APRUEBA REGLAMENTO DE REPORTE DE INCIDENTES DE CIBERSEGURIDAD

Artículo único: Apruébese el reglamento de reporte de incidentes de ciberseguridad.

TÍTULO I
Aspectos Generales

Artículo 1°. De las definiciones. Para efectos del presente Reglamento se entenderá por:

a) Agencia: Agencia Nacional de Ciberseguridad.

b) Ciberataque: Todo intento de destruir, exponer, alterar, deshabilitar, exfiltrar u obtener acceso o hacer uso no autorizado de un activo informático.

c) Equipo de Respuesta a Incidentes de Seguridad Informática o CSIRT: centros multidisciplinarios que tienen por objeto prevenir, detectar, gestionar y responder a incidentes de ciberseguridad o ciberataques, en forma rápida y efectiva, y que actúan conforme a procedimientos y políticas predefinidas, ayudando a mitigar sus efectos.

d) Director o Directora: Director o Directora de la Agencia Nacional de Ciberseguridad

e) Información: Información generada, almacenada o transmitida por sistemas informáticos.

f) Informe: reporte electrónico que contiene los antecedentes fácticos y tecnológicos respecto de un incidente, ciberataque elaborado por una institución que hubiere o pudiere ser afectada.

g) Ley: ley N° 21.663, marco de Ciberseguridad.

h) Operadores de importancia vital: Aquellos proveedores de servicios esenciales y aquellas instituciones privadas que, sin tener la calidad de proveedores de servicios esenciales, han sido calificados como tales, de conformidad a lo dispuesto en el artículo 5° de la Ley y su Reglamento.

i) Plataforma: Sistema tecnológico dispuesto por la Agencia Nacional de Ciberseguridad para realizar el reporte de incidentes dispuesto en el artículo 2° de este Reglamento.

j) Servicios esenciales: aquellos provistos por los organismos de la Administración del Estado y por el Coordinador Eléctrico Nacional; los prestados bajo concesión de servicio público, y los proveídos por instituciones privadas que realicen las siguientes actividades:

generación, transmisión o distribución eléctrica; transporte, almacenamiento o distribución de combustibles; suministro de agua potable o saneamiento; telecomunicaciones, infraestructura digital; servicios digitales y servicios de tecnología de la información gestionados por terceros; transporte terrestre, aéreo, ferroviario o marítimo, así como la operación de su infraestructura respectiva; banca, servicios financieros y medios de pago; administración de prestaciones de seguridad social; servicios postales y de mensajería; prestación institucional de salud por entidades tales como hospitales, clínicas, consultorios y centros médicos, y la producción y/o investigación de productos farmacéuticos y aquellos que hubieren sido calificados como tales de conformidad a lo dispuesto en el inciso tercero del artículo 4° de la Ley.

k) Vulnerabilidad: debilidad de un activo o control que puede ser explotado por una o más amenazas informáticas.

Artículo 2°. Del deber de reportar. Las instituciones públicas y privadas que presten servicios esenciales y aquellas que hubieren sido calificadas como operadores de importancia vital de conformidad a la Ley y su Reglamento, tendrán la obligación de reportar al CSIRT Nacional los ciberataques e incidentes de ciberseguridad que puedan tener efectos significativos.

TÍTULO II
De los incidentes y de la plataforma de reportes

Artículo 3°. Incidente de ciberseguridad. Para efectos del presente reglamento se considerará un incidente de ciberseguridad todo evento que perjudique o comprometa la confidencialidad o integridad de la información, la disponibilidad o resiliencia de las redes y sistemas informáticos; o la autenticación de los procesos ejecutados o implementados en las redes y sistemas informáticos, de una o más instituciones.
.

Artículo 4°. Incidente de ciberseguridad con efecto significativo. Se considerará que un incidente de ciberseguridad tiene efecto significativo si es capaz de producir alguno de los siguientes efectos:

a) Interrumpir la continuidad de un servicio esencial. En dicho caso deberá considerarse, tanto los servicios entregados por proveedores, como la cadena de suministro, de una institución que preste servicios esenciales o de un operador de importancia vital.
b) Afectar la integridad física o la salud de las personas; o
c) Afectar sistemas informáticos que contengan datos personales.

Para determinar la importancia de los efectos de un incidente de ciberseguridad se deberán tener en consideración, especialmente, alguno de los siguientes criterios: número de personas afectadas; duración del incidente; o la extensión geográfica con respecto a la zona afectada por el incidente.

El Director o Directora de la Agencia Nacional de Ciberseguridad, previo informe técnico del CSIRT Nacional, podrá determinar las categorías de incidentes o vulnerabilidades de ciberseguridad que estarán eximidas de notificación, así como los prestadores de servicios esenciales que estarán exentos de la obligación de notificar, conforme a criterios técnicos objetivos.

Artículo 5°. Ciberataque de efecto significativo. Un ciberataque será considerado de efecto significativo si al menos una de sus consecuencias es capaz de producir un incidente de efecto significativo, de conformidad a lo dispuesto en el artículo 4° de este Reglamento.

Artículo 6°. Mantenciones regulares. Las mantenciones planificadas de sistemas informáticos de una institución regida por el presente reglamento no se considerarán incidentes. Para dichos efectos, la institución deberá incluirlas en sus planes de continuidad operacional y ciberseguridad y, además, notificar a la Agencia respecto de su programación.

Artículo 7°. Plataforma de reporte de incidentes. Los reportes de ciberataques e incidentes de ciberseguridad deberán realizarse a través de la plataforma de notificación segura dispuesta por la Agencia.

Dicha plataforma permitirá que la notificación realizada por los sujetos obligados sea comunicada simultáneamente a otras autoridades pertinentes cuando existiere la obligación de notificar a más de una autoridad sectorial.

TÍTULO III
De la taxonomía del informe

Artículo 8°. Taxonomía del Informe. Los informes enviados al CSIRT Nacional deberán contener, como mínimo, la siguiente información:

a) Datos para la debida identificación de la institución afectada: nombre, RUT, dirección y sitio web;
b) Datos de contacto del delegado de ciberseguridad o quien ostente el cargo relacionado a ciberseguridad de mayor responsabilidad en la organización de la institución afectada (nombre, correo electrónico y teléfono), en caso de existir;
c) Fecha y hora en la cual se tomó conocimiento de la ocurrencia del ciberataque o incidente de ciberseguridad.
d) Evidencia, si la hubiera, de la ocurrencia de un ciberataque o incidente de ciberseguridad;
e) Evidencia, si la hubiera, que el ciberataque o incidente de ciberseguridad responde a una acción ilícita;
f) Potenciales repercusiones del ciberataque o incidente de ciberseguridad en otras instituciones;
g) Tipo de incidente si pudiere ser identificado, por ejemplo, denegación de servicio (DoS), escaneo y reconocimiento, acceso no autorizado a la red o al dispositivo, exposición, robo o fuga de datos, código malicioso/malware, ransomware, u otro que corresponda;
h) Activos y recursos potencialmente afectados, detectados al momento de elaboración del informe. Se entenderá por activo la infraestructura física y digital de la organización, entre la que se incluye servidores, data centers, aplicaciones, repositorios de datos, entre otros;
i) Indicadores de compromiso detectados, tipo, fuente o ubicación, si los hubiere; y

j) Cualquier otro dato que la Agencia pudiese requerir para la gestión oportuna del ciberataque o incidente de ciberseguridad.

El contenido mínimo de los reportes enviados a través de la plataforma se actualizará previo informe técnico del CSIRT Nacional, para ello podrá considerar las prácticas y recomendaciones internacionales en la materia.

Artículo 9°. Datos personales. Deberá omitirse en los reportes de incidentes de ciberseguridad todo dato o información personal, conforme a lo dispuesto en el artículo 2°, letra f), de la ley N° 19.628, sobre protección de la vida privada. Para efectos de lo dispuesto en este inciso, no se considerará que la dirección IP sea un dato o información personal.

TÍTULO IV
De las Alertas, reportes e informes

Artículo 10. Alerta Temprana. Una vez que la institución obligada a reportar hubiere tomado conocimiento de la ocurrencia de un ciberataque o incidente de ciberseguridad que pueda tener impacto significativo deberá enviar una alerta temprana sobre la ocurrencia del evento, el cual se materializará mediante un reporte dentro del plazo máximo de tres horas desde que hubiere tomado conocimiento de la ocurrencia del incidente.

El reporte deberá contener, al menos, la información requerida en las letras a), b), y g) del artículo 8° de este Reglamento. Deberá tenerse en especial consideración que, el objetivo del reporte de alerta temprana es informar al CSIRT Nacional de toda evidencia o hecho observable, que a juicio de quien reporta pueda ser causa, consecuencia o efecto de un ciberataque o incidente de ciberseguridad.

En la medida que la institución tomare conocimiento de información adicional deberá actualizar el reporte de la alerta temprana, conforme el flujo dispuesto en la Plataforma.

Artículo 11. Segundo reporte. Transcurrido el plazo máximo de setenta y dos horas, la institución deberá enviar un segundo reporte al CSIRT Nacional. Dicho reporte deberá incluir una actualización de los datos informados en el reporte de alerta temprana procurando incluir la totalidad de los campos dispuestos en el artículo 8°.

Este reporte deberá contener una evaluación inicial de la gravedad e impacto del incidente y, además, indicadores de compromiso obtenidos, así como su fuente, en caso de existir.

El plazo de entrega de este informe se contabilizará desde el momento en que se tuvo conocimiento del ciberataque o incidente de ciberseguridad de efecto significativo. En el caso que la institución afectada fuera un operador de importancia vital y éste viera afectada la prestación de sus servicios esenciales a causa del incidente, la actualización de la información deberá entregarse al CSIRT Nacional en el plazo máximo de veinticuatro horas.

Artículo 12. Plan de acción de los operadores de importancia vital. Los operadores de importancia vital deberán implementar e informar un plan de acción frente al incidente en un plazo que, en ningún

caso, podrá ser superior 7 días corridos, contados desde que se tiene conocimiento de la ocurrencia del ciberataque o incidente de ciberseguridad.

El plan de acción deberá incluir, como mínimo, la siguiente información:

a) Sitio alternativo de operación, en caso de indisponibilidad del sitio principal;
b) Plan de recuperación de información a partir de respaldos;
c) Plan de recuperación de información no registrada o no respaldada desde el inicio del ciberataque o incidente de ciberseguridad;
d) Responsabilidades técnicas y administrativas sobre las tareas anteriores;
e) Individualización del responsable de comunicar los cambios que ocurran durante el ciberataque o incidente de ciberseguridad;
f) Estimación de tiempo de recuperación de los servicios si es que su continuidad fue interrumpida;
g) Estimación de tiempo de recuperación de operaciones normales, si es que esta fue afectada.

Dicha información deberá ser enviada a través de los canales que la Agencia disponga para ello.

Artículo 13. Informe final. El informe final al CSIRT Nacional deberá incluir, como mínimo, una confirmación o actualización de todos los datos informados en los reportes anteriores, además de la siguiente información.

a) Una descripción detallada del incidente, incluyendo su gravedad e impacto.
b) El tipo de amenaza o causa principal que, probablemente, haya causado el incidente.
c) Las medidas de mitigación aplicadas y en curso.
d) Si procede, las repercusiones transfronterizas del incidente.

Si la institución afectada fuera un operador de importancia vital y éste viera afectada la prestación de sus servicios esenciales a causa de un ciberataque o incidente de ciberseguridad, se deberá incluir de forma adicional:

e) La identificación de la o las vulnerabilidades abusadas y las aplicaciones abusivas (exploits) utilizadas para vulnerar los activos afectados, si es que esta información estuviera disponible. Si la información fuera desconocida al momento del informe, deberá indicarse dicha circunstancia explícitamente.
f) La identificación de los controles que deberían haber prevenido o mitigado el incidente de ciberseguridad o ciberataque junto con las causas por las cuales los controles fallaron; o una justificación para la ausencia de controles implementados.
g) Si el CSIRT respectivo o el regulador sectorial hubiese comunicado o publicado información sobre parches o actualizaciones de seguridad disponibles de forma pública o directa a la institución con anterioridad al ciberataque o al incidente de ciberseguridad, debe incluirse una justificación sobre por qué no se instalaron el o los parches correspondientes.

Si el incidente de ciberseguridad hubiere sido gestionado, el informe final deberá ser enviado dentro del plazo máximo de quince días corridos contados desde que se envió la alerta temprana contemplada en el artículo 10.

Se entenderá que un incidente se encuentra gestionado en el momento en que los antecedentes proporcionados por las instituciones afectadas permitan a la Agencia declararlo como cerrado.

Artículo 14. Informe parcial de incidente de ocurrencia prolongada. Si el ciberataque o incidente de ciberseguridad sigue en curso después de quince días desde enviada la alerta temprana, el informe final se postergará conforme el inciso siguiente y en su reemplazo se deberá remitir un informe parcial sobre la situación en dicho momento con los campos definidos en el artículo 8, incluyendo actualizaciones de toda la información entregada desde el inicio del incidente, en caso de existir.

Estos informes deberán enviarse cada 15 días desde el envío del último informe parcial, hasta que se realice el envío del informe final, el que deberá ser presentado en el plazo de quince días corridos contados desde que se haya gestionado el incidente.

En caso de no haber información nueva desde el envío del último informe o reporte, el informe deberá explicitar las razones por las cuales no existen nuevos antecedentes.

Artículo 15. Sin perjuicio de los artículos anteriores, tanto el CSIRT Nacional como la autoridad sectorial competente podrán requerir las actualizaciones pertinentes sobre el estado del incidente.

Artículo 16. En el caso de los organismos del Estado, los jefes de servicio deberán exigir a los proveedores de servicios de tecnologías de la información que compartan la información sobre vulnerabilidades e incidentes que puedan afectar a las redes y sistemas informáticos de los organismos del Estado, y siempre que tenga por objeto prevenir, detectar o responder a incidentes, recuperarse de ellos o reducir su repercusión; o reforzar el nivel de ciberseguridad, y garantizar, a su vez, que se respete la posible naturaleza delicada de la información compartida.

Con el objeto de cumplir con lo anterior, los contratos de prestación de servicios no podrán contener ninguna cláusula que pueda restringir o dificultar de cualquier modo la comunicación de información sobre amenazas por parte del prestador de servicios, siempre y cuando con ello no se comprometa la seguridad y protección de datos, incluida la confidencialidad y protección de la propiedad intelectual.

Artículo 17. La Agencia dictará las demás instrucciones que sean necesarias para la debida realización y recepción de los reportes a que se refiere el presente reglamento.

Cuando las instrucciones tengan efecto en áreas de competencia de otra entidad sectorial, deberá previamente remitir la información relevante a dicha entidad y solicitar un informe con el propósito de prevenir posibles conflictos normativos y garantizar la coordinación, cooperación y colaboración efectiva entre ambas autoridades, de conformidad a lo dispuesto en el artículo 25 de la Ley.

TÍTULO V
Disposiciones finales

Artículo 18. Los CSIRT que pertenezcan a los organismos de la Administración del Estado tendrán la obligación de tomar las providencias necesarias para apoyar el restablecimiento del servicio afectado, bajo la coordinación del CSIRT Nacional.

Artículo 19. La Agencia propiciará las notificaciones voluntarias de instituciones no obligadas conforme el artículo 9° de la Ley. Dicha notificación en ningún caso impondrá a la entidad de origen obligaciones contempladas para los sujetos obligados conforme la presente Ley.

DISPOSICIÓN TRANSITORIA

Artículo único. El presente Reglamento comenzará a regir desde la fecha de iniciación de las actividades de la Agencia, de conformidad a lo dispuesto en el artículo 1° transitorio de la ley N° 21.663.

-