Compendio de Normas del Seguro Social de Accidentes del Trabajo y Enfermedades Profesionales

CAPÍTULO II. Reporte de ciberincidentes

1. Mecanismo de reporte

Los organismos administradores deberán reportar a la Superintendencia de Seguridad Social todos los ciberincidentes que detecten en sus redes, equipos y sistemas y que alcancen los niveles de peligrosidad e impacto establecidos en las tablas indicadas en el número 2. Niveles de peligrosidad y número 3. Niveles de impacto del presente Capítulo II. En caso que un suceso pueda asociarse con dos o más tipos de incidentes con niveles de peligrosidad o impacto distintos, se le asignará el nivel más alto.

2. Niveles de peligrosidad

El nivel de peligrosidad determina la potencial amenaza que supondría la materialización de un incidente en las redes, equipos y sistemas del organismo administrador, así como su efecto en la calidad o continuidad en el otorgamiento de las prestaciones del Seguro de la Ley N°16.744.

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

Niveles de peligrosidad		
Nivel	Clasificación	Tipo de incidente
Crítico	Amenaza avanzada persistente	APT: Ataques dirigidos contra organizaciones concretas, sustentados en mecanismos muy sofisticados de ocultación, anonimato y persistencia. Esta amenaza habitualmente emplea técnicas de ingeniería social para conseguir sus objetivos junto con el uso de procedimientos de ataque conocidos o genuinos.
Muy alto	Código dañino	● Distribución de malware: - Ej: recurso de una organización empleada para distribuir malware. ● Configuración de malware: - Recurso que aloje ficheros de configuración de malware. Ej: ataque de webinjects para troyano.
	Intrusión	● Robo: - Ej: acceso no autorizado a un sistema informático con el fin de conocer sus datos internos, apoderarse de ellos o utilizar sus recursos, acceso no autorizado a Centro de Proceso de Datos. ● Sabotaje: - Ej: destrucción, inutilización, de un sistema de tratamiento de información, la destrucción, alteración de datos contenidos en un sistema de tratamiento de información, cortes de cableados de equipos o incendios provocados.
	Disponibilidad del servicio	● Interrupciones: - Ej: ataque informático.
Alto	Contenido abusivo	● Pornografía infantil, contenido sexual o violento inadecuado: - Ej: Material que represente de manera visual contenido relacionado con pornografía infantil, apología de la violencia, etc.
	Código dañino	● Sistema infectado: - Ej: Sistema, computadora o teléfono móvil infectado con un rootkit. ● Servidor C&C (Mando y Control): - Ej: Conexión con servidor de Mando y Control (C&C) mediante malware o sistemas infectados.
	Intrusión	● Compromiso de aplicaciones: - Ej: Compromiso de una aplicación mediante la explotación de vulnerabilidades de software, como por ejemplo a través de una inyección de

		SQL. ● Compromiso de cuentas con privilegios: - Ej: Compromiso de un sistema en el que el atacante ha adquirido privilegios.
	Intento de Intrusión	Ataque desconocido: Ej: Ataque empleando exploit desconocido.
	Disponibilidad del servicio	● DoS (Denegación de servicio): - Ej: envío de peticiones a una aplicación web que provoca la interrupción o ralentización en la prestación del servicio. ● DDoS (Denegación distribuida de servicio): - Ej: inundación de paquetes SYN, ataques de reflexión y amplificación utilizando servicios basados en UDP.
	Compromiso de la información	● Acceso no autorizado a información: - Ej: robo de credenciales de acceso mediante interceptación de tráfico o mediante el acceso a documentos físicos. ● Modificación no autorizada de información: - Ej: modificación por un atacante empleando credenciales sustraídas de un sistema o aplicación o encriptado de datos mediante ransomware.
	Fraude	● Pérdida de datos: - Ej: pérdida por fallo de disco duro o robo físico ● Phishing.
Medio	Contenido abusivo	● Discurso de odio: - Ej: ciberacoso, racismo, amenazas a una persona o dirigida contra colectivos.
	Obtención de información	● Ingeniería social - Ej: mentiras, trucos, sobornos, amenazas. ● Explotación de vulnerabilidades conocidas: - Ej: desbordamiento de buffer, puertas traseras, cross site scripting (XSS).
	Intrusión	● Intento de acceso con vulneración de credenciales: - Ej: intentos de ruptura de contraseñas,ataque por fuerza bruta. ● Compromiso de cuentas sin privilegios.
	Disponibilidad del servicio	● Mala configuración: - Ej: Servidor DNS con el KSK de la zona raíz de DNSSEC obsoleto. ● Uso no autorizado de recursos: - Ej: uso de correo electrónico para participar en estafas piramidales.
	Fraude	● Derechos de autor: - Ej: uso, instalación, distribución de software sin la correspondiente licencia. ● Suplantación: - Ej: suplantación de una entidad por otra para obtener beneficios ilegítimos.
	Vulnerable	● Criptografía débil: - Ej: servidores web susceptibles de ataques POODLE/FREAK. ● Amplificador DDoS: - Ej: DNS openresolvers o Servidores NTP con monitorización monlist. ● Servicios con acceso potencial no deseado: - Ej: Telnet, RDP o VNC. ● Revelación de información: - Ej: SNMP o Redis. ● Sistema vulnerable:

		- Ej: mala configuración de proxy en cliente (WPAD), versiones desfasadas de sistema.
Bajo	Contenido abusivo	● Spam ● Escaneo de redes: - Ej: peticiones DNS, ICMP, SMTP, escaneo de puertos.
	Obtención de información	● Análisis de paquetes (sniffing).
	Otros	● Otros: - Todo aquel incidente que no tenga cabida en ninguna categoría anterior.

3. Niveles de impacto

Los posibles niveles de impacto de un ciberincidente se clasifican en 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 ciberincidentes	
Nivel	Descripción
Crítico	Afecta a sistemas clasificados como confidenciales o que contengan información calificada como datos sensibles de acuerdo a la ley.
	Afecta a más del 50% de los procesos que soportan los sistemas del organismo administrador.
	Interrupción de la prestación del servicio igual o superior a 12 horas o superior al 40% de los beneficiarios del seguro.
	Afecta a más del 50% de sus agencias o centros de atención a nivel nacional.
	Daños reputacionales de difícil reparación, con eco mediático (amplia cobertura en los medios de comunicación) afectando a la reputación de terceros.
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 del organismo administrador.
	Interrupción de la prestación del servicio igual o superior a 8 horas o superior al 30% de los beneficiarios del seguro.
	Afecta a más del 40% de sus agencias o centros de atención a nivel nacional.
	Daños reputacionales, con eco mediático (amplia cobertura en los medios de comunicación) afectando a la reputación de terceros.
Alto	Afecta a más del 30% de los procesos que soportan los sistemas del organismo administrador.
	Interrupción de la prestación del servicio igual o superior a 6 horas o superior al 20% de los beneficiarios del seguro.
	Afecta a más del 30% de sus agencias o centros de atención a nivel nacional.
	Daños reputacionales, con eco mediático (amplia cobertura en los medios de comunicación) que no afecta la reputación de terceros.
Medio	Afecta a más del 20% de los procesos que soportan los sistemas del organismo administrador.
	Interrupción de la prestación del servicio igual o superior a 4 horas y superior al 10% de los beneficiarios del seguro.
	Afecta a más del 20% de sus agencias o centros de atención a nivel nacional.
	Daños reputacionales sin eco mediático.
Bajo	Afecta al 10% o más, de los sistemas del organismo administrador.
	Interrupción de la prestación del servicio igual o superior a 2 horas y superior al 5% de los beneficiarios del seguro.
	Afecta al 10% o más, de sus agencias o centros de atención a nivel nacional.
Sin impacto	No hay ningún impacto apreciable.

4. Resolución de ciberincidentes

Una vez detectado un ciberincidente que afecte a una red, equipo o sistema utilizado en el otorgamiento de las prestaciones del Seguro de la Ley N° 16.744, el organismo administrador deberá efectuar, de manera oportuna, todas las gestiones que sean necesarias para su resolución y restaurar la normal provisión de los servicios afectados, dando primera prioridad a aquellas medidas que permitan evitar o, en su defecto, minimizar el impacto a los grupos de interés.

En caso que el organismo administrador afectado lo considere necesario, podrá solicitar la colaboración de la Superintendencia de Seguridad Social u otras entidades competentes en materia de ciberseguridad, para la resolución de un ciberincidente.

Los organismos administradores 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.

Asimismo, sin perjuicio de las medidas inmediatas conducentes a la mitigación de los efectos y al restablecimiento de los servicios afectados por un ciberincidente, los organismos administradores deberán subsanar, en la medida que sea técnicamente posible, las vulnerabilidades de sus sistemas, equipos y redes que hubieren permitido o facilitado el ciberincidente.

En caso que un organismo administrador detecte que sus redes, equipos y sistemas fueron utilizados como medio para la

comisión de algún delito informático, éste deberá efectuar las denuncias ante los órganos competentes, ejercer las acciones judiciales pertinentes e informar a la Superintendencia de Seguridad Social.

Los organismos administradores deberán establecer los protocolos de recuperación de la información, en caso de pérdida de ésta por manipulación, ciberincidentes u otras causas de su responsabilidad.

5. Contenido de los reportes de ciberincidentes

Los organismos administradores deberán reportar toda aquella información relativa al ciberincidente, cuyo nivel de impacto o peligrosidad, se encuentra definido en los niveles Alto, Muy Alto o Crítico, según lo establecido en el número 2. Niveles de peligrosidad y en el número 3. Niveles de impacto, ambos del presente Capítulo II.

Esta información deberá ser recopilada con la rapidez que amerita, sin afectar la estrategia de contención del incidente y los mecanismos desplegados para evitar la propagación del mismo en la red interna, en la red externa y la interoperación con los beneficiarios y grupos de interés.

Además de la rapidez para obtener la información, se recomienda seguir las buenas prácticas de primera respuesta forense internacionalmente aceptadas o que hayan sido validadas nacionalmente por el Instituto Nacional de Normalización, con el objetivo de contaminar lo menos posible las evidencias que permitan investigaciones avanzadas por parte de equipos de ciberseguridad altamente especializados o los entes persecutores que correspondan.

Sin perjuicio de lo anterior, los organismos administradores deberán mantener una bitácora con el registro de todos los ciberincidentes identificados:

a) Reporte de alerta de ciberincidente

   Dentro del plazo de 1 hora, contado desde la toma de conocimiento del ciberincidente, los organismos administradores deberán reportar al sistema GRIS, a través del documento **D.14** "Reporte de alerta de ciberincidente", conforme a lo establecido en el Anexo N°21 "Reportes de Ciberincidentes", de la Letra F. Anexos, del presente Título V, la siguiente información:

   i) Identificación del organismo administrador;

   ii) Resumen ejecutivo del ciberincidente;

   iii) Fecha y hora precisas de detección del ciberincidente;

   iv) Recursos tecnológicos afectados, y

   v) Tipo de ciberincidente.

b) Informe parcial de ciberincidente

   Posteriormente, a las 6 horas desde la toma de conocimiento del ciberincidente, los organismos administradores deberán reportar al sistema GRIS, a través del documento **D.15** "Informe parcial de ciberincidente", conforme a lo establecido en el Anexo N°21 "Reportes de Ciberincidentes", de la Letra F. Anexos, del presente Título V, la siguiente información:

   i) Identificación del organismo administrador;

   ii) Resumen ejecutivo del ciberincidente;

   iii) Fecha y hora estimada de ocurrencia del ciberincidente;

   iv) Fecha y hora estimada de detección del ciberincidente;

   v) Descripción detallada de lo sucedido, señalando los activos de información afectados y su nivel de sensibilidad y afectación (confidencialidad/integridad/disponibilidad);

   vi) Recursos tecnológicos afectados;

   vii) Tipo de ciberincidente;

   viii) Extensión geográfica, si se conoce;

   ix) Sistemas de información afectados actuales y potenciales, y

   x) Grupos de interés afectados actuales y potenciales.

c) Informe de Informe de resolución de ciberincidente

   Finalmente, a los 10 días hábiles desde la toma de conocimiento del ciberincidente, los organismos administradores deberán reportar al sistema GRIS, a través del documento **D.16** "Informe de resolución de ciberincidente", conforme a lo establecido en el Anexo N°21 "Reportes de Ciberincidentes", de la Letra F. Anexos, del presente Título V, la siguiente

información:

i) Identificación del organismo administrador;

ii) Resumen ejecutivo del ciberincidente;

iii) Origen o causa identificable del ciberincidente;

iv) Total de sistemas de información afectados;

v) Total de grupos de interés afectados;

vi) Infraestructura crítica afectada;

vii) Descripción de los niveles 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 HASH (MD5/SHA1/SHA256 o el que los reemplace), vulnerabilidades facilitadoras del incidente y posibles vectores de ingreso/egreso de los artefactos, y en general los datos técnicos del incidente, entre otros similares;

viii) Descripción del plan de acción y medidas de resolución y mitigación;

ix) Medios necesarios para la resolución calculados en horas hombre (HH) / persona;

x) Impacto económico estimado, si procede y es conocido;

xi) Daños reputacionales, aun cuando sean eventuales, y

xii) Descripción cronológica de los hechos asociados del ciberincidente.