CONVOCA A CONSULTA CIUDADANA SOBRE NORMATIVA DE CIBERSEGURIDAD EN EL SECTOR DE LAS TELECOMUNICACIONES /

RESOLUCIÓN EXENTA Nº 828 /

SANTIAGO, MAYO 19 DE 2020.

V I S T O S:

a. El decreto ley Nº 1.762, de 1977, que crea la Subsecretaría de Telecomunicaciones.

b. La ley Nº 18.168, General de Telecomunicaciones.

c. La ley N° 20.500, sobre asociaciones y participación ciudadana en la gestión pública.

d. El decreto exento N° 1.053, de 2015, del Ministerio de Transportes y Telecomunicaciones, que aprueba la norma general de participación ciudadana de este Ministerio.

e. La resolución exenta N° 5.077, de 2011, de la Subsecretaría de Telecomunicaciones, que define materias de interés y establece procedimiento de consulta ciudadana.

f. La resolución N° 7, de 2019, de la Contraloría General de la República, que fija normas sobre exención del trámite de toma de razón.

C O N S I D E R A N D O:

a. Que el uso cotidiano, masivo y generalizado de los servicios de telecomunicaciones permite el desenvolvimiento de las personas en diferentes niveles, por lo que cualquier alteración de su funcionamiento provoca grandes consecuencias económicas y sociales. En la medida que siga ampliándose el uso de los servicios de telecomunicaciones irán incrementándose los efectos causados por su alteración. Es por ello que resulta de gran importancia el establecimiento de medidas regulatorias orientadas a mejorar la continuidad y seguridad de tales servicios.

b. Que, en ese sentido, mediante el decreto supremo N° 60, de 2012, del Ministerio de Transportes y Telecomunicaciones, se estableció el reglamento sobre la declaración y resguardo de la infraestructura crítica de telecomunicaciones. Sin embargo, su alcance se acota a los elementos de infraestructura física de las redes y sistemas, con prescindencia de la infraestructura lógica, protocolos, software, datos y contenido de las comunicaciones.

c. Que, asimismo, el decreto supremo N° 368, de 2012, del Ministerio de Transportes y Telecomunicaciones, que aprueba el reglamento que regula las características y condiciones de la neutralidad de la red en el servicio de acceso a internet, impone a los proveedores de acceso a Internet la obligación de preservar la privacidad de los usuarios, brindar protección contra virus y resguardar la seguridad de la red. No obstante, esta regulación no hace explícita la obligación de reportar las ciberincidencias ni la de proceder a su resolución y prevenir su ocurrencia.

d. Que, como se advierte de lo expuesto, existe una ausencia de regulación en materias de gran importancia para los derechos de los usuarios y el buen funcionamiento de los servicios de telecomunicaciones. Por tal motivo, a fin de contar con mayores antecedentes para la elaboración de un marco que regule la ciberseguridad de las redes y sistemas de los servicios de telecomunicaciones, la Subsecretaría ha decidido someter a consulta ciudadana una propuesta normativa sectorial sobre dicha materia, en la que todas las personas y organizaciones interesadas podrán formular sus planteamientos al respecto.

e. Que la dictación de una normativa de ciberseguridad en el ámbito de las telecomunicaciones se funda en las amplias atribuciones con que cuenta la Subsecretaría en la materia. En efecto, conforme a lo dispuesto por el artículo 6° del decreto ley N° 1.762, de 1977, y por el artículo 7º de la ley Nº 18.168, a la Subsecretaría de Telecomunicaciones le corresponde, entre otras funciones, dictar las normas técnicas sobre telecomunicaciones y controlar su cumplimiento; requerir de las entidades que operan en el ámbito de las telecomunicaciones todos los antecedentes e informaciones necesarios para el desempeño de su cometido; y, también, controlar y supervigilar el adecuado funcionamiento de los servicios públicos de telecomunicaciones y la protección de los derechos de los usuarios.

R E S U E L V O:

ARTÍCULO 1°. Sométase a consulta ciudadana la propuesta normativa sobre fundamentos generales de ciberseguridad para el diseño, instalación y operación de redes y sistemas utilizados en la prestación de servicios de telecomunicaciones que se adjunta como anexo a la presente resolución.

ARTÍCULO 2°. Publíquese la presente resolución en un lugar visible de la página web institucional de la Subsecretaría de Telecomunicaciones (www.subtel.gob.cl), junto con la respectiva propuesta normativa.

ARTÍCULO 3º. Fíjase un plazo de 15 días corridos para que las personas naturales y jurídicas que así lo deseen puedan formular al documento anexo sus comentarios, observaciones o consultas través de las ventanillas virtuales de opinión habilitadas en la página web de la Subsecretaría. El plazo se contará desde la publicación de la presente resolución hasta las 23:59 horas del día jueves 4 de junio de 2020.

ARTÍCULO 4º. Todas las respuestas y antecedentes que sean recabados por la Subsecretaría durante el curso de la presente consulta ciudadana serán debida y oportunamente publicados en atención al carácter público de la misma.

ANÓTESE Y PUBLÍQUESE EN EL PORTAL WEB DE LA SUBSECRETARÍA DE TELECOMUNICACIONES

PAMELA GIDI MASIAS
Firmado digitalmente por PAMELA GIDI MASIAS
Fecha: 2020.05.20 12:09:39 -04'00'

PAMELA GIDI MASIAS
Subsecretaria de Telecomunicaciones

ANEXO

PROPUESTA NORMATIVA SOBRE FUNDAMENTOS GENERALES DE CIBERSEGURIDAD PARA EL DISEÑO, INSTALACIÓN Y OPERACIÓN DE REDES Y SISTEMAS UTILIZADOS EN LA PRESTACIÓN DE SERVICIOS DE TELECOMUNICACIONES.

Artículo 1°. Objeto

La presente norma técnica tiene por objeto establecer un marco regulatorio que comprenda los fundamentos generales de ciberseguridad en base a los cuales deben diseñarse, instalarse y operarse las redes y sistemas utilizados para la prestación de servicios de telecomunicaciones por parte de aquellos titulares de concesión o permiso que hayan sido declarados como operadores relevantes por esta Subsecretaría.

De igual manera, esta norma técnica busca normar el envío de información sobre ciberincidencias que los concesionarios y permisionarios de servicios de telecomunicaciones deban reportar a la Subsecretaría, con el objeto de coordinar las acciones orientadas mitigar sus efectos y contribuir a una oportuna restitución de los servicios afectados.

Artículo 2°. **Definiciones**

Para los efectos de esta norma técnica, los términos que a continuación se señalan tendrán el siguiente significado:

a) Ciberespacio: es el ambiente compuesto por las infraestructuras tecnológicas, los componentes lógicos de la información y las interacciones sociales que se verifican en su interior. Las infraestructuras tecnológicas corresponden a los equipos materiales empleados para la transmisión de las comunicaciones, tales como enlaces, enrutadores, conmutadores, estaciones, sistemas radiantes, nodos, conductores, entre otros. Los componentes lógicos de la información, en tanto, son los diferentes softwares que permiten el funcionamiento, administración y uso de la red.

b) Ciberincidencia: es toda acción que comprometa la disponibilidad, autenticidad, integridad o confidencialidad de los datos almacenados, transmitidos o tratados, o los servicios correspondientes ofrecidos por los sistemas de telecomunicaciones, que puedan afectar al normal funcionamiento de los mismos.

c) Ciberseguridad: es una condición caracterizada por un mínimo de riesgos y amenazas a las infraestructuras tecnológicas, los componentes lógicos de la información y las interacciones que se verifican en el ciberespacio, así como también el conjunto de políticas y técnicas destinadas a lograr dicha condición.

d) Equipo de Respuesta ante Incidentes de Seguridad Informática, en adelante “CSIRT”: es el órgano encargado de recibir y analizar reportes de ciberincidencias, con el fin de analizarlos, monitorear el desarrollo de éstas, emitir alertas y proponer medidas tanto de mitigación como de prevención, así como la publicación de alertasy guías de buenas prácticas. La denominación CSIRT proviene de la expresión inglesa *Computer Security Incident Response Team* .

e) Gestión de incidentes: procedimientos para la detección, análisis, manejo, contención y resolución de una incidencia de ciberseguridad y responder ante ésta.

f) Incidente: suceso inesperado o no deseado con consecuencias en detrimento de la seguridad de las redes y sistemas de información de telecomunicaciones.

g) Infraestructura crítica de telecomunicaciones: es el conjunto de redes y sistemas de telecomunicaciones cuya interrupción, destrucción, corte o fallo generaría un serio impacto en la seguridad, privacidad o disponibilidad de servicio de la población afectada, siendo así declarada mediante resolución fundada de la Subsecretaría conforme a los artículos 22 y siguientes del decreto supremo N° 60, de 2012, del Ministerio de Transportes y Telecomunicaciones, que aprueba el reglamento para la interoperación y difusión de la mensajería de alerta, declaración y resguardo de la infraestructura crítica de telecomunicaciones e información sobre fallas significativas en los sistemas de telecomunicaciones.

h) Operadores relevantes: son los titulares de una concesión de servicio público o intermedio de telecomunicaciones, o de un permiso de servicio limitado de telecomunicaciones, que hayan sido declarados como relevantes por SUBTEL en consideración a los criterios de relevancia mencionados en el artículo 4° de la presente norma. Adicionalmente, serán considerados operadores relevantes para los efectos de la presente normativa, los concesionarios y permisionarios que operen redes y sistemas de telecomunicaciones que hayan sido declarados como infraestructura crítica por resolución fundada de la Subsecretaría.

i) Riesgo: toda circunstancia o hecho razonablemente identificable que tenga un posible efecto adverso en la seguridad de las redes y sistemas de información de telecomunicaciones. Se puede cuantificar como la probabilidad de materialización de una amenaza que produzca un impacto en términos de operatividad, de integridad física de personas o material o de imagen corporativa.

Cualquier otro término no definido en esta norma técnica tendrá el significado que se le atribuya en la respectiva normativa sectorial de telecomunicaciones.

Artículo 3°. Ámbito de aplicación

Las disposiciones contenidas en esta norma técnica solamente se aplican al diseño, instalación y operación de redes y sistemas utilizados para la prestación de servicios de telecomunicaciones que se realiza en ejercicio de un título habilitante regulado por la ley Nº 18.168, General de Telecomunicaciones, cuya titularidad recaiga en un operador relevante conforme a la definición señalada en el literal h) del artículo precedente.

Artículo 4°. Criterios de relevancia

La declaración de un titular de servicios de telecomunicaciones como operador relevante se efectuará mediante resolución fundada de esta Subsecretaría, en la que se dejará constancia tanto de los criterios de relevancia tenidos en consideración como de la valoración que de ellos se hiciere.

A fin de determinar si un titular de servicio de telecomunicaciones debe ser declarado relevante para los fines de la presente norma técnica, la Subsecretaría tendrá en consideración, a lo menos, los siguientes criterios:

a) Extensión territorial del servicio;
b) Sustituibilidad del servicio;
c) Impacto social o económico de eventuales interrupciones, en consideración de su duración;
d) Atención a sectores estratégicos;
e) Participación de mercado;

Sin perjuicio de lo anterior, todo concesionario o permisionario de servicios de telecomunicaciones que opere redes y sistemas hayan sido declarados como infraestructura crítica por esta Subsecretaría, serán considerados operadores relevantes para todos los efectos de la presente norma técnica.

Artículo 5°. Obligaciones generales de seguridad

Los operadores relevantes de servicios de telecomunicaciones deberán determinar y adoptar las medidas técnicas y de organización que permitan gestionar adecuadamente los riesgos de las redes y sistemas que utilizan para prestar servicios de telecomunicaciones a terceros en razón de sus títulos habilitantes, aún en caso de que tal gestión estuviere externalizada.

Dichas medidas deberán garantizar un nivel adecuado de seguridad de las redes y sistemas, tomando en consideración la naturaleza y el contexto de los servicios prestados, los riesgos asociados y la tecnología disponible, así como tener en cuenta, a lo menos, los siguientes conceptos:

a) seguridad física y ciberseguridad de los sistemas e instalaciones;
b) costos de implementación;
c) gestión del riesgo propio de la actividad;
d) gestión de incidentes;
e) gestión de la continuidad de los servicios*;*
f) monitoreo permanente de los sistemas ;
g) actividades de supervisión, auditoría y prueba;
h) cumplimiento de normas y estándares internacionales;
i) conocimiento de las alertas de ciberincidencias a nivel nacional e internacional;
j) actualización constante de protocolos y sistemas de seguridad;
k) determinaciones nacionales e internacionales en relación a los riesgos de seguridad asociados al uso de determinados equipos o proveedores;
l) integridad de la cadena de suministros de equipos y software;

De igual forma, los operadores relevantes deberán tomar las medidas adecuadas para prevenir y reducir al mínimo los efectos de las ciberincidencias que afecten la seguridad de las redes y sistemas utilizados para la prestación de los servicios, con el objeto de garantizar su continuidad operativa. En todos los casos, se deberá diseñar, implementar, practicar y evaluar un plan de respuesta que otorgue adecuada cobertura a sus redes y sistemas en conformidad con estándares internacionales, independientes o nacionales, de amplia aplicación.

Los operadores relevantes de servicios de telecomunicaciones deberán aplicar criterios orientados a minimizar los riesgos de ciberincidencias y a facilitar una adecuada gestión de éstos durante su operación desde las etapas de concepción, planeamiento y diseño de sus redes, sistemas y procesos y, en general, durante toda gestión anterior al funcionamiento. Esto incluye tanto la selección del fabricante o proveedor como la selección de los equipos y contratistas. Asimismo, deberán adoptar medidas que permitan verificar el cumplimiento eficaz de dichos criterios a lo largo de toda la cadena de suministros, pasando desde la manufactura de los equipos, su transporte y entrega, su instalación, su puesta en marcha y su entrada en servicio.

Los operadores relevantes deberán contar con planes de gestión de riesgos de seguridad formulados con arreglo a principios, estándares y directrices que guarden la debida coherencia con las características de las redes y sistemas a los cuales se aplican.

Tanto el diseño de las redes y sistemas como la elaboración de los planes de gestión de riesgos serán de responsabilidad exclusiva del respectivo operador relevante, no obstante que, en todos los casos, deberá tener en consideración, a lo menos, las recomendaciones de esta Subsecretaría, del CSIRT de referencia y de todas las entidades que participen del Sistema Nacional de Ciberseguridad.

La documentación y demás antecedentes que den cuenta del detalle de los planes de gestión de riesgos deberá estar permanentemente disponible en caso de inspecciones a realizar por Subtel o a fin de participar en actividades o ejercicios de gestión de incidentes y simulacros de crisis organizados por la autoridad competente en materia de ciberseguridad. Asimismo, los operadores relevantes deberán considerar en sus planes el estado de la técnica y la tecnología disponible en los ámbitos de seguridad de sistemas, seguridad de instalaciones, continuidad de la operación, gestión de ciberincidencias y monitoreo de redes; los lineamientos y recomendaciones de organismos internacionales de estandarización; los servicios de capacitación en ciberseguridad disponibles en el mercado; y cualesquiera otras consideraciones que contribuyan a una gestión más segura de las redes y sistemas.

No obstante lo expuesto, la Subsecretaría de Telecomunicaciones podrá establecer que, en consideración a circunstancias particulares de vulnerabilidad, determinados operadores relevantes deban adoptar los estándares que la autoridad le indique.

Artículo 6°. Encargados de ciberseguridad

Todo operador relevante deberá contar permanentemente con, a lo menos, un encargado titular de ciberseguridad en funciones y un suplente, quienes deberán poseer las competencias suficientes para identificar los riesgos de afectación de los servicios de telecomunicaciones por causa de ciberincidencias, verificar el cumplimiento eficaz de los respectivos planes de gestión, reportar las ciberincidencias y coordinar la gestión ciberseguridad con las autoridades competentes.

Los operadores relevantes deberán informar a Subtel, en el plazo que se instruya, las identidades de sus encargados de ciberseguridad, la unidad a la que pertenecen y los medios de contacto pertinentes, informando oportunamente en caso que exista alguna modificación al respecto.

Artículo 7°. Obligación de reportar ciberincidencias

Los operadores relevantes deberán reportar oportunamente a la Subsecretaría de Telecomunicaciones, directamente o a través del órgano que designe para dichos fines, acerca de todas las ciberincidencias que detecte en sus redes y sistemas y que alcance los umbrales de gravedad establecidos en las instrucciones pertinentes emitidas por Subtel. Igual obligación recaerá en todo operador relevante que dependa de un proveedor u operador no relevante para la prestación de algunos de sus servicios, debiendo reportar cualquier ciberincidencia de gravedad que afecte al proveedor u operador no relevante.

Los reportes deberán ser formulados por los encargados de ciberseguridad de los operadores relevantes y enviados a través de los mecanismos establecidos para ello por la Subsecretaria de Telecomunicaciones en el más breve plazo posible. Con todo, el tiempo que medie entre la detección de la ciberincidencia y la emisión del reporte, no podrán exceder del que se indica a continuación de conformidad a la naturaleza y alcance de cada evento:

Alcance ciberincidencia	Descripción	Obligación de reportar ciberincidencia
Alta	Las redes o sistemas están fuera de operación; datos personales están siendo extraídos o expuestos; o procesos críticos están siendo alterados o manipulados.	30 minutos
Media	Las redes o sistemas están parcialmente fuera de operación; datos personales están en riesgo de ser extraídos o expuestos; o los procesos críticos están en riesgo de ser alterados o manipulados.	1 hora
Baja	Redes o sistemas en operación con fallas reducidas o limitadas.	3 horas

Lo anterior debe entenderse sin perjuicio de las instrucciones específicas, tanto de carácter contingente, temporal o periódico que las autoridades competentes impartan en relación a determinadas categorías de ciberincidencias. Asimismo, toda ciberincidencia que afecte o pudiere afectar infraestructuras críticas de telecomunicaciones deberá ser reportada tan pronto como sea detectada y, en caso de que no fuera posible acceder a los mecanismos dispuestos para ello, a través del más expedito de aquellos medios disponibles.

La obligación de reportar se entenderá formalmente cumplida solamente luego de que Subtel, directamente o través del órgano designado para dichos fines, haya acusado recibo a través de los mecanismos dispuestos para ello, excepto si éstos no se encontrasen disponibles.

Toda consulta formulada a un operador, sea directamente por Subtel o por el órgano designado para dichos fines, generará para éste una nueva obligación de reportar,que deberá cumplir dentro del plazo señalado en el propio requerimiento.

Artículo 8°. Desarrollo de los reportes

En caso de ciberincidencias que se extiendan por un período de tiempo que exceda de treinta minutos, los encargados de ciberseguridad del operador relevante afectado deberán enviar en forma oportuna y sucesiva tantos reportes como sean necesarios para dar adecuada cuenta del desarrollo de ésta hasta su cierre, o bien, conforme a las instrucciones impartidas por Subtel o por el órgano designado para dichos fines.

Artículo 9°. Contenido de los reportes

Sin perjuicio de las instrucciones que al efecto impartan las autoridades competentes, los operadores relevantes deberán mantener, durante un plazo no inferior a un año desde su ocurrencia, registros de ciberincidencias que den cuenta, a lo menos, de los siguientes datos:

a. Titular de servicio de telecomunicaciones.
b. Jefe de seguridad y encargado de seguridad en funciones.
c. Datos de contacto.
d. Afectación actual y eventual de infraestructuras críticas.
e. Hechos indiciarios o reveladores de la ciberincidencia.
f. Momento estimado de inicio de los hechos y duración de la ciberincidencia.
g. Redes y sistemas actual y eventualmente afectados.
h. Estimación de la cantidad de usuarios y clientes actual y/o eventualmente afectados.
i. Grado de afectación a usuarios y clientes.
j. Alcance geográfico actual y eventual de la ciberincidencia.
k. Origen posible de la ciberincidencia.
l. Detalle de medidas de mitigación y restablecimiento.
m. Tiempo estimado para la resolución definitiva de la ciberincidencia.

Deberá mantenerse registro de la evolución de la ciberincidencia conforme su desarrollo y, en caso de que puedan afectar o se afecten infraestructuras críticas, el registro debe extenderse hasta que se hubiere cerrado, es decir, su completa resolución.

Los reportes deberán enviarse en forma oportuna conforme el desarrollo de la ciberincidencia, incorporando toda la información que sea pertinente y reportando cada cambio sustancial a medida que suceda.

El encargado de ciberseguridad en funciones deberá reportar en la oportunidad que corresponda según la gravedad aparente de la ciberincidencia, aún en caso de que no cuente con todos los antecedentes necesarios -los que podrá completar en reportes posteriores-, a fin de coordinar las medidas de mitigación y presentar planes de acción.

Adicionalmente, en el caso particular de ciberincidencias que afecten o puedan afectar infraestructuras críticas, el reporte deberá indicar los motivos por los que no contiene toda la información pertinente, la que deberá ser enviada tan pronto como sea obtenida. En caso de que el impedimento persista, se deberá continuar reportando a Subtel, sea directamente o a través del órgano designado para dicho efecto, los motivos del impedimento y las gestiones efectuadas para subsanarlos. Asimismo, el operador afectado deberá conservar por, a lo menos, seis meses desde el cierre de la ciberincidencia, todos los logs y registros que hubieren podido registrar efectos y actividades relacionadas con el posible ataque así como las medidas de gestión y resolución adoptadas.

Artículo 10°. Tratamiento de los reportes

El contenido de los reportes de ciberincidencias será tratado con reserva por los organismos del Estado que tomen conocimiento de éstos. En particular, se tendrá especial cuidado en revelar cualquier parte del reporte a partir del cual pudiera llegar a inferirse la identidad del operador relevante y de los encargados de ciberseguridad que participaron en su formulación.

Artículo 11. Información a terceros e intercambio de información

En caso de que sea necesario informar a terceros para prevenir, gestionar o resolver una ciberincidencia, el operador relevante podrá solicitar la asistencia del CSIRT de referencia o de Subtel.

Por su parte, la Subsecretaría de Telecomunicaciones podrá difundir aquellas ciberincidencias cuyo conocimiento por parte del público general contribuya a reducir su ocurrencia o mitigar su eventual impacto.

En caso de que esta Subsecretaría decida informar directamente al público o terceros, la publicación estará orientada a la entrega de información sobre las ciberincidencias, posibles causas, medidas de mitigación, recomendaciones de seguridad, alternativas de acciones a seguir, operadores relevantes, zonas geográficas o sistemas afectados y cualquier otra información de importancia para la correcta y oportuna información del público en general, sin que esto signifique afectaciones a la reputación del operador.

Asimismo, conforme las atribuciones que conferidas por la legislación aplicable, Subtel adoptará medidas y efectuará gestiones orientadas a promover el intercambio de información entre actores públicos y privados en materias de seguridad física y de ciberseguridad de redes y sistemas de telecomunicaciones.

Artículo 12. Obligación de resolución de ciberincidencias

Una vez detectada una ciberincidencia que afecte a una red o sistema utilizado para la prestación de servicios de telecomunicaciones, el respectivo operador deberá efectuar de manera oportuna todas las gestiones que sean necesarias para su resolución y restaurar la normal provisión de los servicios afectados, con arreglo a su plan de gestión de riesgos y, en todos los casos, dando primera prioridad a aquellas medidas que permitan evitar o, en su defecto, minimizar el impacto a los usuarios finales.

En caso de que el operador relevante afectado lo considere necesario, podrá solicitar cooperación al CSIRT de referencia, la Subsecretaría u otras entidades competentes en materia de ciberseguridad , para la resolución de una ciberincidencia.

Los operadores relevantes deberán proporcionar la información adicional que les sea requerida para analizar la naturaleza, causas y efectos de los incidentes notificados, y para elaborar estadísticas y reunir los datos necesarios para elaborar informes de resultados. La información adicional proporcionada será tratada con reserva y no será usada para fines distintos de los autorizados.

Asimismo, sin perjuicio de las medidas inmediatas conducentes a la mitigación de los efectos y al restablecimiento de los servicios afectados por una ciberincidencia, los operadores relevantes deberán subsanar las vulnerabilidades de sus sistemas que hubieren permitido o facilitado ciberincidencias.

Artículo 13. Tratamiento de datos personales

En caso de que se deban incorporar datos personales de carácter sensible en un informe de ciberincidencia en razón de ser indispensables para la adecuada comprensión del mismo, el encargado de ciberseguridad deberá limitarse a incluir solamente aquellos que resulten estrictamente necesarios para dicho fin. Asimismo, en los casos en que la autoridad competente instruya al operador para que envíe a un tercero particular una copia del reporte, deberá eliminar todos los datos de carácter sensible que pudieran figurar en él.

En caso de que a partir del análisis de una ciberincidencia se advierta la ocurrencia de una posible vulneración de datos personales, Subtel o el órgano designado para dicho fin, se deberán remitir los informes pertinentes a la entidad a cargo de la protección de los datos personales competente. Junto con las secciones pertinentes de los reportes, se indicarán los motivos por los que pudo haber existido vulneración de datos personales conforme a la ley Nº 19.628.

Artículo 14. Reportes trimestrales

Los operadores relevantes deberán enviar a Subtel, en forma directa o a través del órgano que ésta designe para dicho fin, reportes periódicos que den cuenta de las modificaciones introducidas en sus redes y sistemas, sean en la capa de software o en elementos de hardware, para dar solución a las vulnerabilidades detectadas en el último período informado. El período de los reportes será aquel que Subtel indique en las instrucciones pertinentes.

Artículo 15. Reportes no obligatorios

Los titulares de redes de servicios de telecomunicaciones que no sean considerados operadores relevantes podrán enviar reportes de ciberincidencias a Subtel o al órgano designado para dichos fines. Asimismo, los operadores relevantes podrán reportar sobre ciberincidencias que no alcancen los umbrales de información obligatoria especificados en el artículo 7º. En cualquier caso, todo reporte de ciberincidencia obligará al operador respectivo a proseguir reportando el desarrollo de ésta, si así correspondiere conforme la presente norma técnica, y a gestionar su resolución.

El operador que deliberadamente omita reportar una ciberincidencia que debió serlo en razón de haber alcanzado o superado los umbrales de gravedad aplicables conforme al artículo 7º, estará sujeto a lo previsto en el artículo 18 de la presente norma técnica.

Por su parte, las autoridades competentes podrán ponderar de diversa manera la prioridad con que se gestionen los informes no obligatorios en relación con los obligatorios.

Artículo 16. Supervisión de seguridad

Los operadores relevantes deberán mantener permanentemente actualizados los planes de gestión de riesgos de las redes y sistemas de telecomunicaciones que utilizan para la prestación los servicios autorizados. Dichos planes deberán formularse de forma que permitan anticipar consecuencias derivadas de amenazas tales como ciberataques y ciberincidencias no hostiles, en base a un análisis y evaluación de los riesgos a los cuales se exponen sus redes y sistemas, con el objetivo de evitar o reducir la ocurrencia de tales contingencias y mitigar sus eventuales efectos, indicando acciones inmediatas y medidas progresivas de mejoras, con sus respectivos indicadores, controles y documentación.

Asimismo, los operadores relevantes deberán someter regularmente sus redes y sistemas de telecomunicaciones a pruebas de seguridad. Las pruebas podrán ser efectuadas por los operadores en forma interna, o bien, con asistencia por parte de terceros externos especializados en dichos servicios, con la opción de solicitar la cooperación y asesoría de Subtel u otra autoridad competente en materia de ciberseguridad. En todo caso, deberán efectuarse conforme estándares actualizados, sean internacionales, independientes o nacionales, o bien, conforme criterios ampliamente aceptados por la industria de las telecomunicaciones. Deberá dejarse constancia de las pruebas efectuadas, los estándares aplicados, los resultados obtenidos y las medidas adoptadas en consecuencia.

Las pruebas de seguridad y simulacros de ciberseguridad deberán considerar, a lo menos, las siguientes actividades de control y documentación:

- Actualización de la última versión del Plan de Gestión de Riesgo.
- Identificación y ordenación de las medidas técnicas para la gestión de riesgo.
- Elaboración del conjunto de pruebas de seguridad a realizar, identificando la infraestructura física y lógica a utilizar.
- Descripción detallada de cada prueba o simulación, el procedimiento de ejecución y los medios de evidencia o verificación del cumplimiento satisfactorio de las pruebas.
- Descripción detallada de las actividades o medidas y procedimientos de restauración para la continuidad operacional y de servicio.
- Verificación de la consistencia y seguridad del almacenamiento de los logs o registros que evidencien los incidentes de ciberseguridad y otros datos tales como direcciones, puertos, aplicaciones, contenidos, datos transmitidos, mensajes de los sistemas sometidos a pruebas o simulación de ciberataque o incidente de ciberseguridad.
- Preparar un reporte con el resultado de las pruebas o simulaciones de seguridad, con medios de verificación apropiados.

La Subsecretaría, en forma directa o a través del órgano designado para dicho fin, podrá requerir a los operadores relevantes toda la información acerca de las redes y sistemas que utilizan y que sea necesaria para evaluar su vulnerabilidad, incluyendo su plan de gestión de riesgos, los resultados de las pruebas de seguridad y, en general, todo otro tipo de antecedentes relacionados con políticas de seguridad de sus redes y sistemas.

Artículo 17. Fiscalización

Sin perjuicio de lo establecido en el artículo 15° de la presente norma técnica, la Subsecretaría podrá fiscalizar en cualquier momento el cumplimiento de las obligaciones contenidas en esta normativa.

Artículo 18. Sanciones

Las infracciones a las disposiciones de la presente norma técnica serán sancionadas de acuerdo a lo dispuesto en el Título VII de la Ley.

****