TAXONOMÍA CLASIFICACIÓN CIBERINCIDENTES

TAXONOMÍA			
Clasificación	**Definición**	**Tipo de incidente**	**Descripción**
Contenido abusivo	Ataques destinados a dañar la imagen de la organización o utilizar sus recursos electrónicos para usos ilícitos (como publicidad, extorsión o ciberdelincuencia en general)	**Spam**	Correo electrónico masivo no solicitado. El receptor del contenido no ha otorgado autorización válida para recibir un mensaje compartido.
		Delito de odio	Contenido difamatorio o discriminatorio. Ej: Ciberacoso, racismo, amenazas a una persona o dirigidas contra colectivos o grupos.
		Materiales de abuso/explotación sexual infantil, contenido sexual o violento inadecuado	Material que represente de manera visual contenido relacionado con pornografía infantil, apología de la violencia, etc.
Contenido dañino	Incidentes relacionados con actividades maliciosas, aplicaciones y archivos dañinos para obtener acceso no autorizado al sistema para sustraer, exfiltrar, eliminar, modificar su información privada que pretenden acceder a sus datos u.	**Sistema infectado**	Sistema infectado con malware. Ej: Sistema, computador, dispositivos móviles infectado con un rootkit
		Servidor C&C (Comando y Control)	Conexión con servidor de Comando y Control (C&C) mediante malware o sistemas infectados.
		Distribución de malware	Recurso usado para distribución de malware. Ej: Recurso de una organización empleado para distribuir malware.
		Configuración de malware	Recurso que aloje archivos de configuración de malware Ej: Ataque de webinjects para troyano.
Obtención de información	Incidentes relacionados con la identificación y recopilación de información de personas, infraestructura tecnológica y activos de información de una organización a través de técnicas no autorizadas con fines delictivos.	**Escaneo de redes (scanning)**	Envío de peticiones a un sistema para descubrir posibles debilidades. Se incluyen también procesos de comprobación o testeo para recopilar información de alojamientos, servicios y cuentas. Ej: Peticiones DNS, ICMP, SMTP y escaneo de puertos.
		Análisis de paquetes (sniffing)	Observación y grabación del tráfico de redes.
		Ingeniería social	Recopilación de información personal sin el uso de la tecnología. Ej: Mentiras, trucos, sobornos, amenazas.

Equipo de Respuesta a Emergencias Cibernéticas de Colombia – COLCERT
Edificio Murillo Toro Cra. 8a entre calles 12A y 12B
Bogotá, Colombia
Código Postal 111711
Teléfono: +57 601 344 22 22 Línea Gratuita: 01-800-0952525
www.colcert.gov.co contacto@colcert.gov.co @COLCERT

Intento de intrusión	Incidentes relacionados con la utilización de técnicas que intentan atacar una infraestructura tecnológica o un activo de información aprovechándose de una vulnerabilidad para obtener el control y privilegios administrativos o de ejecución.	**Explotación de vulnerabilidades conocidas**	Intento de compromiso de un sistema o de interrupción de un servicio mediante la explotación de vulnerabilidades con un identificador estandarizado (véase CVE). Ej: Desbordamiento de buffer, puertas traseras y cross site scripting (XSS).
		Intento de acceso con vulneración de credenciales	Múltiples intentos de vulnerar credenciales. Ej: Intentos de ruptura de contraseñas, ataque por fuerza bruta.
		Ataque desconocido	Ataque empleando exploit desconocido
Intrusión	Ataques que aprovechar las vulnerabilidades de diseño, funcionamiento o configuración de las diferentes tecnologías, para entrar de forma fraudulenta a los sistemas de una organización	**Compromiso de cuenta con privilegios**	Compromiso de un sistema en el que el atacante ha adquirido privilegios.
		Compromiso de cuenta sin privilegios	Compromiso de un sistema empleando cuentas sin privilegios.
		Compromiso de aplicaciones	Compromiso de una aplicación mediante la explotación de vulnerabilidades del software. Ej: Inyección SQL y defacement.
		Robo	Intrusión física. Ej: acceso no autorizado a Centro de Procesamiento de Datos.
Disponibilidad	Interrupción de la capacidad de procesamiento y respuesta de los sistemas y redes para dejarlos inoperativos Acción premeditada para dañar un sistema, interrumpir un proceso, cambiar o borrar información.	**DoS (Denegación de Servicio)**	Ataque de 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)	Ataque de Denegación Distribuida de Servicio. Ej: Inundación de paquetes SYN, ataques de reflexión y amplificación utilizando servicios basados en UDP.
		Mala configuración	Configuración incorrecta del software que provoca problemas de disponibilidad en el servicio. Ej: Servidor DNS con el KSK de la zona raíz de DNSSEC obsoleto.
		Sabotaje	Sabotaje físico. Ej: Cortes de cableados de equipos, desconexión de equipos o incendios provocados
		Interrupciones	Interrupciones por causas ajenas. Ej: Desastre natural.
Compromiso de Información	Incidentes relacionados con el acceso, filtraciones (confidencialidad), la modificación o el borrado (integridad) de información.	**Acceso no autorizado a 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	Modificación no autorizada de información. Ej: Modificación por un atacante empleando credenciales sustraídas de un sistema o aplicación o encriptado de datos mediante ransomware.

		Pérdida de datos	Pérdida de información Ej: Pérdida por fallo de disco duro o robo físico.
Fraude	Incidentes relacionados con la pérdida de bienes causada con intención fraudulenta o deshonesta en procura de un beneficio económico para sí mismo, para otra persona o empresa	**Uso no autorizado de recursos**	Uso de recursos para propósitos inadecuados, incluyendo acciones con ánimo de lucro. Ej: uso de correo electrónico para participar en estafas piramidales.
		Derechos de autor	Ofrecimiento o instalación de software carente de licencia u otro material protegido por derechos de autor. Ej: Warez
		Suplantación	Tipo de ataque en el que una entidad suplanta a otra para obtener beneficios ilegítimos.
		Phishing	Suplantación de otra entidad con la finalidad de convencer al usuario para que revele sus credenciales privadas.
Vulnerable	Incidentes relacionados con la identificación del grado de debilidad inherente en un sistema de hardware o software que permitan a un atacante realizar actividades no autorizadas a la misma organización o en contra de otra.	**Criptografía débil**	Servicios accesibles públicamente que puedan presentar criptografía débil. Ej: Servidores web susceptibles de ataques POODLE/FREAK.
		Amplificador DDoS	Servicios accesibles públicamente que puedan ser empleados para la reflexión o amplificación de ataques DDoS. Ej: DNS open-resolvers o Servidores NTP con monitorización monlist.
		Servicios con acceso potencial no deseado	Ej: Telnet, RDP o VNC.
		Revelación de información	Acceso público a servicios en los que potencialmente pueda relevarse información sensible. Ej: SNMP o Redis.
		Sistema vulnerable	Sistema vulnerable. Ej: mala configuración de proxy en cliente (WPAD), versiones desfasadas de sistema.
Otros	Incidentes no clasificados en la taxonomía existente o amenazas persistentes avanzadas	**Incidente no clasificado**	Incidentes que no se ajustan a la clasificación existente, actuando como indicador para la actualización de la clasificación.
		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.

Equipo de Respuesta a Emergencias Cibernéticas de Colombia – COLCERT
Edificio Murillo Toro Cra. 8a entre calles 12A y 12B
Bogotá, Colombia
Código Postal 111711
Teléfono: +57 601 344 22 22 Línea Gratuita: 01-800-0952525
www.colcert.gov.co contacto@colcert.gov.co @COLCERT