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

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.