DIARIO OFICIAL
DE LA REPUBLICA DE CHILE
Ministerio del Interior y Seguridad Pública

I SECCIÓN

LEYES, REGLAMENTOS, DECRETOS Y RESOLUCIONES DE ORDEN GENERAL

Núm. 42.731 | Viernes 14 de Agosto de 2020 | Página 1 de 15

Normas Generales

CVE 1800256

MINISTERIO DE TRANSPORTES Y TELECOMUNICACIONES

Subsecretaría de Telecomunicaciones

APRUEBA NORMA TÉCNICA SOBRE FUNDAMENTOS GENERALES DE CIBERSEGURIDAD PARA EL DISEÑO, INSTALACIÓN Y OPERACIÓN DE REDES Y SISTEMAS UTILIZADOS PARA LA PRESTACIÓN DE SERVICIOS DE TELECOMUNICACIONES

(Resolución)

Núm. 1.318 exenta.- Santiago, 10 de agosto de 2020.

Vistos:

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 Nº 19.628, sobre protección de la vida privada.
d) El decreto supremo Nº 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.
e) El decreto supremo Nº 368, de 2012, del Ministerio de Transportes y Telecomunicaciones, que regula las características y condiciones de la neutralidad de la red en el servicio de acceso a internet.
f) El instructivo presidencial Nº 1/2017, del 27 de abril de 2017, que aprueba e instruye la implementación de la Política Nacional de Ciberseguridad.
g) La resolución Nº 7, de 2019, de la Contraloría General de la República, que fija normas sobre exención del trámite de toma de razón.

Considerando:

a) Que el sostenido incremento en la proporción de habitantes del territorio nacional que acceden cotidianamente a servicios de telecomunicaciones, ha significado que éstos constituyan uno de los principales ámbitos de interacción social. De otra parte, se advierte que una medida sustancial de la actividad económica contemporánea corresponde a una amplia variedad de prestaciones de diversa naturaleza que son provistas, en todo o en parte, mediante el uso de servicios de telecomunicaciones.
b) Que, como consecuencia necesaria de lo expuesto, toda afectación o interrupción importante de los servicios de telecomunicaciones, causará graves perjuicios al bienestar, salud y seguridad de la población; a la integridad de las instituciones públicas e, inclusive, a la seguridad nacional. Dicha relación se volverá progresivamente más significativa en la medida que se extiendan y profundicen los procesos de digitalización. En la misma línea, se advierte que la amplia extensión y comparativa facilidad de acceso de las redes y sistemas de telecomunicaciones, hace que se conviertan en objetivos atractivos para actores criminales.
c) Que la Subsecretaría de Telecomunicaciones, en adelante también e indistintamente “la Subsecretaría” o “Subtel”, tiene como atribuciones dictar las normas técnicas sobre telecomunicaciones y controlar su cumplimiento; requerir los antecedentes e informaciones necesarios para el desempeño de su cometido, tanto de las entidades que operan en el ámbito de las telecomunicaciones como de cualquier organismo público, los que estarán obligados a proporcionarlos; así también, controlar y supervigilar el adecuado funcionamiento de los

servicios públicos de telecomunicaciones y la protección de los derechos del usuario. Lo anterior por expresa disposición del artículo 6º del decreto ley Nº 1.762 en sus literales g) y k), respectivamente, y del artículo 7º de la ley Nº 18.168, Ley General de Telecomunicaciones.

d) Que, adicionalmente, el artículo 6º de la citada ley Nº 18.168 de manera explícita dispone que corresponde al Ministerio de Transportes y Telecomunicaciones, a través de esta Subsecretaría, la aplicación y control de dicha ley y sus reglamentos y que, asimismo, le compete en forma exclusiva la interpretación técnica de las disposiciones legales y reglamentarias que rigen las telecomunicaciones.

e) Que las atribuciones indicadas habilitan legalmente a la Subsecretaría para establecer las condiciones de diseño, instalación y operación de los servicios de telecomunicaciones en cada uno de sus ámbitos, en particular, en lo que concierne a la seguridad de las comunicaciones y al manejo de ciberincidencias, particularmente en el referido sector. Ello busca velar por el adecuado funcionamiento de tales servicios; prevenir o reducir las posibilidades de que sean interrumpidos o afectados por incidentes de seguridad informática; contribuir a prevenir los ataques de que puedan ser objeto los usuarios durante su desenvolvimiento en el ciberespacio y facilitar la posterior investigación de tales hechos. En consecuencia, resulta procedente regular determinados aspectos de la operación de las redes destinadas a la prestación de los servicios de telecomunicaciones regulados por la ley Nº 18.168, con el fin de lograr los objetivos planteados.

f) Que el reglamento que trata sobre la declaración y resguardo de la infraestructura crítica de telecomunicaciones, aprobado mediante el decreto supremo Nº 60, de 2012, del Ministerio de Transportes y Telecomunicaciones, constituye una normativa cuyo ámbito de aplicación se enfoca principalmente en los elementos de la red que soportan la infraestructura física, con menor énfasis en la infraestructura lógica, protocolos, software, sistemas y datos informáticos y contenido mismo de las comunicaciones. Esta insuficiencia regulatoria obliga a tomar las providencias del caso en favor de los derechos del usuario y del buen funcionamiento de los servicios de telecomunicaciones, dictando la correspondiente norma técnica en la materia.

g) Que el reglamento que regula las características y condiciones de la neutralidad de la red en el servicio de acceso a internet, aprobado mediante decreto supremo Nº 368, de 2012, del Ministerio de Transportes y Telecomunicaciones, impone a los proveedores de acceso a internet la obligación de preservar la privacidad de los usuarios, la protección contra virus y la seguridad de la red, utilizando para ello las herramientas tecnológicas disponibles. Sin embargo, dicha normativa no regula la obligación de reportar a la autoridad competente las ciberincidencias que afecten la normal provisión del servicio ni la de proceder a su resolución y prevenir su ocurrencia, vacío normativo que es abordado por las disposiciones contenidas en la presente norma técnica.

Resuelvo:

Apruébase la presente norma técnica sobre fundamentos generales de ciberseguridad para el diseño, instalación y operación de redes y sistemas utilizados para la prestación de servicios de telecomunicaciones:

Título I. Disposiciones generales

Artículo 1º. 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 ser diseñadas, instaladas y operadas de manera segura las redes y sistemas utilizados para la prestación de servicios de telecomunicaciones regulados por la ley Nº18.168, Ley General de Telecomunicaciones, en adelante “la Ley”. Lo anterior, habida consideración al resguardo y a la resiliencia de las redes, sistemas y su continuidad operacional, confidencialidad, integridad y disponibilidad de la información.

La presente norma cubre aspectos de gestión de riesgo en materias de ciberseguridad en el ámbito de los servicios de telecomunicaciones regulados por la Ley, identificando tanto el análisis de impacto operacional como los riesgos y controles mitigantes; además del ciclo de vida de una ciberincidencia, considerando tanto la prevención, detección, análisis, notificación, contención, erradicación, recuperación y documentación a su respecto.

De igual manera, esta norma técnica busca normar los reportes sobre ciberincidencias que los concesionarios y permisionarios de servicios de telecomunicaciones deben enviar a la Subsecretaría, sea directamente o a través del órgano que ésta indique, con el objeto de coordinar

las acciones orientadas a mitigar sus efectos e impactos y contribuir a una oportuna normalización y estabilización de los servicios afectados.

Artículo 2º. Definiciones

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

- Autenticación:
Proceso utilizado en los mecanismos de control de acceso con el objetivo de verificar la identidad de un usuario, dispositivo o sistema mediante la comprobación de credenciales de acceso.

- Ciberespacio:
Dominio global y dinámico dentro del entorno de la información que corresponde al ambiente compuesto por las infraestructuras tecnológicas, los componentes lógicos de la información, los datos (almacenados, procesados o transmitidos) que abarcan los dominios físico, virtual y cognitivo 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.

- Ciberincidencia o ciberincidente:
Todo evento que comprometa la disponibilidad, autenticidad, integridad o confidencialidad de los sistemas o datos informáticos almacenados, transmitidos o procesados, o los servicios correspondientes ofrecidos por los sistemas de telecomunicaciones y su infraestructura, que puedan afectar al normal funcionamiento de los mismos.

- Ciberseguridad:
Conjunto de acciones posibles para la prevención, mitigación, investigación y manejo de las amenazas e incidentes sobre los activos de información, datos y servicios, así como para la reducción de los efectos de los mismos y del daño causado antes, durante y después de su ocurrencia.

- Ciberataque:
Cualquier incidente cibernético, provocado deliberadamente y que afecte a un sistema informático.

- Confidencialidad:
Principio de seguridad que requiere que los datos deberían únicamente ser accedidos por el personal autorizado a tal efecto.

- Disponibilidad:
Capacidad de ser accesible y estar listo para su uso a demanda de una entidad autorizada.

- Equipo de Respuesta ante Incidentes de Seguridad Informática, en adelante “CSIRT”:
Centros conformados por especialistas multidisciplinarios capacitados para prevenir, detectar, gestionar y responder a incidentes informáticos, en forma rápida y efectiva, y que actúan según procedimientos y políticas predefinidas, coadyuvando asimismo a mitigar los efectos de ataques de ciberseguridad.

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

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

- Infraestructura crítica de telecomunicaciones:

Es el conjunto de redes y sistemas de telecomunicaciones cuya interrupción, perturbación, degradación, 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 lo señalado en el reglamento sobre 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.

- Integridad:

Principio de seguridad que certifica que los datos y elementos de configuración sólo son modificados por personal y actividades autorizadas. La Integridad considera todas las posibles causas de modificación, incluyendo fallos software y hardware, eventos medioambientales e intervención humana.

- Neutralidad tecnológica:

Principio regulatorio conforme el cual las normas técnicas destinadas a limitar las externalidades negativas de una actividad deben describir el resultado que se logrará, pero otorgando a los regulados libertad para adoptar la tecnología más apropiada para lograr el resultado, asimismo, implica aplicar unos mismos principios reguladores indistintamente de qué tecnología es utilizada y que la regulación no sea usada como un medio para impulsar el mercado hacia una estructura particular que el regulador considera óptima.

- No repudio:

Servicio de seguridad que provee al emisor y receptor de los datos de una prueba del origen y destino de los mismos, que puede usarse ante intentos del emisor o receptor de negar su remisión.

- Operador relevante:

Todo proveedor de servicio público, intermedio o limitado de telecomunicaciones que haya sido declarado como relevante por Subtel mediante resolución fundada para los efectos de la presente norma, así como todas aquellas entidades que operen sistemas de telecomunicaciones que hayan sido declarados como infraestructura crítica de Nivel 1 o Nivel 2 conforme el reglamento pertinente. Asimismo, serán considerados operadores relevantes los ISP Relevantes Móviles y los ISP Relevantes Fijos.

- ISP Relevante Fijo:

Proveedor del servicio de transmisión de datos fijo que por sí solo o en conjunto con otros ISP filiales, coligados o relacionados en los términos dispuestos por las leyes Nº 18.045, de Mercado de Valores, y Nº 18.046, sobre Sociedades Anónimas, y que utilicen la misma infraestructura central para la prestación de servicio de conectividad a Internet a los usuarios finales, atienda a más del 10% del total de suscriptores o usuarios del servicio de acceso a Internet fijo a nivel nacional.

- ISP Relevante Móvil:

Proveedor del servicio de transmisión de datos móvil que por sí solo o en conjunto con otros ISP filiales, coligados o relacionados en los términos dispuestos por las leyes Nº 18.045, de Mercado de Valores, y Nº 18.046, sobre Sociedades Anónimas, y que utilicen la misma infraestructura central para la prestación de servicio de conectividad a Internet a los usuarios finales, atienda a más del 10% del total de suscriptores o usuarios del servicio de acceso a Internet móvil a nivel nacional.

- Resiliencia:

Capacidad de los sistemas o redes para seguir operando pese a estar sometidos a un incidente o ciberataque, aunque sea en un estado degradado, debilitado o segmentado. Así como, incluye la capacidad de restaurar con presteza sus funciones esenciales después de un incidente o ataque de modo de recuperarse con presteza de una interrupción, por lo general con un efecto reconocible mínimo.

- 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 3º. Ámbito de aplicación

Las disposiciones contenidas en esta norma técnica se aplican al diseño, instalación, operación y optimización de las redes y los sistemas utilizados para la prestación de servicios de telecomunicaciones regulados por la Ley Nº 18.168, General de Telecomunicaciones. En consecuencia, se excluyen del ámbito de estas disposiciones los sistemas informáticos destinados a la administración de la empresa proveedora.

Artículo 4º. Declaración de relevancia

Todo prestador de servicios de telecomunicaciones que opere redes y sistemas que hayan sido declarados como infraestructura crítica por esta Subsecretaría, será considerado operador relevante para todos los efectos de la presente norma técnica, sin necesidad de declaración adicional. De igual manera, se considerará operadores relevantes para los efectos de la presente norma a todos los operadores de servicios de telecomunicaciones móviles que operen en seis o más regiones del país o que tengan más de 200.000 suscriptores o usuarios titulares.

Sin perjuicio de lo anterior, Subtel podrá declarar un proveedor de servicios de telecomunicaciones como operador relevante exclusivamente para los fines de la presente norma técnica. Dicha declaración se efectuará mediante resolución fundada en la que se dejará constancia tanto de los factores 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 únicamente para los fines de la presente norma técnica, la Subsecretaría tendrá en consideración, a lo menos, lo siguiente:

a) Zona de servicio en tres o más regiones contiguas o cuatro no contiguas;

b) Atención a empresas declaradas como estratégicas por el Ministerio de Economía, Fomento y Turismo;

c) Participación de mercado igual o superior al 5%, a nivel nacional;

d) Cantidad de usuarios atendidos igual o superior a 50.000.

Previo a la declaración, la Subsecretaría comunicará a los operadores su decisión de estudiar su situación con la finalidad de estudiar su relevancia para la aplicación de la presente norma técnica, solicitándole información pertinente para dicho fin. Los operadores tendrán un plazo máximo de dos meses a contar de la comunicación antes señalada para enviar a la Subsecretaría la información solicitada y sus observaciones fundamentadas, con indicación del impacto social de la interrupción, destrucción, corte o fallo de los sistemas de telecomunicaciones respectivos, así como la viabilidad técnica y económica de la implementación de las medidas que resulten de la declaración de relevancia.

En base a la información y observaciones proporcionadas, la Subsecretaría determinará la necesidad de declarar la relevancia del operador estudiado. Los operadores podrán reclamar de esta declaración conforme lo establecido en la ley Nº 19.880.

El procedimiento de declaración de relevancia tendrá una revisión cada cuatro años, con el objeto de actualizar las definiciones de acuerdo con los cambios tecnológicos, las modificaciones realizadas en los sistemas de telecomunicaciones y la experiencia obtenida.

Asimismo, a efectos de asegurar la continuidad de las comunicaciones, considerará para la definición de relevancia la necesidad de contar con una pluralidad de sistemas de telecomunicaciones, susceptibles de interconectarse y/o interoperar, incluyendo los sistemas físicos y lógicos que sobre dichos sistemas de telecomunicaciones se soportan y que permiten la comunicación de los usuarios entre sí.

Título II. Medidas generales de ciberseguridad

Artículo 5º. Obligaciones generales de Ciberseguridad

1. Medidas de gestión.

Todo operador de servicios públicos de transmisión de datos, indistintamente de si es o no relevante, deberá implementar medidas técnicas y de organización para gestionar los riesgos de ciberseguridad de las redes y sistemas que utiliza para la prestación de servicios de telecomunicaciones a sus usuarios, indistintamente de si tal gestión estuviere o no externalizada.

Cada operador deberá determinar y adoptar las medidas de gestión que sean necesarias para garantizar la disponibilidad, integridad y confidencialidad de las redes y sistemas que utilizan para prestar servicios de telecomunicaciones, de conformidad con el tipo de organización, la naturaleza y contexto de los servicios prestados, los riesgos asociados y la tecnología disponible, teniendo en cuenta, a lo menos, los siguientes conceptos:

a) seguridad física y ciberseguridad de los sistemas e instalaciones;
b) resiliencia de la red;
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) conocimiento de las alertas de ciberincidencias a nivel nacional e internacional;
i) actualización constante de protocolos y sistemas de seguridad;
j) seguridad en los componentes tecnológicos de los equipos para los servicios entregados, que garanticen adecuadamente la integridad, confidencialidad y disponibilidad de las transmisiones;
k) calificación, capacitación y seguridad del personal que opera los componentes tecnológicos;
l) los principios y estándares internacionalmente aceptados en materia de ciberseguridad, tales como, y sin ser taxativos, International Organization for Standardization (ISO), Organisation for Economic Cooperation and Development (OCDE), International Telecommunication UnionI (ITU) y The 3rd Generation Partnership Project (3GPP).

2. Medidas de prevención y mitigación.

De igual forma, los operadores 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 o nacionales, de amplia aplicación y, a su vez, desde el punto de vista de los usuarios, garantizar la integridad, disponibilidad y confidencialidad de la información.

3. Análisis de riesgo y seguridad por diseño.

El uso intensivo de tecnologías de la información en el diseño, desarrollo y ejecución de una multiplicidad de procesos cotidianos y críticos de cada una de las instituciones públicas y privadas, han incrementado el nivel de dependencia y vulnerabilidad propia de estas tecnologías, que deben ser abordados de manera sistémica y con enfoque en la gestión de riesgo.

El despliegue de nuevas tecnologías traerá una compleja amenaza a la ciberseguridad. En general, las amenazas consideradas más relevantes son las relacionadas al compromiso de la confidencialidad, disponibilidad e integridad de la información.

En lo específico, existe una serie de escenarios de amenazas dirigidos a la implementación de nuevas tecnologías, siendo estas:

• Interrupción de la red local o global (disponibilidad);
• Captura no autorizada de tráfico / datos en la infraestructura de red (confidencialidad);
• Modificación o redireccionamiento del tráfico / datos en la infraestructura de red (integridad y/o confidencialidad);

• Destrucción o alteración de otras infraestructuras o información digital, a través de las redes (integridad y/o disponibilidad);
• Interceptación de cualquier forma de comunicación.

La gravedad de los escenarios de amenazas específicas para la implementación de nuevas tecnologías podrá variar de acuerdo a varios factores, en particular los que se destacan:

• La severidad del daño;
• El número y tipo de usuarios afectados;
• La duración del evento antes de la detección o remediación;
• El tipo de servicios afectados (seguridad pública, servicios de emergencia, salud, actividades gubernamentales, electricidad, agua, etc.) y el alcance del daño;
• El tipo de información alterada/modificada/desvío de tráfico.

Los operadores de servicios de telecomunicaciones desde las etapas de concepción, planeamiento y diseño de sus redes, sistemas y procesos y, en general, durante toda gestión anterior a la operación, deberán aplicar criterios orientados a minimizar los riesgos de ciberincidencias y a facilitar una adecuada gestión de éstas durante su operación, mantención y optimización.

El diseño, instalación y operación de redes y sistemas utilizados en la prestación de servicios de telecomunicaciones regulados por la ley Nº 18.168, deberá considerar el desarrollo de procesos de análisis y gestión de riesgos que permitan identificar las vulnerabilidades, amenazas y riesgos implícitos en el uso, procesamiento, almacenamiento y transmisión de la información; considerando la protección, detección, respuesta y recuperación ante incidentes de ciberseguridad que se presenten, contribuyendo a un ciberespacio seguro y resiliente.

Para la implementación de nuevas tecnologías, los operadores y proveedores deberán garantizar la operación y seguridad de las partes sensibles de sus redes, así como también la obligación de resguardar la confidencialidad, disponibilidad e integridad de la información que se transmita por sus tecnologías.

Con el objeto de garantizar la ciberseguridad en la implementación de nuevas tecnologías, los operadores y proveedores de servicios deberán considerar un conjunto de medidas de mitigación, las cuales deberán abordar todo tipo de riesgos de Ciberseguridad. Lo anterior será validado y aprobado por el operador y presentado a Subtel u organismo competente.

4. Planes de gestión de riesgo.

Los operadores deberán contar con planes de gestión de riesgos de ciberseguridad 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.

Al menos una vez al año los planes de gestión de riesgo deberán ser sometidos a conocimiento y aprobación del directorio o alta gerencia del operador. La presentación que se haga deberá mencionar el estado de los riesgos de ciberseguridad e indicadores clave, con los incidentes y planes de acción de mejoras. Se entregará a Subtel una versión de la presentación de la cual el operador podrá omitir la información no pertinente a ciberseguridad, y que será tratada con la debida reserva.

5. Documentación de planes de gestión.

La documentación y demás antecedentes que den cuenta del detalle de los planes de gestión de riesgos deberán estar permanentemente disponibles en caso de inspecciones a realizar por Subtel o con la finalidad 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 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.

6. Circunstancias especiales.

No obstante lo dispuesto en este artículo, la Subsecretaría de Telecomunicaciones podrá establecer, en consideración a circunstancias especiales de vulnerabilidad y mediante resolución debidamente fundada, que determinados operadores deban adoptar los estándares técnicos o medidas precisas de operación de redes que la autoridad indique en la forma que sea legalmente procedente.

Título III. Unidades de ciberseguridad

Artículo 6º. Unidades de ciberseguridad

Todo operador relevante deberá contar con un equipo de respuesta para la adecuada gestión de la ciberseguridad. Además, deberá contar permanentemente con una unidad de ciberseguridad integrada por, a lo menos, un titular y un suplente, quienes deberán poseer las competencias suficientes en dichas materias 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 de ciberseguridad con las autoridades competentes.

Todo operador no relevante deberá contar permanentemente con, a lo menos, un encargado titular de ciberseguridad en funciones y un suplente, quienes deberán poseer las competencias suficientes en dichas materias, 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 de ciberseguridad con las autoridades competentes.

Los operadores 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, dando cuenta oportunamente en caso que exista alguna modificación al respecto.

Título IV. Reporte obligatorio de ciberincidentes

Artículo 7º. Obligación de reportar ciberincidencias

Los operadores deberán reportar oportunamente a la Subsecretaría de Telecomunicaciones, al CSIRT de referencia o al órgano que designe para dichos fines, acerca de todas las ciberincidencias que detecte en sus redes y sistemas y que alcancen los Niveles de peligrosidad e impacto establecidos en esta normativa, sin perjuicio de las instrucciones precisas que emita Subtel respecto de tipos específicos de incidentes.

Como criterio de referencia para el reporte de una ciberincidencia se utilizará el Nivel de peligrosidad que se le asigne conforme la tabla indicada más adelante. Sin perjuicio de lo anterior, a lo largo del desarrollo, mitigación o resolución de la ciberincidencia, se categorizará con un Nivel de impacto que determinará la obligatoriedad de su reporte a Subtel, al CSIRT de referencia o al órgano designado por Subtel para dichos fines. En caso de que un suceso pueda asociarse con dos o más tipos de incidentes con niveles de peligrosidad distintos, se le asignará el nivel de peligrosidad más alto.

A. Niveles de peligrosidad.

El Nivel de peligrosidad determina la potencial amenaza que supondría la materialización de un incidente en las redes y sistemas del operador, así como para la calidad o continuidad de servicios prestados. Este indicador se fundamenta en las características intrínsecas a la tipología de amenaza.

Conforme sus características, las amenazas serán clasificadas con los siguientes niveles de peligrosidad: Crítico, Muy Alto, Alto, Medio y Bajo. El nivel asignado se determinará según se indica en la tabla a continuación:

Nivel de Peligrosidad		
Nivel	Clasificación	Tipo de incidente
Crítico	Otros	Amenaza Avanzada Persistente
Muy alto	Código dañino	Distribución de malware Configuración de malware
	Intrusión	Robo Sabotaje
	Disponibilidad del servicio	Interrupciones
Alto	Contenido abusivo	Pornografía infantil, contenido sexual o violento inadecuado
	Código Dañino	Sistema infectado Servidor C&C (Mando y Control)
	Intrusión	Compromiso de aplicaciones Compromiso de cuentas con privilegios
	Intento de Intrusión Disponibilidad del servicio Compromiso de la información Fraude	Ataque desconocido DoS (Denegación de servicio) DDoS (Denegación distribuida de servicio) Acceso no autorizado a información
		Modificación no autorizada de información
		Pérdida de datos Phishing
Medio	Contenido abusivo	Discurso de odio
	Obtención de información	Ingeniería social Explotación de vulnerabilidades conocidas.
	Intrusión	Intento de acceso con vulneración de credenciales. Compromiso de cuentas sin privilegios.
	Disponibilidad del servicio	Mala configuración Uso no autorizado de recursos
	Fraude	Derechos de autor Suplantación
	Vulnerable	Criptografía débil Amplificador DDoS
		Servicios con acceso potencial no deseado
		Revelación de información Sistema vulnerable
Bajo	Contenido abusivo Obtención de información Otros	Spam Escaneo de redes
		Análisis de paquetes (sniffing) Otros

B. Niveles de impacto.

Los criterios empleados para la determinación del nivel de impacto asociado a un ciberincidente atienden los parámetros que se indican a continuación, sin un orden de prelación o importancia predeterminado:

- Impacto en la Seguridad Nacional o en la Seguridad Ciudadana.
- Efectos en la prestación de un servicio de telecomunicaciones o en una infraestructura crítica.
- Tipología de la información o sistemas afectados.
- Grado de afectación a las instalaciones de la organización.
- Posible interrupción en la prestación del servicio normal de la organización.
- Tiempo y costes propios y ajenos hasta la recuperación del normal funcionamiento de las instalaciones.
- Pérdidas económicas.
- Extensión geográfica afectada.
- Daños reputacionales asociados.

Los posibles niveles de impacto de una ciberincidencia son Crítico, Muy Alto, Alto, Medio, Bajo o Sin Impacto. El nivel de impacto correspondiente se asignará usando como referencia la siguiente tabla:

Niveles de impacto de ciberincidencias	
Nivel	Descripción
Crítico	Afecta apreciablemente a la Seguridad Nacional. Afecta a la seguridad ciudadana, con potencial peligro para la vida de las personas.
	Afecta a elementos declarados como Infraestructura Crítica por Subtel. Afecta a sistemas clasificados como confidenciales.
	Afecta a más del 90% de los sistemas del operador. Interrupción en la prestación del servicio superior a 24 horas y superior al 50% de los usuarios.
	La ciberincidencia requiere más de 800 horas hombre (HH), para su resolución.
	Extensión geográfica nacional o supranacional.
	Daños reputacionales muy elevados y cobertura continua en medios de comunicación nacionales como internacionales.
Muy alto	Afecta a la seguridad ciudadana con potencial peligro para bienes materiales.
	Afecta apreciablemente a actividades oficiales o misiones en el extranjero.
	Afecta a un servicio esencial.
	Afecta a sistemas clasificados como reservado. Afecta a más del 75% de los sistemas del operador.
	Interrupción en la prestación del servicio superior a 8 horas y superior al 35% de los usuarios. El ciberincidente precisa para resolverse entre 30 personas y 800 HH.
	Extensión geográfica igual o superior a 4 regiones o de 1 territorio de interés especial.
Alto	Afecta a más del 50% de los sistemas del operador.
	Interrupción en la prestación del servicio superior a 1 hora y superior al 10% de usuarios.
	La ciberincidencia requiere entre 5 personas y 240 HH, para su resolución.
	Extensión geográfica igual o superior a 3 regiones.
	Daños reputacionales de difícil reparación, con eco mediático (amplia cobertura en los medios de comunicación) y afectando a la reputación de terceros.
Medio	Afecta a más del 20% de los sistemas de la entidad. Interrupción en la presentación del servicio superior al 5% de usuarios.
	La ciberincidencia requiere entre 1 persona y 40 horas hombre (HH), persona para su resolución. Extensión geográfica igual o superior a 2 regiones.
	Daños reputacionales de difícil reparación, con eco mediático (amplia cobertura en los medios de comunicación) y afectando a la reputación de terceros.
Bajo	Afecta a los sistemas del operador. Interrupción de la prestación de un servicio. La ciberincidencia requiere menos de 1 persona para su resolución.
	Extensión geográfica igual o superior a 1 región
Sin impacto	Daños reputacionales puntuales, sin eco mediático. No hay ningún impacto apreciable.

C. Ciberincidencias de reporte obligatorio.

Las ciberincidencias se asociarán a los niveles de peligrosidad e impacto que les correspondan de conformidad con lo dispuesto en el presente artículo, siendo obligatorio el reporte de todas aquellas que alcancen niveles Crítico, Muy Alto o Alto.

Los operadores deberán reportar en tiempo y forma todas las ciberincidencias que registren en sus redes y sistemas de información y estén obligados a notificar por superar los umbrales de impacto o peligrosidad dispuesto en el presente artículo. Sin perjuicio de lo anterior, Subtel podrá establecer reglas de reportes especiales aplicables a tipos específicos de incidentes o territorios de interés especial.

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 para operadores no relevantes, en caso de que éstos no se encontrasen disponibles. Con todo, cualquier consulta adicional, generará una nueva obligación para el operador relevante de reportar, dentro del plazo señalado en el propio requerimiento.

El operador que deliberadamente omita reportar una ciberincidencia de reporte obligatorio, estará sujeto a lo previsto en el artículo 18 de la presente norma técnica.

Artículo 8º. Contenido de los reportes

Los sujetos obligados por la presente norma, deberán reportar en tiempo y forma toda aquella información relativa a la ciberincidencia que sea exigible. Sin embargo, en el reporte inicial solamente deberá proporcionar la información que tenga en su conocimiento en ese momento, debiendo completarla en los reportes que envíe con posterioridad.

Los reportes de ciberincidencias deberán contener, a lo menos, los siguientes campos de información:

a. Resumen ejecutivo de la ciberincidencia.
b. Identificación del operador relevante.
c. Encargado de ciberseguridad en funciones.
d. Fecha y hora precisas de ocurrencia de la ciberincidencia.
e. Fecha y hora precisas de detección de la ciberincidencia.
f. Descripción detallada de lo sucedido.
g. Recursos tecnológicos afectados.
h. Origen o causa identificable de la ciberincidencia.
i. Taxonomía, clasificación o tipo de ciberincidencia.
j. Nivel de peligrosidad.
k. Nivel de impacto.
l. Impacto transfronterizo, si corresponde.
m. Indicadores de compromiso: indicadores de compromiso de nivel IP, indicadores de compromiso de nivel de dominios y subdominios, indicadores de compromiso de correos, indicadores de compromiso a nivel MD5, entre otros similares.
n. Plan de acción y medidas de resolución y mitigación.
o. Afectados actuales y potenciales.
p. Medios necesarios para la resolución calculados en horas hombre (HH) / persona.
q. Impacto económico estimado, si procede y es conocido.
r. Extensión geográfica, si se conoce.
s. Daños reputacionales, aun cuando sean eventuales.
t. Las bitácoras generadas de forma automática por los sistemas.
u. Antecedentes que se adjuntan, si procede.

En el caso particular de ciberincidencias que afecten o puedan afectar infraestructuras críticas, el reporte deberá indicar los motivos por los que un reporte no contiene toda la información pertinente, la que deberá ser enviada tan pronto como sea obtenida.

Para ciberincidentes que afecten a infraestructuras críticas o impacten sectores estratégicos, el operador deberá contratar un análisis independiente forense, indicando las medidas tomadas para su correcta mitigación y solución.

Artículo 9º. Oportunidad de los reportes.

Los operadores que se vean afectados por una ciberincidencia deberán generar un reporte obligatorio, el cual deberá ser remitido en tiempo y forma, considerando un reporte inicial, reportes intermedios y un reporte final.

El reporte inicial es una comunicación consistente en poner en conocimiento y alertar de la existencia de una ciberincidencia.

Los reportes intermedios actualizan los datos disponibles en ese momento en relación a la ciberincidencia comunicada. Se efectuarán tantos reportes intermedios como se consideren necesarios a partir de la hora en que se generó el reporte inicial inmediato.

El reporte final amplía y confirma los datos definitivos en relación a la ciberincidencia reportada a partir del día en que se generó el reporte inicial inmediato.

El envío del reporte se realizará siempre que sea posible por escrito usando los medios indicados por Subtel para ello o, en caso de no estar disponibles, mediante correo electrónico, o en su defecto, por el medio más idóneo que se encuentre disponible.

Oportunidad de reportes obligatorios			
Nivel de peligrosidad o impacto	Reporte inicial	Reporte intermedio	Reporte final
Crítico	Inmediato	3 / 6/ 12 / 24 / 48 horas	Máximo 10 días
Muy alto	Inmediato	48 / 72 horas	Máximo 20 días
Alto	Inmediato	Sin plazo	Máximo 30 días

Los reportes deberán enviarse en forma oportuna y sucesiva conforme el desarrollo de la ciberincidencia, incorporando toda la información que sea pertinente y reportando cada cambio sustancial a medida que suceda. Además, el operador deberá aplicar las medidas de seguridad durante el proceso de transmisión de los reportes de incidencias.

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.

Artículo 10º. Tratamiento de los reportes

Los reportes de ciberincidencias serán tratados como documentación confidencial por los organismos del Estado que tomen conocimiento de ellos. En particular, en aquellos datos que pudiera exponer antecedentes técnicos propios del operador, que pongan en riesgo la ciberseguridad del operador, así como la información de clientes en conformidad a la legislación sobre protección de la vida privada.

Título V. Información a terceros e intercambio de información

Artículo 11º. Información a terceros e intercambio de información

En caso de reportar y/o alertar a terceros para prevenir, gestionar o resolver una ciberincidencia, el operador relevante podrá solicitar la asistencia de Subtel o del CSIRT de referencia u otro órgano designado por Subtel para dichos efectos, si procediese. En caso de requerir apoyo de Equipos de Respuesta en el extranjero, el operador deberá velar por la privacidad y el debido resguardo de los datos involucrados.

Por su parte, la Subsecretaría de Telecomunicaciones, el CSIRT de referencia o el órgano designado por Subtel para dichos fines, actuará en conformidad a las indicaciones que figuren en los reportes respecto del alcance que puede tener la difusión de la información que contiene conforme el estándar Traffic Light Protocol o TLP. En caso de estimarse que es necesario difundir la información a terceros más allá del alcance de la designación TLP indicada por el autor del reporte, se requerirá autorización de la fuente original. En general, no se revelarán cualesquiera datos que pudieran exponer antecedentes técnicos propios del operador, que pongan en riesgo la ciberseguridad del operador, así como cualquier información de sus usuarios, conforme lo dispuesto en ley sobre protección de la vida privada.

En caso de que se 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, 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 de los involucrados.

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

Título VI. Resolución de ciberincidentes

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 afectado lo considere necesario para la resolución de una ciberincidencia, podrá solicitar cooperación a la Subsecretaría u otras entidades competentes en materia de ciberseguridad, tales como el CSIRT de referencia señalado por Subtel u otros equipos de respuesta ante incidentes informáticos.

Los operadores deberán proporcionar la información adicional que les sea requerida para analizar la naturaleza, causas y efectos de los incidentes notificados, así como 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 fin alguno que sea distinto 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 deberán subsanar, en la medida que sea técnicamente posible, según los respaldos fundados, las vulnerabilidades de sus sistemas que hubieren permitido o facilitado ciberincidencias.

En caso de que un operador detecte que sus redes y sistemas fueron utilizados como medio para la comisión de algún delito informático, el operador deberá formular las denuncias ante los órganos competentes, ejercer las acciones judiciales pertinentes e informar a Subtel.

Todo operador será responsable, previo proceso sustanciado de conformidad a la Constitución y las leyes, por las pérdidas o filtración de información que sea producto de su negligencia con respecto a la recepción, tenencia, manipulación, almacenamiento y entrega de la información que se transmite o deposita en custodia en los sistemas del proveedor, para garantizar la certeza, confidencialidad, seguridad y no repudiación de la comunicación.

El operador debe establecer los protocolos de recuperación de la información en caso de pérdida de esta por manipulación, ciberincidentes u otras causas de su responsabilidad.

Artículo 13°. Resguardo de datos personales y datos sensibles

Deberán omitirse en los reportes de ciberincidencias todo dato o información personal de carácter sensible, así como toda otra información a partir de la cual sea posible inferirlos. Asimismo, en los casos en que la autoridad competente instruya al operador para que envíe a un tercero una copia de un reporte, deberá eliminar todos los datos personales o que permitan deducir la identidad de la persona aludida.

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, deberá 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.

En todos los casos, deberán considerarse las regulaciones de utilización de la información del usuario y su metadata, ya sea para beneficio propio del operador o de terceros, sin la expresa

autorización del cliente, conforme lo establecido en el artículo 9º de la citada ley Nº19.628, sobre Protección de la Vida Privada y conforme los principios transversales de derechos humanos reconocidos por la comunidad internacional.

Título VII. Reportes obligatorios sobre modificación a las redes y sistemas

Artículo 14°. Reportes periódicos

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 trimestral.

Las exigencias de reportes mencionadas anteriormente serán obligatorias semestralmente para los operadores no relevantes.

Subtel utilizará la información proporcionada en los reportes periódicos únicamente con fines estadísticos y para estudios destinados a la formulación de políticas.

Título VIII. Reportes no obligatorios

Artículo 15°. Reportes no obligatorios

Los proveedores de servicios de telecomunicaciones que no sean considerados operadores relevantes podrán enviar reportes de ciberincidencias a Subtel, al CSIRT de referencia o al órgano designado para dichos fines. Asimismo, todo proveedor de servicios de telecomunicaciones podrá 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.

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.

Título IX. Supervisión de seguridad

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 de 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, con la frecuencia que corresponda de acuerdo al plan de riesgo aprobado y sancionado por su alta dirección. 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 nacionales o internacionales, 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.

Título X. Disposiciones finales

Artículo 17°. Fiscalización

Sin perjuicio de lo establecido en el artículo 15º 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.

Artículo 19°. Entrada en vigencia

La presente norma técnica entrará en vigencia a contar de su publicación en el Diario Oficial.

Anótese y publíquese en el Diario Oficial.- Pamela Gidi Masías, Subsecretaria de Telecomunicaciones.

Lo que transcribo para su conocimiento.- Saluda atentamente a usted, Adolfo Oliva Torres, Jefe División Política Regulatoria y Estudios.