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"> ● Distribución de malware: <ul style="list-style-type: none"> - Ej: recurso de una organización empleada para distribuir malware. ● Configuración de malware: <ul style="list-style-type: none"> - Recurso que aloje ficheros de configuración de malware. Ej: ataque de webinjects para trojano.
	Intrusión	<ul style="list-style-type: none"> ● Robo: <ul style="list-style-type: none"> - 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: <ul style="list-style-type: none"> - 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	<ul style="list-style-type: none"> ● Interrupciones: <ul style="list-style-type: none"> - Ej: ataque informático.
Alto	Contenido abusivo	<ul style="list-style-type: none"> ● Pornografía infantil, contenido sexual o violento inadecuado: <ul style="list-style-type: none"> - Ej: Material que represente de manera visual contenido relacionado con pornografía infantil, apología de la violencia, etc.
	Código dañino	<ul style="list-style-type: none"> ● Sistema infectado: <ul style="list-style-type: none"> - Ej: Sistema, computadora o teléfono móvil infectado con un rootkit. ● Servidor C&C (Mando y Control): <ul style="list-style-type: none"> - Ej: Conexión con servidor de Mando y Control (C&C) mediante malware o sistemas infectados.
	Intrusión	<ul style="list-style-type: none"> ● Compromiso de aplicaciones: <ul style="list-style-type: none"> - 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: <ul style="list-style-type: none"> - 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	<ul style="list-style-type: none"> ● DoS (Denegación de servicio): <ul style="list-style-type: none"> - Ej: envío de peticiones a una aplicación web que provoca la interrupción o ralentización en la prestación del servicio. ● DDoS (Denegación distribuida de servicio): <ul style="list-style-type: none"> - Ej: inundación de paquetes SYN, ataques de reflexión y amplificación utilizando servicios basados en UDP.

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