Resolución 7 EXENTA

APRUEBA TAXONOMÍA DE INCIDENTES DE CIBERSEGURIDAD

MINISTERIO DEL INTERIOR Y SEGURIDAD PÚBLICA; AGENCIA NACIONAL DE CIBERSEGURIDAD

Fecha Publicación: 01-MAR-2025 | Fecha Promulgación: 28-FEB-2025
Tipo Versión: Única De : 01-MAR-2025
Url Corta: https://bcn.cl/J0KSUG

APRUEBA TAXONOMÍA DE INCIDENTES DE CIBERSEGURIDAD

Núm. 7 exenta.- Santiago, 28 de febrero de 2025.

Vistos:

Lo dispuesto en la Constitución Política de la República; en la ley N° 21.663, marco de ciberseguridad; en el decreto supremo N° 295, de 2024, del Ministerio del Interior y Seguridad Pública, que aprueba reglamento de reportes de incidentes de ciberseguridad de la ley N° 21.663; en el decreto supremo N° 479, de 2024, del Ministerio del Interior y Seguridad Pública; en el decreto supremo N° 483, de 2024, del Ministerio del Interior y Seguridad Pública, que aprueba reglamento que determina la estructura interna de la Agencia Nacional de Ciberseguridad, y la resolución N° 7, de la Contraloría General de la República.

Considerando:

1.- Que la ley N° 21.663, marco de Ciberseguridad creó la Agencia Nacional de Ciberseguridad como un servicio público descentralizado, dotado de personalidad jurídica y patrimonio propio, de carácter técnico y especializado en materias propias de ciberseguridad, con competencia para velar por la protección, promoción y respeto del derecho a la seguridad informática. ley N° 21.663

2.- Que el artículo 24° de la ley creó, dentro de la Agencia, el Equipo Nacional de Respuesta a Incidentes de Seguridad Informática (CSIRT Nacional).

3.- Que el artículo 9° de la ley establece la obligación de reportar al CSIRT Nacional los ciberataques e incidentes de ciberseguridad que puedan tener efectos significativos en los términos del artículo 27° de la ley, tan pronto les sea posible y conforme al esquema establecido en dicho artículo. artículo 9°

4.- Que, el artículo 5° del decreto supremo N° 295, de 2024, del Ministerio del Interior y Seguridad Pública, establece el contenido mínimo que deberán contener los informes de reportes de incidentes de ciberseguridad.

5.- Que, conforme el señalado artículo 9° de la ley, la Agencia dictará las instrucciones que sean necesarias para la debida realización y recepción de los reportes a que se refiere el mencionado artículo.

6.- Que, en virtud de lo anteriormente señalado, se emite la presente resolución.

Resuelvo:

Artículo primero. Las instituciones públicas y privadas que presten servicios calificados como esenciales y aquellas que hubieren sido calificadas como operadores de importancia vital de conformidad a la ley N° 21.663, deberán reportar al CSIRT Nacional los ciberataques e incidentes de ciberseguridad que puedan tener efectos significativos, tan pronto les sea posible.

140 años Biblioteca del Congreso Nacional de Chile / BCN | Ley Chile

Dicho reporte deberá realizarse a través de la plataforma dispuesta por la Agencia Nacional de Ciberseguridad o a través de otros medios que la Agencia establezca para tal finalidad.

La plataforma de reporte estará disponible en la URL https://portal.anci.gob.cl, las veinticuatro horas, todos los días del año.

Artículo segundo. De conformidad con lo dispuesto en el artículo 5° letra f) del decreto supremo N° 295, del Ministerio del Interior y Seguridad Pública, los informes enviados al CSIRT Nacional deberán incluir una descripción del incidente, si pudiere ser identificado.

Para efectos de clasificar el incidente de ciberseguridad se deberán considerar los efectos observables del hecho acaecido, es decir, todo contexto, escenario o circunstancia que puede ser observada directamente, independientemente de cuál pueda ser su causa u origen.

Artículo tercero. Establézcase la siguiente taxonomía de incidentes de ciberseguridad, que consiste en cuatro áreas de impacto, y en once efectos observables, tal como se indica a continuación:

a. Impacto en el uso legítimo de recursos:

i. Uso no autorizado de redes y sistemas informáticos: Uso no autorizado de sistemas de la institución afectada, ya sea a través de explotación de vulnerabilidades, uso no autorizado de credenciales, acceso a almacenamiento en nube, u otros.

ii. Actividades de phishing o fraude en infraestructura propia: Envío de phishing a través de servidores de la institución afectada, o almacenamiento de sitios fraudulentos en redes y sistemas informáticos de la institución afectada.

iii. Actividades de phishing o fraude relacionadas con la institución: Envío de phishing relacionado con la institución afectada por parte de terceros, o almacenamiento de sitios fraudulentos por parte de terceros.

iv. Ejecución no autorizada de código: Inclusión y ejecución no autorizada de código en sistemas de la institución afectada.

b. Impacto en la confidencialidad de la información:

i. Exfiltración y/o exposición de datos: Pérdida de información confidencial con o sin divulgación pública, y/o información confidencial expuesta accidental o intencionalmente.

ii. Exfiltración y/o exposición de configuraciones: Pérdida o exposición accidental de configuraciones y parámetros confidenciales de un sistema o aplicación de la institución afectada.

iii. Exfiltración y/o exposición de código fuente: Pérdida o exposición excesiva del código fuente de un sistema de la institución afectada.

c. Impacto en la disponibilidad de un servicio esencial:

i. Indisponibilidad y/o denegación de servicio: Pérdida total del funcionamiento de un servicio, sistema o servidor, o saturación de red impidiendo su operación normal.

ii. Degradación de servicio: Pérdida parcial del rendimiento o funcionalidad de un servicio, sistema o servidor.

d. Impacto en la integridad de la información:

i. Modificación no autorizada de datos: Alteración no autorizada de información contenida en sistemas, servicios o servidores.

Biblioteca del Congreso Nacional de Chile / BCN | Ley Chile

ii. Manipulación no autorizada de configuración: Cambio no autorizado de configuraciones en sistemas, servicios o servidores.

Artículo cuarto. Establézcanse las siguientes categorías de incidentes, según el efecto observable:

i. Uso no autorizado de redes y sistemas informáticos:

a. Acceso no autorizado a almacenamiento.
b. Ataque de fuerza bruta exitoso.
c. Explotación de vulnerabilidades de autenticación.
d. Uso de credenciales comprometidas.

ii. Actividades de phishing o fraude en infraestructura propia:

a. Envío de correo no deseado o phishing desde infraestructura propia.
b. Inclusión de sitio fraudulento en infraestructura propia.

iii. Actividades de phishing o fraude relacionadas con la institución:

a. Envío de correo no deseado o phishing sobre una organización.
b. Envío de correo no deseado o phishing usando remitentes de la institución.

iv. Ejecución no autorizada de código:

a. Ejecución remota de código a través de parámetros de aplicación.
b. Inyección de requerimientos (prompts) en modelos grandes de lenguaje (LLM).
c. Inyección de consultas NoSQL.
d. Inyección de consultas SQL.

v. Exfiltración y/o exposición de datos:

a. Adversario en el medio (MitM).
b. Apropiación de credenciales mediante phishing.
c. Base de datos sin protección (S3 buckets, Elasticsearch, MongoDB expuestos).
d. Documentos públicos con datos sensibles.
e. Filtración de datos personales.
f. Keylogger en uso.
g. Divulgación de enumeraciones de usuarios y/o credenciales de usuarios en foros.

vi. Exfiltración y/o exposición de configuraciones:

a. Filtración de configuraciones en rutas de aplicación.
b. Filtración de secretos en rutas de aplicación.

vii. Exfiltración y/o exposición de código fuente:

a. Archivo(s) de control de versión expuestos en aplicación.
b. Sistema de control de versión expuesto.

viii. Indisponibilidad y/o denegación de servicio:

a. Agotamiento de conexiones TCP.
b. Apagado no autorizado de sistemas informáticos.
c. Ataque de amplificación DNS/NTP.
d. Ataque físico contra infraestructura TI.
e. Denegación de servicio a través de la explotación de vulnerabilidades.

Biblioteca del Congreso Nacional de Chile / BCN | Ley Chile

f. Eliminación de configuraciones críticas.
g. Tráfico de red excesivo (volumétrico).

ix. Degradación de servicio:

a. Secuestro de recursos (cryptojacking).
b. Sobrecarga de bases de datos.
c. Uso excesivo de ancho de banda.

x. Modificación no autorizada de datos:

a. Alteración de bases de datos.
b. Alteración de sitio web (defacement).
c. Manipulación de datos no autentificados.
d. Modificación de logs de auditoría.

xi. Manipulación no autorizada de configuración:

a. Alteración de reglas de firewall.
b. Desactivación de registros de seguridad.
c. Modificación de políticas de acceso.

Anótese y publíquese.- Daniel Álvarez Valenzuela, Director Nacional, Agencia Nacional de Ciberseguridad.