Categorización de incidentes (taxonomía)

Clase de ciberincidente	Descripción	Tipo de ciberincidente
Código dañino	Software cuyo objetivo es infiltrarse o dañar un equipo, servidor u otro dispositivo de red, sin el conocimiento de su responsable o usuario y con finalidades muy diversas.	Virus, Gusanos, troyanos, spyware, rootkit, ransomware, herramientas para acceso remoto RAT
Disponibilidad	Ataques dirigidos a poner fuera de servicio los sistemas, al objeto de causar daños en la productividad y/o la imagen de las instituciones atacadas.	Denegación [Distribuida] del Servicio DoS / DDoS, Fallo (Hardware/Software), Error humano, Sabotaje.
Obtención de información	Técnicas utilizadas por el atacante para obtener información de la plataforma tecnológica como parte de las etapas de un ataque cibernético	Identificación de vulnerabilidades (scanning), Sniffing, Ingeniería social, phishing.
Intrusiones	Ataques dirigidos a la explotación de vulnerabilidades de diseño, de operación o de configuración de diferentes tecnologías, al objeto de introducirse de forma fraudulenta en los sistemas de una entidad.	Compromiso de cuenta de usuario, Defacement (desfiguración), Cross- Site Scripting (XSS), Cross-Site Request Forgery (CSRF) Falsificación de petición entre sitios cruzados, Inyección SQL, Spear Phishing, Pharming (DNS), Ataque de fuerza bruta, Inyección de archivos Remota, Explotación de vulnerabilidad software, Explotación de vulnerabilidad en hardware
Compromiso de la información	Incidentes relacionados con el acceso y fuga (Confidencialidad), modificación o borrado (Integridad) de información no pública.	Acceso no autorizado a información, modificación y borrado no autorizado de información, Publicación no autorizada de información, Ex filtración de información.
Fraude	Incidentes relacionados con acciones fraudulentas derivadas de suplantación de identidad, en todas sus variantes.	Suplantación / Spoofing, uso de recursos no autorizados, uso ilegitimo de credenciales, violaciones de derechos de propiedad intelectual o industrial.
Contenido Abusivo	Ataques dirigidos a dañar la imagen de la organización o a utilizar sus medios electrónicos para otros usos ilícitos (tales como la publicidad, la extorsión o, en general la ciberdelincuencia).	Spam (correo basura), acoso, extorsión, mensajes ofensivos, pederastia, racismo, apología de la violencia/delito.
Política de seguridad	Incidentes relacionados por violaciones por parte de usuarios de las políticas de seguridad aprobadas por la entidad.	Abuso de privilegios por usuarios, acceso a servicios no autorizados, sistema desactualizados Otros
Otros	Otros incidentes no incluidos en los apartados anteriores	

CLASE_CIBERINCIDENTE	TIPO
CODIGO_DAÑINO_MALWARE	VIRUS
	GUSANOS
	TROYANOS
	SPYWARE
	ROOTKIT
	RAMSONWARE
	RAT (REMOTE ACCESS TOOLS)
DISPONIBILIDAD	DENEGACIÓN [DISTRIBUIDA] DEL SERVICIO DOS / DDOS
	FALLO (HARDWARE/SOFTWARE)
	ERROR HUMANO
	SABOTAJE
OBTENCION_DE_INFORMACION	IDENTIFICACIÓN DE ACTIVOS Y VULNERABILIDADES (ESCANEO)
	SNIFFING
	INGENIERÍA SOCIAL
	PHISHING
INTRUSIONES	COMPROMISO DE CUENTA DE USUARIO
	DEFACEMENT (DESFIGURACIÓN)
	CROSS-SITE SCRIPTING (XSS)
	FALSIFICACIÓN DE PETICIÓN ENTRE SITIOS CRUZADOS (CSRF)
	INYECCIÓN SQL
	SPEAR PHISHING
	PHARMING
	ATAQUE DE FUERZA BRUTA
	INYECCIÓN DE ARCHIVOS DE FORMA REMOTA
	EXPLOTACIÓN DE VULNERABILIDAD SOFTWARE
	EXPLOTACIÓN DE VULNERABILIDAD HARDWARE
	ACCESO NO AUTORIZADO A RED
COMPROMISO_DE_INFORMACION	ACCESO NO AUTORIZADO A INFORMACIÓN
	MODIFICACIÓN Y BORRADO NO AUTORIZADA DE INFORMACIÓN.
	PUBLICACIÓN NO AUTORIZADA DE INFORMACIÓN
	EXFILTRACIÓN DE INFORMACIÓN
FRAUDE	SUPLANTACIÓN / SPOOFING
	USO DE RECURSOS NO AUTORIZADO
	USO ILEGÍTIMO DE CREDENCIALES
	VIOLACIONES DE DERECHOS DE PROPIEDAD INTELECTUAL O INDUSTRIAL.
CONTENIDO_ABUSIVO	SPAM (CORREO BASURA)
	ACOSO/EXTORSIÓN/ MENSAJES OFENSIVOS
	PEDERASTIA/ RACISMO/ APOLOGÍA DE LA VIOLENCIA/DELITO, ETC.
POLITICA_DE_SEGURIDAD	ABUSO DE PRIVILEGIOS POR USUARIOS
	ACCESO A SERVICIOS NO AUTORIZADOS
	SISTEMA DESACTUALIZADO
OTROS	OTROS