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

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.