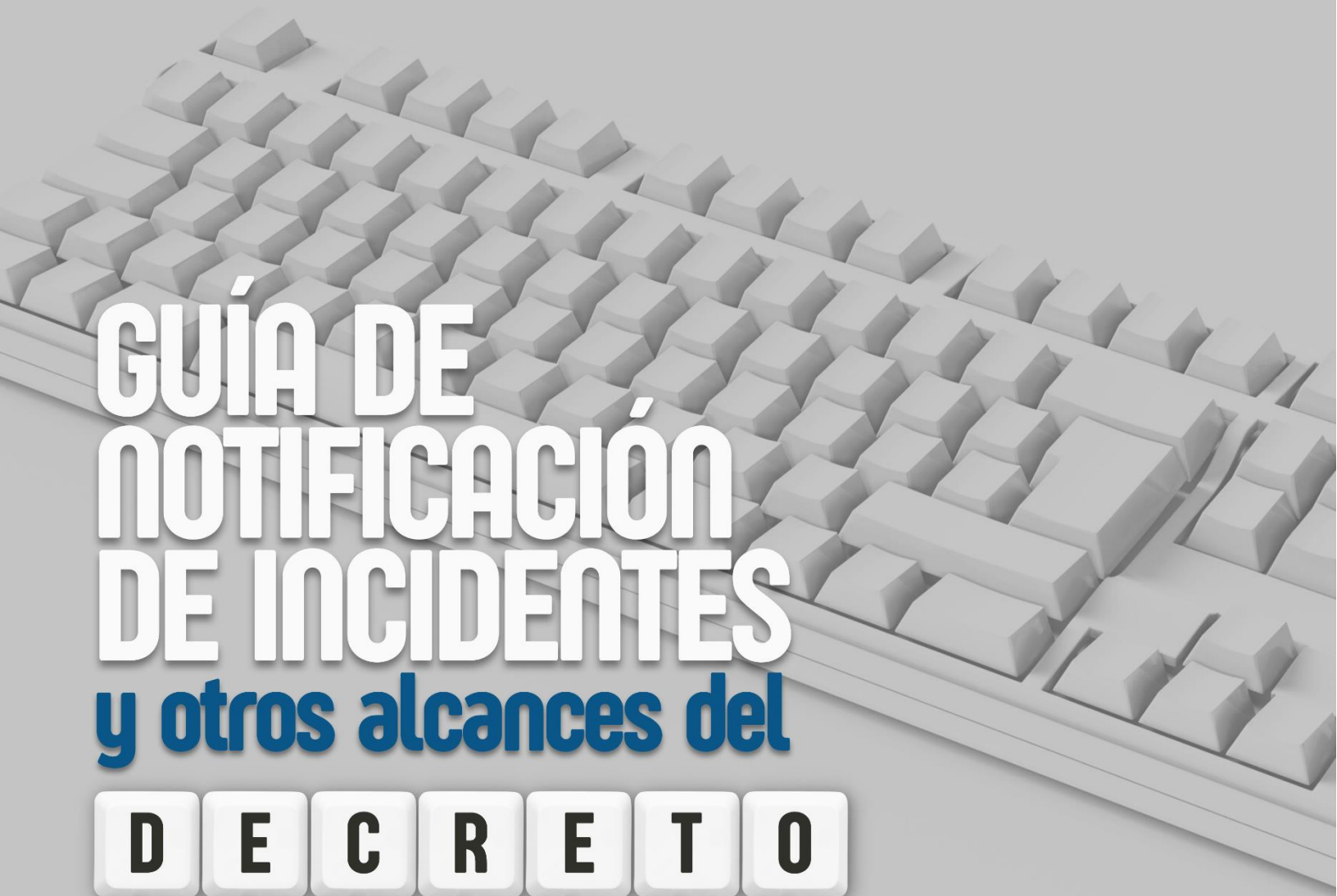
CSIRT

Equipo de Respuesta ante Incidentes de Seguridad Informática

SERIE DE BUENAS PRÁCTICAS

Volumen 1 | Enero de 2023



GUÍA DE NOTIFICACIÓN DE INCIDENTES y otros alcances del DECRETO 273

www.csirt.gob.cl

ÍNDICE

Dirección Ingrid Inda Camino | **Edición general** Carlos Silva Caffi | **Revisión y edición de contenidos** Hernán Espinoza Medina | **Contenido** Patricio Quezada Andaur | **Colaboración** Cristian Bravo Lillo, Francisca Cristi Worm, Sabina Torres Figueroa y Gonzalo Concha Concha | **Diseño** Patricio Quezada Andaur | **Corrección de estilo** Carolina Covarrubias Escobar y Ramón Rivera Notario | **Equipo de Respuesta ante Incidentes de Seguridad Informática de Chile, CSIRT**.

CSIRT
Equipo de Respuesta ante Incidentes de Seguridad Informática

1. Acerca de esta guía

El Equipo de Respuesta ante Incidentes de Seguridad Informática, CSIRT, del Gobierno de Chile, ha elaborado esta guía para suministrar a los organismos públicos del Estado una visión normalizada de conocimientos sobre los conceptos aludidos en el Decreto 273 de 2022, del Ministerio del Interior, con especial énfasis en el procedimiento de notificación de incidentes de ciberseguridad.

Esta guía aclara, entre otras incertidumbres, qué se entiende por incidente de ciberseguridad, quien debe notificar el incidente, cuándo, dónde y cómo notificar.

1.1. ¿A quién va dirigida esta guía?

Esta guía está dirigida a los funcionarios de los organismos de la Administración centralizada y descentralizada del Estado, especialmente a quienes tienen la responsabilidad administrativa de dar cumplimiento al Decreto 273 del 13 de septiembre de 2022, y quienes en el cumplimiento de sus roles de Encargados de Ciberseguridad y Especialistas de Seguridad TI deben liderar las gestiones de ciberseguridad en sus organizaciones.

1.2. El Decreto 273

El pasado 13 de septiembre de 2022, se estableció por decreto la obligación de reportar incidentes de ciberseguridad al Equipo de Respuesta ante Incidentes de Seguridad Informática del Ministerio del Interior y Seguridad Pública, CSIRT.

El decreto, que fue publicado en el diario oficial el pasado viernes 2 de diciembre de 2022, se compone de cuatro artículos. Los artículos 1° y 2° abordan la notificación de incidentes de ciberseguridad y el plazo en que debe ser realizada la notificación; el artículo 3° trata sobre la gestión que se debe realizar para obtener información oportuna de parte de los proveedores de servicios de tecnologías de información sobre las amenazas y que ésta fluya hacia los órganos de la administración del Estado; por último, el artículo 4° se refiere a la importancia de la búsqueda preventiva de vulnerabilidades en estos organismos del Estado.

1.3. Sobre el CSIRT

El Decreto n.° 273 establece que los jefes de servicio deben notificar sobre los incidentes de ciberseguridad que los afecten al Equipo de Respuesta ante Incidentes de Seguridad Informática del Ministerio del Interior y Seguridad Pública, CSIRT, el que fue formalmente creado por la Resolución Exenta n° 5.006, el 20 de agosto de 2019, como un departamento dependiente de la División de Redes y Seguridad Informática de dicho ministerio.

En la misión del CSIRT se establece la creación de una capacidad de respuesta -preventiva, reactiva y proactiva- para enfrentar los incidentes de ciberseguridad que afecten la integridad, disponibilidad o confidencialidad de, entre otros, los órganos de la Administración del Estado.

2. Conceptos de ciberseguridad en el Decreto 273

El Decreto 273 menciona varios conceptos de ciberseguridad. Esta guía define esos conceptos para ayudar a su comprensión. Los conceptos mencionados y definidos en esta guía son:

- Afectación de un incidente
- Amenaza de ciberseguridad
- Buenas prácticas de seguridad de la información
- Incidente de ciberseguridad
- Medidas de mitigación
- Políticas de seguridad de la información
- Vulnerabilidad informática

Las definiciones de ciberseguridad que se utilizan en esta guía han sido en su mayoría obtenidas de la ISO[1] y del NIST[2], y han sido adaptadas para su uso en ciberseguridad por el CSIRT de Gobierno.

2.1. Afectación de un incidente

Se entiende por afectación de un incidente al nivel de impacto real o potencial causado por un incidente de ciberseguridad. Todos los incidentes de ciberseguridad tienen algún grado de afectación. La afectación puede ir desde un nivel de afectación bajo, como mínimo, hasta un nivel de afectación crítico, como máximo.

Corresponde a cada organización establecer la afectación de un incidente. Con ese propósito, en la sección de anexos se adjuntan una “tabla de afectación de incidentes de ciberseguridad” y una tabla de “Taxonomía de Incidentes”.

2.2. Amenaza de ciberseguridad

En esta guía se entenderá por amenaza de ciberseguridad a cualquier circunstancia o evento con el potencial de afectar negativamente las operaciones de una organización (incluida la misión, las funciones, la imagen o la reputación), sus activos o las personas.

2.3. Buenas prácticas de seguridad de la información

Las buenas prácticas de la seguridad de la información son formas, modos o métodos de hacer ciertas operaciones que en la industria o comunidad son consideradas como acertadas o buenas, para enfrentar riesgos vinculados a seguridad de la información. Por ejemplo, la ISO27002:2022 recopila un conjunto de 93 buenas prácticas o controles para el tratamiento del riesgo relacionado con seguridad de la información.

[1] Organización Internacional de Normalización
[2] Instituto Nacional de Tecnología y Estándares del Departamento de Comercio de los Estados Unidos

2.4. Incidente de ciberseguridad

Para efectos de esta guía y de lo señalado por el Decreto 273, se entenderá como incidente de ciberseguridad a los *eventos de seguridad de la información*[3] únicos o a una serie de eventos de seguridad de la información no deseados o inesperados que tengan una probabilidad significativa de comprometer las operaciones de las organizaciones del Estado y amenazar la seguridad de la información.

2.5. Medidas de mitigación

Una medida de mitigación es toda decisión, acción o práctica destinada a reducir el nivel de riesgo asociado con uno o más eventos de amenazas, escenarios de amenazas o vulnerabilidades.

2.6. Políticas de seguridad de la información

Las políticas de seguridad de la información son orientaciones o directrices que rigen la actuación de los usuarios de un sistema con el propósito de brindar seguridad de la información para la institución y sus funcionarios.

La política de seguridad contempla, al menos:

- La definición de la seguridad de la información, los objetivos y principios para guiar a todas las actividades relacionadas con la seguridad de la información;
- La asignación de responsabilidades generales y específicas para la administración de la seguridad de la información de acuerdo a los roles definidos;
- Los procesos para manejar desviaciones y excepciones.

A un nivel inferior, la política de seguridad de la información se debería respaldar por políticas específicas de un tema, que estipulen la implementación de controles de seguridad de la información y que típicamente se estructure para abordar las necesidades de ciertos grupos objetivo dentro de una organización para abarcar ciertos temas.

2.7. Vulnerabilidad informática

Se entenderá por vulnerabilidad informática a toda debilidad de un activo, de un control o de una implementación que pueda ser explotada por una o más amenazas. La búsqueda preventiva de vulnerabilidades contribuye a la disminución de riesgos informáticos.

[3] Un evento de seguridad de la información es una ocurrencia identificada de un sistema, servicio o estado de la red que indica una posible violación de la política de seguridad de la información o falla de los controles, o una situación previamente desconocida que puede ser relevante para la seguridad.

3. La notificación de incidentes de seguridad informática

El principal objetivo del Decreto 273 es la obligación de reportar o notificar incidentes de ciberseguridad. En consecuencia, comprender y ejecutar correctamente el procedimiento de notificación es fundamental para cumplir ese objetivo.

3.1. Artículos 1° y 2° del Decreto 273, sobre la notificación de incidentes

El Artículo 1° del Decreto 273, que trata sobre la notificación de incidentes de ciberseguridad, indica lo siguiente:

"Los jefes de servicio de los Ministerios y demás organismos de la Administración centralizada y descentralizada del Estado deberán comunicar los incidentes de ciberseguridad que les afecten, al Ministerio del Interior y Seguridad Pública, mediante su notificación al Centro de Respuesta ante Incidentes de Seguridad Informática ("CSIRT"), en el sitio web: https://csirt.gob.cl".

Por su parte, el Artículo 2° es un complemento del anterior que señala el plazo para la notificación del ciberinciente:

"La comunicación anterior deberá realizarse tan pronto se constate su ocurrencia, no pudiendo ser este plazo superior a 3 horas desde que se tome conocimiento".

3.2. El rol del Jefe de servicio

El Decreto 273 señala específicamente que serán los Jefes de servicios los responsables de comunicar los incidentes de ciberseguridad al CSIRT.

Cuando los Jefes de servicio no puedan ser informados sobre los incidentes, corresponderá a quienes lo subrogan o hayan recibido la delegación respectiva, cumplir con ese deber.

Los jefes de servicio deberán, mediante una directiva interna, circular u orden de servicio, determinar quiénes son los subrogantes para el cumplimiento específico de esta norma e informar de esta subrogancia a todos los funcionarios de sus reparticiones y a los proveedores de servicios involucrados en la gestión de los sistemas y activos informáticos de la organización, si corresponde.

Para todos los efectos, la responsabilidad delegada deberá ser cumplida por el subrogante, cualquiera sea la circunstancia.

De igual manera, la directiva, circular u orden de servicio deberá informar a los funcionarios o proveedores de servicio, que estos deberán comunicar el incidente al Jefe de servicio o subrogante tan pronto como tengan conocimiento del incidente de ciberseguridad.

Los jefes de servicio también deberán asegurarse de informar a los proveedores de servicios externos que administren los sistemas y activos informáticos de sus organizaciones, que todos los incidentes

de ciberseguridad que tengan afectación en su organización deberán ser comunicados oportunamente a su persona, a quienes le subrogan y a los contactos establecidos como contrapartes técnicas y administrativas derivadas de los contratos celebrados con el proveedor.

En esta circunstancia, y mientras los contratos no sean modificados para fijar el correcto escalamiento y cumplimiento de los SLA (Acuerdos de Nivel de Servicio) en el espíritu del Artículo 3° del Decreto 273, se entenderá que el plazo para realizar la notificación del incidente comienza desde el momento en que un funcionario con responsabilidad administrativa tome constancia de un incidente.

Siguiendo el punto anterior, y dado que existe un plazo máximo de 3 horas para comunicar el incidente al CSIRT desde el momento de su constatación, si el jefe de servicio o los funcionarios que lo subrogan no pudieran ser hallados, el deber de comunicar el incidente corresponderá siempre al funcionario de mayor rango de la organización que esté en conocimiento de lo acaecido.

Se entenderá que el incumplimiento de la obligación de informar al CSIRT sobre los incidentes en el plazo estipulado por el Decreto 273 podría dar inicio a una investigación sumaria para definir sanciones de acuerdo a lo estipulado en la Ley 18.575, sobre las bases generales de la administración del Estado y en la Ley 18.834 sobre estatuto administrativo.

3.3. El procedimiento de notificación

El Artículo 1° del Decreto 273, indica que los jefes de servicio deberán comunicar los incidentes de ciberseguridad que les afecten al CSIRT, específicamente en el sitio web https://csirt.gob.cl.

En el sitio web del CSIRT, los jefes de servicio o responsables de realizar la notificación podrán utilizar para esos efectos el formulario de notificación que se desplegará ocupando el enlace o botón de “notificar un incidente”, el que está disponible en la página de inicio del sitio.

Una vez que despliega el formulario, el Jefe de servicio o quien lo subrogue, deberá completar una serie de campos de identificación personal y de la organización afectada. Entre los datos solicitados se encuentran el nombre, un número de teléfono de contacto, el correo electrónico, la entidad a la que representa, el asunto, el nombre de la entidad afectada, el o los activos afectados y un especio para dar una breve descripción del incidente.

Una vez que se completa esta información, el Jefe de servicio deberá enviar el formulario y constatar que ha recibido un correo automático que confirma la notificación del incidente.

En forma alternativa, o por razones de fuerza mayor, el jefe de servicio o quien lo subrogue podrán realizar la notificación vía telefónica, marcando el número 1510 en su teléfono. En ese caso, quien comunica el incidente deberá informar a la persona que conteste a la llamada en la mesa de ayuda telefónica que está realizando el reporte de un incidente en conformidad al Decreto 273. Con esta información presente, los funcionarios de la mesa de ayuda serán los encargados de completar los datos del formulario con la información que se proporcione telefónicamente. Es importante dejar

claro que este reporte se produce en los primeros momentos en que ha ocurrido un incidente y es probable que no existan tantos detalles a comunicar. En posteriores y sucesivos reportes pueden ir apareciendo y agregándose detalles técnicos en la medida que los equipos técnicos actúen.

De todas formas, una vez terminado el proceso, quien informa deberá asegurarse de haber recibido el correspondiente correo de verificación del procedimiento realizado. Ese correo de verificación constituye la prueba de que el incidente de seguridad informática fue notificado dentro del plazo estipulado en el Decreto.

3.4. Deber de denunciar delitos informáticos

Adicionalmente, cuando se trate de incidentes que han sido tipificados como delitos informáticos en la Ley 21.459, los Jefes de servicio deberán asegurarse de realizar la denuncia correspondiente en forma oportuna a la policía o a la fiscalía.

Bajo ninguna circunstancia el Jefe de servicio debe interpretar que la notificación realizada al CSIRT implica que se ha cumplido con el procedimiento de denuncia del delito informático acaecido en su organismo.

3.5. Deber de comunicar amenazas de ciberseguridad

Los Especialistas de Seguridad TI y los Encargados de Ciberseguridad, de acuerdo con lo señalado por el Instructivo Presidencial N°8 de 2018, deberán seguir cumpliendo con su rol de informar al CSIRT a través de los canales habituales de comunicación, sobre las amenazas de ciberseguridad que, por su naturaleza, no corresponden a incidentes de ciberseguridad.

4. Gestión para exigir información de amenazas y vulnerabilidades a proveedores

Muchas de las organizaciones de la administración pública del Estado cuentan con proveedores privados que prestan servicios de tecnologías de la información en sus procesos de trabajo cotidiano.

El rol de estos proveedores es crítico para garantizar la confidencialidad, integridad y disponibilidad de los activos y servicios informáticos de las organizaciones.

Sin embargo, estos proveedores no tienen otras responsabilidades legales salvo las específicamente señaladas en los contratos que han sido celebrados entre éstos y los organismos del Estado.

El Artículo 3° del Decreto 273 tiene como objetivo cambiar esa relación y para ello determina que *"los jefes de servicio establecidos en el artículo 1, dentro del ámbito de sus facultades, y respecto de los contratos que se celebren con posterioridad a la entrada en vigencia del presente decreto, deberán exigir a los proveedores de servicios de tecnologías de la información, que compartan la información sobre las amenazas y vulnerabilidades que puedan afectar a las redes, plataformas y sistemas informáticos de los órganos de la administración del Estado, al igual que las medidas de mitigación aplicadas a éstas, así como las políticas y prácticas de seguridad de la información incorporadas en los servicios prestados"*.

Pese a lo anterior, los jefes de servicio deben agotar desde ya todas las posibilidades de obtener la mayor cooperación por parte de los proveedores de servicios acerca de la información de amenazas y vulnerabilidades que puedan afectar a los activos de su organización, así como las medidas de mitigación, políticas y buenas prácticas de seguridad de la información que incorporan estos servicios.

Además, es importante que, al celebrar los contratos con los proveedores, los jefes de servicio indiquen el escalamiento de información correspondiente en el evento que se produzca un incidente, asegurándose que en ese procedimiento ellos, las personas que lo subrogan o los interlocutores fijados en los respectivos protocolos, sean oportunamente informados de lo acaecido.

5. Búsqueda preventiva de vulnerabilidades

El Artículo 4° del Decreto 273 establece que "*para mejorar la seguridad de las redes y sistemas informáticos de su respectiva institución, los jefes de servicio indicados en el artículo 1º, pueden solicitar a los equipos técnicos del CSIRT su revisión y análisis, incluyendo la búsqueda preventiva de vulnerabilidades informáticas, otorgando las facilidades que sean necesarias para ello*".

En el caso de las vulnerabilidades, la búsqueda preventiva de éstas es crítica para evitar que ocurran incidentes de ciberseguridad, en la medida que son detectadas y corregidas oportunamente.

Para disminuir el riesgo de incidentes en los sistemas y activos informáticos de las organizaciones, los Jefes de servicio están llamados a impulsar la adopción de medidas preventivas, políticas y buenas prácticas de ciberseguridad en sus organizaciones.

Una de estas medidas preventivas, en la que pone énfasis el Artículo 4° del Decreto 273, es la evaluación (detección, revisión y análisis) de vulnerabilidades, la que se realizada en la forma de un servicio de escaneo.

Con la entrada en vigencia del Decreto 273, esta evaluación se realizará como un beneficio sin costo para todas las organizaciones del Estado que la soliciten.

Para solicitar a los equipos técnicos del CSIRT la búsqueda preventiva de vulnerabilidades informáticas, su revisión y análisis, las organizaciones deberán enviar un correo electrónico a la casilla soc@interior.gob.cl con copia a scan-csirt@interior.gob.cl.

Adicionalmente, las entidades que se encuentran dentro de la Red de Conectividad del Estado (RCE) pueden consultar por otros servicios de ciberseguridad que entrega el CSIRT. Estos servicios son un beneficio sin costo para estas organizaciones. Las organizaciones del Estado fuera de la RCE pueden obtener otros beneficios suscribiendo un convenio de colaboración con el CSIRT. Las organizaciones de Gobierno, por su parte, pueden iniciar gestiones para ingresar a la RCE y obtener los mismos beneficios. Para mayor información, las entidades interesadas pueden comunicarse al CSIRT, a través del correo soc@interior.gob.cl o al teléfono 1510.

ANEXOS

I. Normas legales de ciberseguridad mencionadas en el Decreto 273.

Junto con las disposiciones constitucionales y legales que establecen el ordenamiento jurídico de los organismos de la Administración Pública del Estado, el Decreto 273 también invoca normas legales asociadas a la ciberseguridad que se deben seguir al momento de su ejecución.

Esta guía enumera esas normas, las que se acompañan de un enlace para que puedan ser consultadas por los interesados, siendo muy recomendable su lectura.

Dada la relevancia de los delitos tipificados en la Ley 21.459 (sobre delitos informáticos) para establecer la afectación de un incidente, la que se explicita en el considerando N°5, que subraya la obligación de los funcionarios públicos de denunciar, con la debida prontitud, los crímenes o simples delitos y, a la autoridad competente, los hechos de carácter irregular de que tengan conocimiento en el ejercicio de sus funciones; y en el considerando N°6, que señala que la Ley 21.459 tipifica como delitos a los ciberataques que afecten a la integridad de los sistemas y/o datos informáticos, así como el acceso ilícito, esta guía excepcionalmente agrega una síntesis de la mencionada ley de delitos informáticos.

Las siguientes son las normativas asociadas a ciberseguridad mencionadas en el Decreto 273:

- Ley 21.459, que establece normas sobre delitos informáticos, deroga la ley Nª 19.223 y modifica otros cuerpos legales con el objeto de adecuarlos al convenio de Budapest. Esta Ley actualiza la legislación chilena en materia de delitos informáticos, adecuándola a las exigencias del Convenio de Budapest, del cual Chile es parte.

  La ley tipifica como delitos informáticos las siguientes conductas:
  - Ataque a la integridad de un sistema informático
  - Acceso ilícito
  - Interceptación ilícita
  - Ataque a la integridad de los datos informáticos
  - Falsificación informática
  - Receptación de datos informáticos
  - Fraude informático
  - Abuso de dispositivos

  Para estos delitos se contemplan penas, según su gravedad, que van desde presidio menor en su grado mínimo a presidio mayor en su grado mínimo, así como aplicación de multas.

  Adicionalmente, se incorporan circunstancias modificatorias de responsabilidad penal, en particular, como atenuante, la cooperación eficaz, y como agravantes, a modo ejemplar, cometer el delito abusando de una posición de confianza en la administración del sistema informático o custodio de los datos informáticos contenidos en él, en razón del ejercicio de un cargo o función, o de la vulnerabilidad, confianza o desconocimiento de niños, niñas, adolescentes o adultos mayores.

Asimismo, se agregan reglas especiales en materia de procedimiento, concediéndose legitimación activa al Ministerio del Interior y Seguridad Pública, delegados presidenciales regionales y delegados presidenciales provinciales cuando las conductas señaladas en la ley afecten servicios de utilidad pública. Se permite ordenar técnicas de investigación de aquellas reguladas en los artículos 222 a 226 del Código Procesal Penal, cumpliendo los requisitos previstos en la ley, y se hace referencia expresa al comiso y evidencia digital.

Finalmente, se deja sin efecto la Ley N° 19.223, que tipifica figuras penales relativas a la informática, y modifica otros textos legales para adecuarlos a esta nueva normativa.

Enlace: https://bcn.cl/32uaf

- Ley 19.628, sobre protección de la vida privada.
  Enlace: https://bcn.cl/33x5h

- Decreto Nº 5.996, de 1999, del entonces Ministerio del Interior, que crea la red interna (Intranet) del Estado, modificado por el decreto supremo Nº1.299, de 2004, que establece nuevas normas que regulan la Red de Conectividad del Estado que administra el Ministerio del Interior y fija los procedimientos, requisitos y estándares tecnológicos para la incorporación a dicha red de instituciones públicas.
  Enlace: https://bcn.cl/2r2u6

- Decreto Nº 83, de 2004, del Ministerio Secretaría General de la Presidencia, que aprueba norma técnica para los órganos de la administración del Estado, sobre seguridad y confidencialidad de los documentos electrónicos.
  Síntesis:
  Enlace: https://bcn.cl/2r2tw

- Decreto supremo Nº 533, de 2015, del Ministerio del Interior y Seguridad Pública, que crea el Comité Interministerial sobre Ciberseguridad.
  Enlace: https://bcn.cl/2kbyz

- Política Nacional de Ciberseguridad, de abril de 2017.
  Enlace: https://biblioteca.digital.gob.cl/handle/123456789/738

- Instructivo Presidencial Nº 8, del 23 de octubre de 2018, que imparte instrucciones urgentes en materia de ciberseguridad, para la protección de redes, plataformas y sistemas informáticos de los órganos de la administración del Estado.
  En: https://digital.gob.cl/biblioteca/regulacion/instructivo-presidencial-no8-ciberseguridad/

- Decreto supremo Nº 579, de 2019, del Ministerio del interior y Seguridad Pública, que modifica el decreto supremo Nº 533, de 2015, del Ministerio del Interior y Seguridad Pública, que crea Comité Interministerial sobre Ciberseguridad.
  Enlace: https://bcn.cl/2k880

II. Tablas de afectación y taxonomía de incidentes.

TABLA DE AFECTACIÓN DE INCIDENTES DE CIBERSEGURIDAD	
NIVEL DE AFECTACIÓN	EJEMPLO DE CONDICIONES
Crítico	Afecta a la seguridad ciudadana con potencial peligro para la vida de las personas.
	Afecta a sistemas clasificados como confidenciales (ley 20.285) o que contengan información calificada como datos sensibles de acuerdo con la (ley 19.628)
	Afecta a más del 50% de los procesos que soportan los sistemas de la institución.
	Interrupción en la prestación del servicio igual o superior a 12 horas
	Interrupción en la prestación del servicio superior al 40% de los usuarios.
	Afecta a más del 50% de sus instalaciones a nivel nacional.
	Daños reputacionales muy elevados y cobertura continua en medios de comunicación nacionales e internacionales.
Muy Alto	Afecta a la seguridad ciudadana con potencial peligro para bienes materiales.
	Afecta la vida privada y/o la honra de la persona y su familia, y asimismo, la protección de sus datos personales.
	Afecta a más del 40% de los procesos que soportan los sistemas de la institución.
	Interrupción en la prestación del servicio igual o superior a 8 horas.
	Interrupción en la prestación del servicio superior al 30% de los usuarios.
	Afecta a más del 40% de sus instalaciones a nivel nacional.
	Daños reputacionales elevados y cobertura continua en medios de comunicación nacionales.
Alto	Afecta a más del 30% de los procesos que soportan los sistemas de la institución.
	Interrupción en la prestación del servicio igual o superior a 6 horas.
	Interrupción en la prestación del servicio superior al 20% de los usuarios.
	Afecta a más del 30% de sus instalaciones a nivel nacional.
	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 procesos que soportan los sistemas de la institución.
	Interrupción en la prestación del servicio igual o superior a 4 horas.
	Interrupción en la prestación del servicio superior al 10% de los usuarios.
	Afecta a más del 20% de sus instalaciones a nivel nacional.
	Daños reputacionales apreciables, con eco mediático (amplia cobertura en los medios de comunicación).
Bajo	Afecta al 20% o menos, de los sistemas de la institución.
	Interrupción en la prestación del servicio igual o superior a 2 horas.
	Interrupción en la prestación del servicio igual superior al 5% de los usuarios.
	Afecta al 20% o menos, de sus instalaciones a nivel nacional.
	Daños reputacionales puntuales, sin eco mediático

MATRIZ DE CLASIFICACIÓN DE INCIDENTES[4]			
CLASE	DESCRIPCION	TIPO	DESCRIPCIÓN
Contenido Abusivo	Son incidentes que comprometen la imagen de una entidad o persona, mediante el uso de sistemas para realizar acciones que contienen aspectos prohibidos, ilícitos u ofensivos.	Pornografía Infantil	Es la transmisión o almacenamiento de material pornográfico infantil.
		Violencia	Promover contenido de odio para perseguir o incitar a la persecución de personas u organizaciones.
		Acoso Sexual o Extorsión	Conducta persistente o reiterada dirigida hacia una persona y que causa angustia emocional. Presión o coerción ejercida contra persona o instituciones para que ejecuten una conducta contraria a su voluntad.
		Spam	Es la distribución de correo masivo no solicitado.
		Difamación	Es el acto de divulgar una acusación hacia otra persona que puede causar un daño en el honor, dignidad o reputación.
Código Malicioso	Es un programa o código dañino, cuya función es afectar la confidencialidad, integridad o disponibilidad de la información.	Sistema Infectado	Dispositivo computacional infectado con algún Malware (Troyanos, Dealer, Rootkit, Ransomware, Exploits, Gusanos, Spyware, Adware, Servidor de Mando y Contro (C&C), entre otros, que podría afectar su correcto funcionamiento)
		Distribución de Software Malicioso	Uso indebido de los activos de la organización para distribuir malware.
		Minería ilegal Criptomonedas	Abuso de recursos de la organización para minar criptomonedas.
Recopilación de Información	Consiste en recabar información de las plataformas tecnológicas para crear un perfil de la infraestructura de la organización.	Escaneo de Redes (Scanning)	Envío de solicitudes a un sistema con el objetivo de identificar activos y descubrir posibles vulnerabilidades, por ejemplo, escaneos a puertos, DNS, ICMP, SMTP, entre otros.
		Análisis de paquetes (Sniffing)	Corresponde al almacenamiento de flujo de datos y análisis, relacionados a la interceptación del tráfico de red.
		Ingeniería Social	Recopilación de información personal, mediante engaños, sobornos o amenazas.
		Inteligencia de fuentes abiertas (OSINT)	Datos recogidos de forma pública, por ejemplo redes sociales, sitios web entre otros.
Intentos de Intrusión	Ataque dirigido con el objeto de explotar vulnerabilidades de sistemas y/o configuraciones con el fin de introducirse a los sistemas.	Intentos de acceso	Múltiples intentos de inicio de sesión, por ejemplo, ataque de fuerza bruta.
		Explotación de vulnerabilidades	Intentos de comprometer un sistema o interrumpir cualquier servicio explotando vulnerabilidades conocidas (CVE). Por ejemplo, XSS, SQL Injection, CSRF, SSL, entre otros.
		Ataques desconocidos	Ataques que utilizan vulnerabilidades desconocidas, mediante técnicas o programas.
Intrusión	Es una actividad no autorizada, donde el	Compromiso de cuentas	Sistema comprometido donde el atacante utiliza cuentas con o sin privilegios.

[4] Esta tabla solo contempla incidentes de ciberseguridad que tienen afectación, lo que explica porque no se incluye la categoría de vulnerabilidades.

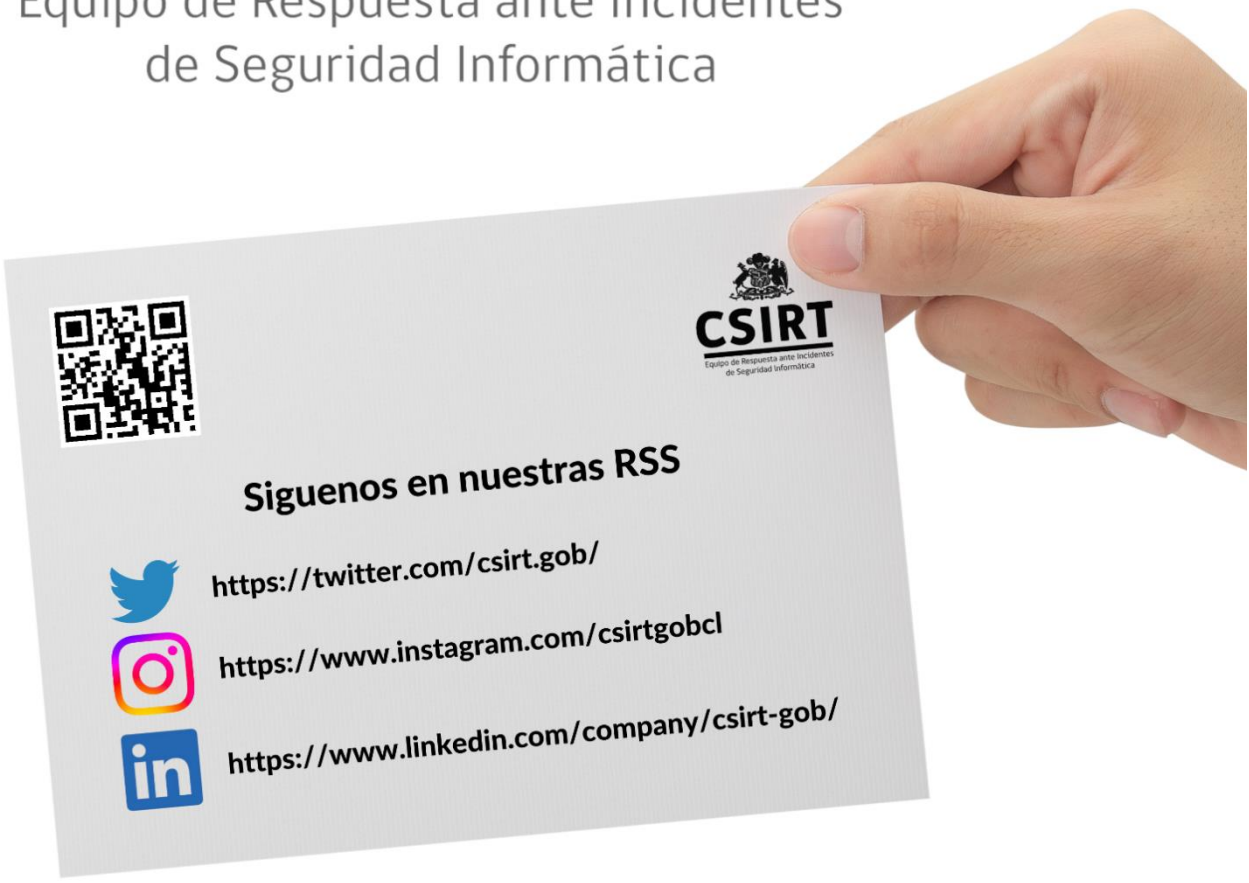
	atacante accede ilícitamente a la infraestructura informática de una organización.	Compromiso de aplicativo	Explotación de una vulnerabilidad para comprometer un software o aplicativo.
		Intrusión física	Acceso ilícito a un lugar restringido con fines maliciosos.
Amenaza a la Disponibilidad	Corresponde a la degradación de los accesos a los sistemas informáticos. La disponibilidad es una de las tres dimensiones de la seguridad de la información.	Ataque de denegación de servicio (DoS / DDoS)	Corresponde a múltiples envíos de paquetes (solicitudes) a un servicio en red determinado en un corto período de tiempo con el objetivo de abrumar un sitio y provocar su indisponibilidad. Por ejemplo, inundación de paquetes SYS, amplificación de paquetes UDP, TCP.
		Sabotaje	Corresponde al daño, deterioro o interrupción intencional de un servicio, utilizando medios tecnológicos o físicos.
		Interrupción	Son fallas fortuitas que interrumpen, degradan o inhabilitan las funciones de un servicio.
Seguridad de contenidos	Eventos relacionados con la confidencialidad e integridad de la información. Corresponde a dos de las tres dimensiones de la seguridad de la información.	Acceso no autorizado a la información	Corresponde al uso de permisos y/o credenciales obtenidas ilícitamente para acceder a servicios, recursos o activos informáticos, afectando la confidencialidad de la información.
		Modificación no autorizada de la información	Cualquier alteración ilícita sobre los datos de un sistema o aplicación que afectan su integridad.
		Exfiltración de información	Extracción (copia, transferencia o recopilación no autorizada) de datos ilícitos que afecta a la confidencialidad de la información.
		Pérdida de Información	Corresponde a una situación (robo, pérdida o fallo físico de un dispositivo de almacenamiento) en la cual se deja de poseer información.
Fraude	Perjuicio patrimonial mediante la manipulación, alteración de datos o sistemas informáticos.	Uso no autorizado de recursos	Uso ilícito de recursos de una organización.
		Derechos de Autor	Copia, distribución o instalación ilícita de activos digitales, por ejemplo, software comercial u otro tipo de material protegido por derechos de autor.
		Phishing	Se refiere al envío de correos electrónicos que tienen apariencia legítima, pero que en realidad pretenden manipular al receptor para robar información confidencial.
		Suplantación	Consiste en el robo de identidad en internet para hacerse pasar por otra persona u organización con el fin de cometer actividades delictivas, tales como fraude o estafas.

CSIRT Gobierno de Chile

Firmado digitalmente por CSIRT Gobierno de Chile
Fecha: 2023.01.11 17:31:57 -03'00'

CSIRT

Equipo de Respuesta ante Incidentes
de Seguridad Informática



EQUIPO DE RESPUESTA ANTE INCIDENTES DE SEGURIDAD INFORMÁTICA
MINISTERIO DEL INTERIOR Y SEGURIDAD PÚBLICA
SUBSECRETARÍA DEL INTERIOR
https://www.csirt.gob.cl/
Teatinos 92 piso 6 Santiago, Chile
Teléfono 1510
soc-csirt@interior.gob.cl

CSIRT
Equipo de Respuesta ante Incidentes de Seguridad Informática