

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

/ LIBRO VII. ASPECTOS OPERACIONALES Y ADMINISTRATIVOS / TÍTULO V. Gestión de la Seguridad de la Información / D. Ciberseguridad / CAPÍTULO II. Reporte de ciberincidentes / 2. Niveles de peligrosidad

## 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                | <ul style="list-style-type: none"> <li>● Distribución de malware:                             <ul style="list-style-type: none"> <li>- Ej: recurso de una organización empleada para distribuir malware.</li> </ul> </li> <li>● Configuración de malware:                             <ul style="list-style-type: none"> <li>- Recurso que aloje ficheros de configuración de malware. Ej: ataque de webinjects para trojano.</li> </ul> </li> </ul>                                                                                                                                                                                                                         |
|                         | Intrusión                    | <ul style="list-style-type: none"> <li>● Robo:                             <ul style="list-style-type: none"> <li>- 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.</li> </ul> </li> <li>● Sabotaje:                             <ul style="list-style-type: none"> <li>- 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.</li> </ul> </li> </ul> |
|                         | Disponibilidad del servicio  | <ul style="list-style-type: none"> <li>● Interrupciones:                             <ul style="list-style-type: none"> <li>- Ej: ataque informático.</li> </ul> </li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| Alto                    | Contenido abusivo            | <ul style="list-style-type: none"> <li>● Pornografía infantil, contenido sexual o violento inadecuado:                             <ul style="list-style-type: none"> <li>- Ej: Material que represente de manera visual contenido relacionado con pornografía infantil, apología de la violencia, etc.</li> </ul> </li> </ul>                                                                                                                                                                                                                                                                                                                                               |
|                         | Código dañino                | <ul style="list-style-type: none"> <li>● Sistema infectado:                             <ul style="list-style-type: none"> <li>- Ej: Sistema, computadora o teléfono móvil infectado con un rootkit.</li> </ul> </li> <li>● Servidor C&amp;C (Mando y Control):                             <ul style="list-style-type: none"> <li>- Ej: Conexión con servidor de Mando y Control (C&amp;C) mediante malware o sistemas infectados.</li> </ul> </li> </ul>                                                                                                                                                                                                                   |
|                         | Intrusión                    | <ul style="list-style-type: none"> <li>● Compromiso de aplicaciones:                             <ul style="list-style-type: none"> <li>- Ej: Compromiso de una aplicación mediante la explotación de vulnerabilidades de software, como por ejemplo a través de una inyección de SQL.</li> </ul> </li> <li>● Compromiso de cuentas con privilegios:                             <ul style="list-style-type: none"> <li>- Ej: Compromiso de un sistema en el que el atacante ha adquirido privilegios.</li> </ul> </li> </ul>                                                                                                                                                |
|                         | Intento de Intrusión         | Ataque desconocido:<br>Ej: Ataque empleando exploit desconocido.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
|                         | Disponibilidad del servicio  | <ul style="list-style-type: none"> <li>● DoS (Denegación de servicio):                             <ul style="list-style-type: none"> <li>- Ej: envío de peticiones a una aplicación web que provoca la interrupción o ralentización en la prestación del servicio.</li> </ul> </li> <li>● DDoS (Denegación distribuida de servicio):                             <ul style="list-style-type: none"> <li>- Ej: inundación de paquetes SYN, ataques de reflexión y amplificación utilizando servicios basados en UDP.</li> </ul> </li> </ul>                                                                                                                                  |

|       |                              |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
|-------|------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|       | Compromiso de la información | <ul style="list-style-type: none"> <li>● Acceso no autorizado a información: <ul style="list-style-type: none"> <li>- Ej: robo de credenciales de acceso mediante interceptación de tráfico o mediante el acceso a documentos físicos.</li> </ul> </li> <li>● Modificación no autorizada de información: <ul style="list-style-type: none"> <li>- Ej: modificación por un atacante empleando credenciales sustraídas de un sistema o aplicación o encriptado de datos mediante ransomware.</li> </ul> </li> </ul>                                                                                                                                                                                                                                                  |
|       | Fraude                       | <ul style="list-style-type: none"> <li>● Pérdida de datos: <ul style="list-style-type: none"> <li>- Ej: pérdida por fallo de disco duro o robo físico</li> </ul> </li> <li>● Phishing.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| Medio | Contenido abusivo            | <ul style="list-style-type: none"> <li>● Discurso de odio: <ul style="list-style-type: none"> <li>- Ej: ciberacoso, racismo, amenazas a una persona o dirigida contra colectivos.</li> </ul> </li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
|       | Obtención de información     | <ul style="list-style-type: none"> <li>● Ingeniería social <ul style="list-style-type: none"> <li>- Ej: mentiras, trucos, sobornos, amenazas.</li> </ul> </li> <li>● Explotación de vulnerabilidades conocidas: <ul style="list-style-type: none"> <li>- Ej: desbordamiento de buffer, puertas traseras, cross site scripting (XSS).</li> </ul> </li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                        |
|       | Intrusión                    | <ul style="list-style-type: none"> <li>● Intento de acceso con vulneración de credenciales: <ul style="list-style-type: none"> <li>- Ej: intentos de ruptura de contraseñas, ataque por fuerza bruta.</li> </ul> </li> <li>● Compromiso de cuentas sin privilegios.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
|       | Disponibilidad del servicio  | <ul style="list-style-type: none"> <li>● Mala configuración: <ul style="list-style-type: none"> <li>- Ej: Servidor DNS con el KSK de la zona raíz de DNSSEC obsoleto.</li> </ul> </li> <li>● Uso no autorizado de recursos: <ul style="list-style-type: none"> <li>- Ej: uso de correo electrónico para participar en estafas piramidales.</li> </ul> </li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                  |
|       | Fraude                       | <ul style="list-style-type: none"> <li>● Derechos de autor: <ul style="list-style-type: none"> <li>- Ej: uso, instalación, distribución de software sin la correspondiente licencia.</li> </ul> </li> <li>● Suplantación: <ul style="list-style-type: none"> <li>- Ej: suplantación de una entidad por otra para obtener beneficios ilegítimos.</li> </ul> </li> </ul>                                                                                                                                                                                                                                                                                                                                                                                             |
|       | Vulnerable                   | <ul style="list-style-type: none"> <li>● Criptografía débil: <ul style="list-style-type: none"> <li>- Ej: servidores web susceptibles de ataques POODLE/FREAK.</li> </ul> </li> <li>● Amplificador DDoS: <ul style="list-style-type: none"> <li>- Ej: DNS openresolvers o Servidores NTP con monitorización monlist.</li> </ul> </li> <li>● Servicios con acceso potencial no deseado: <ul style="list-style-type: none"> <li>- Ej: Telnet, RDP o VNC.</li> </ul> </li> <li>● Revelación de información: <ul style="list-style-type: none"> <li>- Ej: SNMP o Redis.</li> </ul> </li> <li>● Sistema vulnerable: <ul style="list-style-type: none"> <li>- Ej: mala configuración de proxy en cliente (WPAD), versiones desfasadas de sistema.</li> </ul> </li> </ul> |
| Bajo  | Contenido abusivo            | <ul style="list-style-type: none"> <li>● Spam</li> <li>● Escaneo de redes: <ul style="list-style-type: none"> <li>- Ej: peticiones DNS, ICMP, SMTP, escaneo de puertos.</li> </ul> </li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
|       | Obtención de información     | <ul style="list-style-type: none"> <li>● Análisis de paquetes (sniffing).</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
|       | Otros                        | <ul style="list-style-type: none"> <li>● Otros: <ul style="list-style-type: none"> <li>- Todo aquel incidente que no tenga cabida en ninguna categoría anterior.</li> </ul> </li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |

