, éstas deberán ser adoptadas por el mismo en el menor plazo posible.

Artículo 8.- Notificación de Brecha de seguridad.

PODER EJECUTIVO
MINISTERIO DE TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIÓN

RESOLUCIÓN MITIC Nº 346

POR LA CUAL SE APRUEBA E IMPLEMENTA EL REGLAMENTO DE REPORTE OBLIGATORIO DE INCIDENTES CIBERNÉTICOS POR PARTE DE LOS ORGANISMOS Y ENTIDADES DEL ESTADO (OEE), AL EL MINISTERIO DE TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIÓN.----------

En caso de existir datos que se encuentren comprometidos, es obligación de los OEE reportar este incidente al CERT-PY dependiente de la Dirección General de Ciberseguridad y Protección de la Información del MITIC, conforme a lo establecido en la presente Resolución, así como también notificar esta situación a los individuos afectados, comunicando los hechos confirmados y las acciones tomadas o a tomar para su investigación y/o mitigación.

Esta comunicación deberá ser realizada con la cooperación del MITIC a fin de proporcionar una información que se encuentre correcta en los aspectos tanto técnico como comunicacional, siendo el Responsable de Seguridad de la Información designado del OEE o en su defecto el Director de UETIC, el punto de coordinación para estas gestiones.

Artículo 9° - Rol y alcance de la responsabilidad del MITIC en cuanto a la gestión de los incidentes

El MITIC, a través del CERT-PY dependiente de la Dirección General de Ciberseguridad y Protección de la Información, tiene como rol la coordinación entre los diferentes actores involucrados en un incidente cibernético que afecta al ecosistema digital nacional.

El alcance de la gestión de un incidente cibernético por parte del MITIC abarca:

- *Análisis preliminar del incidente cibernético.*
- *La notificación, coordinación y guía a los actores involucrados y responsables de los sistemas afectados para la toma de acciones pertinentes.*
- *La propuesta de recomendaciones pertinentes para la corrección y prevención futura.*

Dependiendo de la naturaleza del incidente, de la solicitud y/o cooperación de un actor involucrado en un incidente y los procedimientos establecidos, el MITIC podrá colaborar en la aplicación de acciones de contención inmediata, así como también en la investigación y análisis del sistema comprometido.

El MITIC no será responsable de la aplicación de las acciones y recomendaciones que derivan de la gestión de un incidente, siendo éstas responsabilidad del OEE y sus responsables designados para administrar el recurso comprometido o afectado.

Artículo 10. - Mecanismos de reporte de incidentes

El MITIC, a través del CERT-PY, dependiente la Dirección de Ciberseguridad y Protección de la Información, establecerá los mecanismos de reporte de incidentes, los cuales serán publicados en su página web y comunicados a los OEE para su toma de conocimiento. Estos podrán ser actualizados en la medida que ello resulte necesario y serán publicados y comunicados por las mismas vías.

Artículo 11. - Actuación de oficio del MITIC frente a incidentes.

Sin perjuicio de la obligación de los OEE de reportar aquellos incidentes advertidos por los mismos, el MITIC podrá intervenir de oficio en los incidentes que sean considerados de criticidad alta para la seguridad digital nacional, articulando todas aquellas medidas que sean conducentes a obtener una solución eficaz y eficiente, conforme a las disposiciones de esta reglamentación.

En caso de incidentes que necesiten la articulación de otros OEE con competencia para ello, el MITIC deberá inmediatamente articular las herramientas y las comunicaciones respectivas con estos organismos.

PODER EJECUTIVO
MINISTERIO DE TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIÓN

RESOLUCIÓN MITIC Nº 346 - -

POR LA CUAL SE APRUEBA E IMPLEMENTA EL REGLAMENTO DE REPORTE OBLIGATORIO DE INCIDENTES CIBERNÉTICOS POR PARTE DE LOS ORGANISMOS Y ENTIDADES DEL ESTADO (OEE), AL EL MINISTERIO DE TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIÓN.----------

Artículo 12. - Incidentes que puedan constituir hechos punibles de acción penal pública.

El MITIC, a través del CERT-PY, dependiente la Dirección de Ciberseguridad y Protección de la Información, pondrá a conocimiento del Ministerio Público aquellos incidentes o reportes que le sean comunicados desde los diversos OEE, y que pudieran constituir un hecho de relevancia penal pública.
Durante el proceso de gestión de incidentes cibernéticos de seguridad, el MITIC así como los OEE involucrados en el incidente seguirán los lineamientos emitidos por el Ministerio Público para la preservación de la evidencia probatoria de contenido digital.

CAPÍTULO III

Información y comunicación de incidentes

Artículo 13. - Información al público.

En caso de que la información al público sea necesaria debido a los intereses y derechos comprometidos, toda publicación deberá ser coordinada previamente por el MITIC.

Mientras exista una investigación en curso, los OEE no publicarán información sobre los incidentes, salvo aquella coordinada con el MITIC, conforme a las guías y lineamientos que éste establezca, de modo a informar de manera clara y certera, sin comprometer la investigación. Los OEE no deberán realizar comunicados sobre incidente cibernético de seguridad o ciberataques sin que éstos hayan sido confirmados por el Responsable de Seguridad de la Información designado del OEE y éstos hayan sido notificados al MITIC conforme la presente Resolución.

Artículo 14.- Información a titulares de derechos afectados.

En caso de que el incidente hubiera afectado derechos o libertades de terceros, el OEE deberá obligatoriamente informar a los titulares afectados dicho acontecimiento, sin dilación alguna, de manera clara y precisa, debiendo incluir como mínimo:

- *La naturaleza del incidente.*
- *Los datos o servicios comprometidos.*
- *Las acciones correctivas realizadas de forma inmediata.*
- *Las recomendaciones a los afectados sobre las medidas que éste pueda adoptar para proteger sus intereses.*

Esta obligatoriedad no será aplicable en caso de que hubiera evidencia suficiente y que el MITIC compruebe que el incidente cibernético constituye un hecho de interés de seguridad nacional, mientras hubiera una investigación en curso.

Artículo 15.- Confidencialidad de la información por parte del MITIC

El MITIC no publicará información detallada de incidentes cibernéticos que le hayan sido reportados, salvo cuando sea necesario para evitar futuros eventos similares, aquella información que ya ha tomado público conocimiento y/o que hubiera sido autorizado explícitamente por los afectados. También podrá remitir informes cuando éstos sean solicitados por vía judicial.

El MITIC podrá publicar información estadística, así como también información anonimizada sobre incidentes concretos con fines de concienciación y capacitación únicamente, sin revelar datos que permitan identificar a víctimas o divulgar detalles que pongan en riesgo a actores involucrados.