Auditoría de Incidentes de Ciberseguridad.

Incidentes de Ciberseguridad

INCIBE. *Incidente de Ciberseguridad* (CC0)

Un **incidente de ciberseguridad** es un evento o una serie de eventos singulares, inesperados o no deseados, que tienen una probabilidad significativa de **comprometer las operaciones del negocio y de amenazar la seguridad de la información**.

Por ello, es clave conocer su tipología, analizar su impacto, determinar su causa raíz u origen y reaccionar para contenerlo.

En esta unidad se reflexionará acerca de cómo efectuar las tareas pertinentes con objeto de prepararse adecuadamente antes de la aparición del posible incidente.

1.- Taxonomía de Incidentes de Ciberseguridad.

La Clasificación de los Incidentes de Ciberseguridad

INCIBE. *Contenido Dañino* (CC0)

La **taxonomía empleada por INCIBE-CERT**, en concordancia con la taxonomía definida en la **Guía Nacional de Notificación y Gestión de Ciberincidentes**, se basa en la **Taxonomía de Referencia** para la Clasificación de Incidentes de Seguridad, desarrollada coordinadamente por un **grupo internacional de equipos de respuesta a incidentes.**

Su propósito es **alinear los conceptos de análisis, impacto, contención, tratamiento y estudio de todos los incidentes**, con objeto de **adoptar políticas similares** y **diseñar respuestas sinérgicas** entre las diferentes organizaciones.

Contenido abusivo

- SPAM: correo electrónico masivo no solicitado. El receptor del contenido no ha otorgado autorización válida para recibir un mensaje colectivo.
- Delito de odio: contenido difamatorio o discriminatorio. Ejemplos: ciberacoso, racismo, amenazas a una persona o dirigidas contra colectivos.
- Pornografía infantil, contenido sexual o violento inadecuado: material que represente de manera visual contenido relacionado con pornografía infantil, apología de la violencia, etc.

Contenido dañino

- Sistema infectado: sistema infectado con malware. Ejemplo: sistema, ordenador o teléfono móvil infectado con un *rootkit* (malware que brinda acceso y control remoto de un dispositivo a un hacker).
- Servidor C&C: conexión con servidor de Mando y Control (control centralizado de redes de robots o *botnets*, además de otras amenazas complejas) mediante malware o sistemas infectados.
- Distribución de malware: recurso usado para distribución de malware. Ejemplo: recurso de una organización empleado para distribuir malware.
- Configuración de malware: recurso que aloje ficheros de configuración de malware. Ejemplo: ataque de *webinjects* (robo de credenciales e información personal a través de un navegador) para troyano.
- Malware dominio DGA: nombre de dominio generado mediante DGA, empleado por malware para contactar con un servidor de Mando y Control.

Obtención de información

- 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. Ejemplos: peticiones DNS, ICMP (ping), SMTP (correo), escaneo de puertos.
- Análisis de paquetes (*sniffing*): observación y grabación del tráfico de redes.
- Ingeniería Social: recopilación de información personal con técnicas cercanas al puro espionaje. Ejemplos: mentiras, trucos, sobornos, amenazas aunque, por lo general, en esta categoría también se suelen incluir los mecanismos de recopilación de información personal basados en herramientas tecnológicas, como pueden ser los *stealers* y los *keyloggers*.

Intento de intrusión

- 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 (CVE). Ejemplos: desbordamiento de buffer, puertas traseras, XSS.
- Intento de acceso con vulneración de credenciales: múltiples intentos de vulnerar credenciales. Ejemplos: intentos de ruptura de contraseñas, ataque por fuerza bruta.
- Ataque desconocido: ataque empleando *exploit* desconocido.

Intrusión

- 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 de software. Ejemplo: inyección SQL.
- Robo: intrusión física. Ejemplo: acceso no autorizado a Centro de Proceso de Datos y sustracción de equipo.

Disponibilidad

- DoS: ataque de Denegación de Servicio. Ejemplo: envío de peticiones a una aplicación web que provoca la interrupción o ralentización en la prestación del servicio.
- DDoS: ataque de Denegación Distribuida de Servicio. Ejemplos: inundación de paquetes SYN (sincronización), ataques de reflexión y amplificación utilizando servicios basados en UDP(datagramas, no orientados a conexión).
- Sabotaje: sabotaje físico. Ejemplos: cortes de cableados de equipos o incendios provocados.
- Interrupciones: interrupciones por causas externas. Ejemplo: desastre natural.

Compromiso de la información

- Acceso no autorizado a información. Ejemplos: robo de credenciales de acceso mediante interceptación de tráfico o mediante el acceso a documentos físicos.
- Modificación no autorizada de información. Ejemplos: modificación por un atacante empleando credenciales sustraídas de un sistema o aplicación, o encriptado de datos mediante *ransomware*.
- Pérdida de datos: pérdida de información. Ejemplos: pérdida por fallo de disco duro o robo físico.
- Fuga de Información Confidencial. Información confidencial filtrada, como credenciales o datos personales.

Fraude

- Uso no autorizado de recursos: uso de recursos para propósitos inadecuados, incluyendo acciones con ánimo de lucro. Ejemplo: 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. Ejemplos: *Warez* (distribución de información a grupos, violando los derechos de autor).
- 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.

Vulnerabilidad

- Criptografía débil: servicios accesibles públicamente que pueden presentar criptografía débil. Ejemplo: servidores web susceptibles de ataques POODLE/FREAK (vulnerabilidades y ataques a sistemas de cifrado).
- Amplificador DDoS: servicios accesibles públicamente que puedan ser empleados para la reflexión o amplificación de ataques DDoS. Ejemplos: DNS open-resolvers o Servidores NTP con monitorización *monlist* (para obtener información de depuración de servidores de hora).
- Servicios con acceso potencial no deseado: servicios accesibles públicamente potencialmente no deseados. Ejemplos: Telnet, RDP o VNC.
- Revelación de información: acceso público a servicios en los que potencialmente pueda revelarse información sensible. Ejemplos: SNMP (mantenimiento) o Redis (gestor de bases de datos en memoria, basado en tablas de *hash*).
- Sistema vulnerable. Ejemplos: mala configuración de proxy en cliente (WPAD), versiones desfasadas de sistema.

Otros

- Todo aquel incidente que no tenga cabida en ninguna categoría anterior.
- 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.
- Ciberterrorismo: uso de redes o sistemas de información con fines de carácter terrorista.
- Daños informáticos PIC: borrado, dañado, alteración, supresión o inaccesibilidad de datos, programas informáticos o documentos electrónicos de una infraestructura crítica. Conductas graves relacionadas con los términos anteriores que afecten a la prestación de un servicio esencial.

Para saber más

La versión actualizada de la Taxonomía de Referencia se puede consultar a través del enlace al sitio mantenido por el grupo de trabajo:

https://github.com/enisaeu/Reference-Security-Incident-Taxonomy-Task-Force/blob/master/working_copy/humanv1.md

Ejercicio - Phishing y Emulación Web

En este ejercicio se mostrará un escenario de Phishing y Emulación Web.

Para ello, se emularán las pantallas de entrada de algunos portales populares mediante un Phisher, con objeto de capturar las credenciales de acceso de los usuarios forma fraudulenta.

Ejercicio Resuelto (pdf - 855464 B)

Ejercicio - Stealers y Keyloggers

Existen multitud de herramientas de Ingeniería Social, aparte del espionaje en directo. Estas herramientas permiten robar credenciales e información personal, como se verá a continuación.

En este ejercicio se efectuará una práctica basada en Stealers y Keyloggers, con objeto de capturar información crítica de forma imperceptible y fraudulenta.

Ejercicio Resuelto (pdf - 1315864 B)

Ejercicio - Vectores de Infeccion

"Vector de Infección" es un concepto que procede del mundo de la biología, por ejemplo, el mosquito *Anopheles* es el vector de infección del parásito *Plasmodium*, causante de la malaria. El procedimiento de actuación de un Vector Informático es idéntico, esto es, es un portador de una infección maliciosa que puede contaminar un sistema informático.

Existen muchas variantes de vectores, según el método de infección y el tipo de ataque asociado a la misma. En este ejercicio se generará un vector que actuará a través de un *exploit* y abrirá una *shell* inversa en un servidor, permitiendo al hacker tomar el control del mismo.

Ejercicio Resuelto (pdf - 463365 B)

Autoevaluación

¿A qué categoría de la taxonomía de incidentes pertenece el Compromiso de Cuenta, con o sin privilegios?

Contenido Abusivo

Contenido Dañino

Obtención de Información

Intento de Intrusión

Intrusión

Disponibilidad

Compromiso de la Información

Fraude

Vulnerabilidad

¡CORRECTO!

Ya se ha visto anteriormente la clasificación utilizada por INCIBE-CERT, basada en la de ENISA (*EU Agency for Cibersecurity*). No obstante, los incidentes se pueden clasificar de múltiples formas, obteniendo de esa

forma diferentes taxonomías posibles. Además, hay que tener en cuenta que no son excluyentes entre sí, es decir, un incidente puede pertenecer a varias taxonomías simultáneamente. Así, se muestran unos ejemplos de clasificaciones:

- Clasificación de incidentes basada en el impacto. Su foco es conocer el impacto que tendría el incidente en el sistema de información. Podría ser en los datos, las comunicaciones, la propia organización, etc.
- Clasificación de incidentes basada en el método. En este caso se centra en la técnica o método empleados por el atacante originario del incidente. Por ejemplo, denegación de servicio, *spam*, *phishing*, ingeniería social, etc.
- Clasificación de incidentes basada en el objetivo. Aquí se tiene en cuenta el objetivo que pretende alcanzar el atacante. Podrían ser personas concretas, empresas, sistemas en particular o países enteros.
- Clasificación del incidente según el origen. Se clasifica según el origen del atacante, que podría ser interno o externo. Cuando son incidentes internos, proceden de empleados de la propia organización (por múltiples motivos) o incidentes externos originados por agentes externos a la organización.
- Clasificación de incidentes basada en la intención. Con esta clasificación se muestra qué intención tiene el atacante con provocar el incidente. Por ejemplo, podría ser dejar inoperativo un servicio online o directamente obtener datos confidenciales de clientes.
- Clasificación de incidentes basada en la finalidad. Busca conocer la finalidad del ataque. Puede haber múltiples posibilidades, como puede ser una finalidad lucrativa (obtener información para posteriormente venderla o pedir un rescate tras cifrar información). Puede haber finalidades reivindicativas, como puede ser la exposición pública de información confidencial de una empresa u organización.

2.- Controles, Herramientas y Mecanismos.

¿Realmente se ha producido un incidente?

INCIBE. *Caja de Herramientas* (CC0)

No es fácil en todos los casos determinar con precisión si se ha producido o no un ciberincidente y, si es así, identificar su tipo y evaluar a priori su peligrosidad.

Por esta razón **se recomienda implementar y utilizar controles, herramientas y mecanismos de análisis de incidentes**, como se estudia a continuación.

Para poder conocer que se ha producido un incidente de ciberseguridad es necesario establecer una serie de **controles, herramientas y mecanismos** que ayuden al equipo de ciberseguridad a responder lo más rápido posible. Se pueden encontrar los siguientes tipos de controles:

- **Técnicos**. Pueden ser de tipo software o hardware, utilizados para proteger a los sistemas y datos. Ejemplo: antivirus, *firewalls*.
- **Físicos**. Protegen los elementos físicos. Unos ejemplos pueden ser los controles de acceso a las instalaciones o los sistemas de vigilancia.
- **Personales**. Buscan poder gestionar a los miembros de una organización y controlar lo relacionado con su comportamiento. Por ejemplo, por medio de sesiones de concienciación y formación de empleados.

Los controles mencionados son aplicados por medio de unos mecanismos o técnicas que permiten detectar e identificar los posibles incidentes de ciberseguridad. Podemos clasificarlos como:

- **Monitorización**. Esta técnica consiste principalmente en vigilar y supervisar los distintos sistemas de la organización, en tiempo real, para poder responder lo más rápido posible ante cualquier indicio que pudiera materializarse en un incidente. Es muy utilizada en los registros del sistema y las comunicaciones de las redes.
- **Recopilación de información**. En este caso, el objetivo consiste en recopilar datos relevantes que permitan posteriormente realizar una detección de vulnerabilidades, brechas de seguridad o encontrar el origen de amenazas o acciones inseguras.
- **Análisis de eventos**. Cuando se dispone de información recopilada, se procede a analizarla (registros de sistemas, transferencia de ficheros, correos electrónicos, etc.) y, de este modo, tratar de identificar comportamientos inusuales que muestren que se está produciendo un incidente de ciberseguridad.

Todas estas técnicas y procedimientos son aplicados por el equipo de ciberseguridad que puede haber en una organización haciendo uso de las herramientas de identificación y monitorización correspondientes. Los equipos de ciberseguridad pueden ser **internos** o **externos** a la organización.

Debes conocer

A la hora de elegir una organización cómo organizar a su equipo de ciberseguridad (si mantener un equipo interno a la organización o contratar los servicios a una empresa externa especializada) debe tener en cuenta las ventajas e inconvenientes de cada posibilidad.

<table>
<tr><td rowspan="2">Internos</td><td>Ventajas:
Conocimiento de la lógica interna de la organización.
Menor tiempo de respuesta.
Realizan un trabajo directo de manera constante.</td></tr>
<tr><td>Inconvenientes:
Las habilidades del personal pueden ser limitadas.
El coste de mantener todo el personal puede ser elevado.
Puede haber una posible dependencia de una persona en concreta.
Lleva tiempo formar al equipo.</td></tr>
<tr><td rowspan="2">Externos</td><td>Ventajas:
El coste es gestionable de antemano.
Proporciona equipos ya formados.
Los conocimientos y habilidades del personal especializado suele ser mayor.
Más fácil escalar en caso de necesidad.</td></tr>
<tr><td>Inconvenientes:</td></tr>
</table>

	• Desconocen la lógica interna de la organización. • No tienen control directo sobre las acciones a aplicar. • Menor control sobre las decisiones a tomar.

Dentro de los equipos de ciberseguridad se pueden encontrar los siguientes roles:

- **Centro de operaciones de Seguridad (*Security Operation Center*, SOC)**. Realiza la gestión de amenazas y herramientas gestión de incidentes.
- ***Blue Team***. Protege la organización monitorizando con herramientas y técnicas.
- ***Red Team***. Buscar posibles vulnerabilidades. La idea es atacar a la organización (realizar Hacking Ético), monitorizar y que el equipo de Blue Team proceda a corregir o mitigar.
- **CSIRT (*Computer Security Incident Response Team*)**. Se trata del equipo de respuesta a incidentes. Son los profesionales encargados de realizar la monitorización de los sistemas y aplicaciones para poder identificar los incidentes y proceder con la contención/mitigación y posterior restauración.
- **CERT (*Computer Emergency Response Team*)**. Es el equipo de respuesta a emergencias informáticas. Se usa indistintamente junto al CSIRT, aunque presenta ligeras diferencias. Se trata de una marca registrada y, para poder usarlo, se debe realizar un proceso de autorización y cumplimiento de requisitos. El CERT es un equipo que normalmente ofrece sus recursos y servicios a sectores grandes, como puede ser la administración de un gobierno público o sectores industriales o ciudadanía (como es el caso de INCIBE-CERT).
- **CISO (*Chief Information Security Officer*)**. Es el responsable de gestionar y supervisar la estrategia general del equipo de ciberseguridad y poner en marcha los planes necesarios para garantizar la ciberseguridad de la organización.

Y entre las tareas más comunes que suelen realizar, se encuentran:

- Buscar vulnerabilidades.
- Implementar soluciones de seguridad.
- Establecer el plan de comunicación.
- Auditar el cumplimiento de normativa de ciberseguridad.
- Desarrollar políticas y normativas de ciberseguridad.
- Proteger los datos confidenciales de la organización.
- Asegurarse de que se actualiza el *software*/*hardware*.
- Monitorizar los eventos del sistema para detectar anomalías.
- Dar respuesta a los incidentes que se produzcan.

Debes conocer

Como se ha visto antes, existen los roles de red team y blue team. Del mismo modo, es común conocer a los hackers como:

- ***Black hat* (sombreros negros)**. Son los hackers o grupo de hackers que buscan algún beneficio con el acceso u obtención de datos confidenciales de las organizaciones.
- ***White hat* (sombreros blancos)**. Son los conocidos como hacker éticos. Tratan de buscar vulnerabilidades en sistemas, aplicaciones u organizaciones, pero con un objetivo constructivo de que solucionar esas brechas de seguridad.

Para saber más

El siguiente enlace apunta a una página del INCIBE en la que se muestran los diferentes servicios disponibles para analizar y gestionar los incidentes de Ciberseguridad, acoplados a la taxonomía publicada asimismo por INCIBE-CERT:

https://www.incibe.es/protege-tu-empresa/blog/incidentes-seguridad-los-enemigos-tu-negocio

Autoevaluación

¿Cuál de las siguientes características es un inconveniente de tener un equipo de ciberseguridad interno?

La independencia asegurada de sus miembros.

El buen conocimiento de la lógica interna de la organización.

El alto coste de los miembros del equipo.

Un tiempo de respuesta bajo.

¡CORRECTO!

2.1.- Monitorización, Identificación, Detección y Alerta de Incidentes: Tipos y Fuentes.

INCIBE. *Detección y Alerta* (CC0)

Básicamente, los **indicios de la existencia de un ciberincidente** pueden provenir de dos tipos de fuentes: los **precursores** y los **indicadores**.

- Un **precursor** es un indicio de que puede ocurrir un incidente en el futuro.
- Un **indicador** es un indicio de que un incidente puede haber ocurrido o puede estar ocurriendo ahora.

Algunos ejemplos de **precursores** son:

- Las **entradas de log del servidor Web**, con los resultados de un escáner de vulnerabilidades.
- El **anuncio de un nuevo exploit**, dirigido a una atacar una vulnerabilidad que podría estar presente en los sistemas de la organización.
- **Amenazas explícitas provenientes de grupos o entidades concretos**, anunciando ataques a organizaciones objetivo (es el caso del anuncio de ataques por grupos *hacktivistas*, por ejemplo).

Los **indicadores** son muy comunes, tales como:

- El **sensor de intrusión** de una red emitiendo una alerta cuando ha habido un intento de desbordamiento de buffer de un servidor de base de datos.
- Las **alertas** generadas por software **antivirus**.
- La presencia de un **nombre** de archivo con **caracteres inusuales**.
- Un registro de log sobre un **cambio no previsto** en la configuración de un host.
- Los logs de una aplicación, advirtiendo de **reiterados intentos fallidos de login** desde un sistema externo desconocido.
- La detección de un número importante de **correos electrónicos rebotados** con contenido sospechoso.
- Una **desviación inusual del tráfico** de la red interna.
- etc.

La gestión y coordinación de incidentes desarrollada por el CCN-CERT para los organismos del sector público español, a través del **Sistema de Alerta Temprana de Red SARA** (SAT-SARA) y del **Sistema de Alerta Temprana para Sistemas de Control Industrial** (SAT-ICS) da adecuada respuesta a todas estas necesidades.

2.1.1.- Herramientas de identificación y monitorización.

Los equipos de ciberseguridad hacen uso de unas herramientas que les ayudan a detectar, identificar, dar respuesta y gestionar los incidentes que surjan. Hay multitud de herramientas y normalmente se pueden clasificar según para qué son utilizadas. Los ejemplos más típicos son:

- **Herramientas de protección de terminales (*Endpoint Protection Platform*, EPP)**. Son los conocidos antivirus o aplicaciones para detectar *malware*. Están instalados en los terminales de usuarios y ayudan a dar protegerlos. Ejemplos: ESET, Avast, etc.

- **Software de protección y respuesta (*Endpoint Detection and Response*, ERP)**. Igual que los anteriores, pero con alguna funcionalidad adicional, además de monitorizar gracias a distintas posibilidades (por ejemplo, haciendo uso de IA o aprendizaje automático).

- **Herramienta de monitorización de redes**. Vigilan a los dispositivos y al tráfico de la red. Buscan vulnerabilidades, anomalías, actividades sospechosas. Ejemplos de estas aplicaciones pueden ser Nagios, Auvik.

- **Escáneres de vulnerabilidades**. Son herramientas concretas y automatizadas para realizar el escaneo de puertos (redes, sistemas, aplicaciones, web, etc.). Están especializadas para vulnerabilidades conocidas. Por ejemplo:
    - **Acunetix**. Busca vulnerabilidades en páginas web como las típicas de inyección SQL o *cross-site scripting* (XXS).
    - **Nessus**. Herramienta con una gran base de datos de vulnerabilidades actualizada.
    - **OpenVAS**. Se ha desarrollado a partir de Nessus y, en este caso, es un proyecto gratuito. Es muy popular entre los escáneres de seguridad de red gratuitos y recibe actualizaciones con frecuencia.
    - **Nexpose**. Otra herramienta de código abierto que permite buscar configuraciones erróneas y vulnerabilidades en sistemas operativos.

- **Sistemas de detección/prevención de Intrusiones (*Intrusion Detection/Prevention System*, IDS/IPS)**. Ejemplo de herramientas: Snort, Suricata.
    - **IDS**. Monitorizan la red o sistemas para buscar señales maliciosas o accesos no autorizados. En el momento que encuentran algo, producen un evento al equipo de seguridad.
    - **IPS**. Es la funcionalidad que trata de obstaculizar a la intrusión. Con frecuencia, las herramientas IDS incorporan la funcionalidad IPS también.

- **Sistemas de gestión de eventos e información (*Security Information and Event Management*, SIEM)**. Son los que recopilan y analizan registros de diversas fuentes para detectar o identificar posibles amenazas. Por ejemplo, están las aplicaciones Splunk, QRadar (IBM), Elastic Stack.

- **Herramientas de prevención de pérdida de datos (*Data Loss Prevention*, DLP)**. Son las aplicaciones que utilizan reglas para monitorizar los accesos y manipulaciones de datos, en definitiva, está previendo posibles fugas de información. En caso de emergencia, alertan y actúan en consecuencia. Por ejemplo, los firewalls y proxy también contribuyen a ello.

2.2.- Detección e Identificación de Incidentes de Seguridad Física.

ISO. *ISO 27001* (CC0)
La seguridad física trata del **conjunto de medidas que protegen la documentación, equipos y activos físicos en general ante pérdidas, robos o accesos por personal no autorizado**, incluyendo además la formación y habilitación de las personas que deban acceder a materias clasificadas.

La **Norma ISO/IEC 27001** da una serie de recomendaciones en el ámbito de la seguridad física y del entorno, en lo relativo a **Áreas Seguras** y **Seguridad de los Equipos**, que se resumen a continuación.

Debes conocer

Hay múltiples **tipos de riesgos físicos** que afecten a una organización. Por ejemplo:

- **Acceso no autorizado**. Hay que controlar el acceso a edificios, salas internas, etc. (según el nivel de criticidad).
- **Robo**. De documentos, discos duros, pendrives, móviles, portátiles, etc.
- **Caída de suministros**. La electricidad, el acceso a internet.
- **Desastres naturales o climatológicos**. Pueden afectar a infraestructuras de suministros y comunicaciones.
- **Gestión deficiente de eliminación de residuos**. Cuando se sustituyen los discos duros o pendrives, hay que tener cuidado con el destino de los mismos y la preparación para su desecho.

2.2.1.- Áreas Seguras.

INCIBE. *Área Física Segura* (CC0)
El objetivo de estas recomendaciones es **prevenir el acceso físico no autorizado, los daños e interferencias** a la información de la organización y a los recursos de tratamiento de la información.

- **Perímetro de seguridad física.** Se deben utilizar perímetros de seguridad para proteger las áreas que contienen información sensible, así como los recursos de tratamiento de la información.
- **Controles físicos de entrada**. Las áreas seguras deben estar protegidas mediante controles de entrada adecuados, para asegurar que únicamente se permite el acceso al personal autorizado.
- **Seguridad de oficinas, despachos y recursos.** Para las oficinas, despachos y recursos, se debe diseñar y aplicar la seguridad física.
- **Protección contra las amenazas externas y ambientales.** Se debe diseñar y aplicar una protección física contra desastres naturales, ataques provocados por el hombre o accidentes.
- **Trabajo en áreas seguras.** Se deben diseñar e implementar procedimientos para trabajar en las áreas seguras.
- **Áreas de carga y descarga.** Deben controlarse los puntos de acceso, tales como las áreas de carga y descarga y otros puntos, donde pueda acceder personal no autorizado a las instalaciones, y si es posible, aislar dichos puntos de los recursos de tratamiento de la información para evitar accesos no autorizados.

Debes conocer

Se muestran a continuación unos ejemplos de medidas a tomar:

- Medidas de control de acceso: llaves de acceso, tarjeta, puerta, elementos biométricos (huella, iris, facial, voz,...), personal de seguridad, barreras, bolardos, etc.
- Medidas disuasorias y alerta. Ayuda a disuadir posibles ataques: sistemas de vigilancia (CCTV en puntos sensibles, entradas/salidas), sistemas de alarma (sensores de movimiento, detección de intrusión).
- Medidas contra desastres naturales: ubicaciones altas, habitaciones estancas, sensores de agua, sistema integral de detección y alarma contra incendios (sensores humo), protección estructural frente a terremotos, elementos fijación, plataformas que absorban vibraciones, aire acondicionado frente a olas de calor, elementos protección de sobretensión, alejar equipos estructura metálicas.

2.2.2.- Seguridad de los Equipos.

INCIBE. *Seguridad de los Equipos* (CC0)

El objetivo de estas recomendaciones es **evitar la pérdida, daño, robo o el compromiso de los activos y la interrupción de las operaciones** de la organización.

- **Emplazamiento y protección de equipos**. Los equipos deben situarse o protegerse de forma que se reduzcan los riesgos de las amenazas y los riesgos ambientales, así como las oportunidades de que se produzcan accesos no autorizados.
- **Instalaciones de suministro.** Los equipos deben estar protegidos contra fallos de alimentación y otras alteraciones causadas por fallos en las instalaciones de suministro.
- **Seguridad del cableado.** El cableado eléctrico y de telecomunicaciones que transmite datos o que sirve de soporte a los servicios de información debe estar protegido frente a interceptaciones, interferencias o daños.
- **Mantenimiento de los equipos.** Los equipos deben recibir un mantenimiento correcto que asegure su disponibilidad y su integridad continuas.
- **Retirada de materiales propiedad de la empresa.** Sin autorización previa, los equipos, la información o el software no deben sacarse de las instalaciones.
- **Seguridad de los equipos fuera de las instalaciones.** Deben aplicarse medidas de seguridad a los equipos situados fuera las instalaciones de la organización, teniendo en cuenta los diferentes riesgos que conlleva trabajar fuera de dichas instalaciones.
- **Reutilización o eliminación segura de equipos.** Todos los soportes de almacenamiento deben ser comprobados para confirmar que todo dato sensible y software bajo licencia se ha eliminado de manera segura, antes de deshacerse de ellos.
- **Equipo de usuario desatendido.** Los usuarios deben asegurarse que el equipo desatendido tiene la protección adecuada.
- **Política de puesto de trabajo despejado y pantalla limpia.** Debe adoptarse una política de puesto de trabajo despejado de papeles y medios de almacenamiento desmontables y una política de pantalla limpia para los recursos de tratamiento de la información.

Debes conocer

Se muestran a continuación unos ejemplos de medidas a tomar:

- Medidas de protección activos físicos: cables de seguridad para equipos, racks con cerradura, sistemas de seguimiento y localización para terminales móviles, etiquetado y registro.
- Medidas de protección de los suministros: tomas de tierra, reguladores de tensión, sistemas de alimentación ininterrumpida (con batería), protección del cableado externo/interno.

2.3.- Monitorización, Identificación, Detección y Alerta de Incidentes a través de la Investigación en Fuentes Abiertas.

Una vez que se va a iniciar el análisis e investigación del incidente, es el momento de recopilar toda la información posible procedente del **entorno digital**, como puede el compuesto por los sistemas y aplicaciones, los empleados y usuarios de los sistemas, las redes de comunicaciones, etc.

Esta recopilación de información se puede llevar a cabo gracias a las distintas herramientas de monitorización del tráfico de red (como puede ser Wireshark, Kismet, etc.), la recopilación de datos de registro por medio de los logs y su posterior análisis y visualización (como el SIEM Elastic Stack), las entrevistas con el personal involucrado que tienen información de primera mano y el ***footprinting*** de los distintos sistemas.

El ***footprinting*** se puede entender como una huella digital que posee los sistemas y, en el campo de la ciberseguridad, es de gran utilidad recopilar toda esa información porque sirve de ayuda para encontrar posibles vulnerabilidades que pudieran ser objeto de ataques. La información se obtiene tanto de los propios sistemas informáticos (sistema operativo, equipo usado, red, configuración de servidores, etc.) como de la propia organización (empleados, proveedores, nombre de dominio, etc.).

Debes conocer

Se pueden definir dos tipos de ***footprinting***:

- **Activo**: el obtenido por medio de diferentes herramientas aplicadas en los distintos sistemas.
- **Pasivo**: el que se obtiene a través de la investigación en distintos sitios y ubicaciones: motores de búsqueda, redes sociales, fuentes de datos abiertas, etc. Este caso es el conocido como la Inteligencia de fuentes abiertas (**OSINT**).

INCIBE. *Proceso OSINT* (CC0)
Inteligencia de fuentes abiertas u *Open Source Intelligence* (OSINT) hace referencia al **conocimiento recopilado a partir de fuentes de información de acceso público**. El proceso incluye la búsqueda, selección y adquisición de la información, así como su posterior procesado y análisis, con el fin de obtener conocimiento útil y aplicable en distintos ámbitos.

Existen **multitud de fuentes abiertas a partir de las cuales se puede obtener información relevante**, entre las que destacan:

- Medios de comunicación: revistas, periódicos, radio, etc.
- Información pública de fuentes gubernamentales.
- Foros, redes sociales, blogs, wikis, etc.
- Conferencias, simposios, *papers*, bibliotecas online, etc.

Algunos **ejemplos de la utilización de OSINT** son los siguientes:

- Conocer la reputación online de un usuario o empresa.
- Realizar estudios sociológicos, psicológicos, lingüísticos, etc.
- Auditoria de empresas y diferentes organismos con el fin de evaluar el nivel de privacidad y seguridad.
- Evaluar tendencias de mercados.
- Identificación y prevención de posibles amenazas en el ámbito militar o de la seguridad nacional.
- Como aspecto negativo, es utilizado por cibercriminales para lanzar ataques APT (Amenaza Persistente Avanzada) y *Spear Phishing* (estafa de correo electrónico o comunicaciones dirigida específicamente a una empresa o una persona).

El **Proceso OSINT** consta de las siguientes **fases**:

- **Requisitos**: es la fase en la que se establecen todos los requerimientos que se deben cumplir, es decir, aquellas condiciones que deben satisfacerse para conseguir el objetivo o resolver el problema que ha originado el desarrollo del sistema OSINT.
- **Identificar fuentes de información relevante**: consiste en especificar, a partir de los requisitos establecidos, las fuentes de interés que serán exploradas y recopiladas. Hay que tener presente que el

volumen de información disponible en Internet es prácticamente inabordable por lo que se deben identificar y concretar las fuentes de información relevante con el fin de optimizar y acotar el proceso de adquisición.
- **Adquisición**: etapa en la que se obtiene la información a partir de los orígenes indicados.
- **Procesamiento**: consiste en dar formato a toda la información recopilada de manera que pueda analizarse posteriormente.
- **Análisis**: es la fase en la que se genera inteligencia a partir de los datos recopilados y procesados. El objetivo es relacionar la información de distintos orígenes buscando patrones que permitan llegar a alguna conclusión significativa.
- **Presentación de inteligencia**: consiste en presentar la información obtenida de una manera eficaz, potencialmente útil y comprensible, de manera que pueda ser correctamente explotada.

Se pueden identificar principalmente 2 **problemas** a la hora de utilizar un sistema OSINT:

- **Demasiada información:** como ya se ha puesto de manifiesto, **la cantidad de información pública disponible en Internet es más que notable**. Es por ello, que se debe realizar un proceso muy exhaustivo a la hora de identificar y seleccionar las fuentes de información de interés que se van a recopilar, y que posteriormente servirán para la generación de inteligencia. El hecho de utilizar un catálogo extenso de fuentes conlleva obviamente un mayor gasto a la hora de implementar el sistema, y en el caso de no tener disponibles los recursos necesarios, provoca una significativa ralentización del mismo.
- **Fiabilidad de las fuentes:** es importante **valorar previamente las fuentes** que van a nutrir el sistema de información, ya que una selección incorrecta de las mismas puede provocar resultados erróneos y desinformación.

La inteligencia recopilada a partir de fuentes de acceso público (OSINT) ha cobrado una especial relevancia en los últimos años, principalmente promovida por la proliferación del uso de Internet y de las redes sociales. Existe una enorme cantidad de información disponible en la web y especialmente en la *Deep Web*, que puede resultar de gran interés en muy diversos campos que abarcan desde la seguridad de la información, la reputación online o la identificación y gestión de posibles riesgos para la seguridad nacional. Asimismo, cada vez se llevan a cabo más estudios sociológicos, psicológicos, o de otras materias que utilizan como base la información pública disponible en internet.

Otro aspecto significativo, y que permite darse cuenta de la importancia de este tipo de información, es la **aparición en el mercado laboral de la figura del Analista OSINT**, el cual es el encargado, entre otras cosas, de implementar y gestionar los sistemas OSINT.

Todo esto ha provocado que diferentes países destinen **cada vez más recursos a implementar estos sistemas**, creando incluso organismos como el ***Open Source Center* (OSC) en Estados Unidos** o asociaciones como ***Eurosint* en Bélgica**, encargadas de analizar los datos públicos con el fin de identificar y prevenir amenazas.

Por todo lo anteriormente indicado, es innegable que **la inteligencia de fuentes abiertas puede aportar gran cantidad de beneficios.**

Autoevaluación

¿Cuál **no** es una fase del proceso OSINT?

Difundir la información en sitio web.

Procesamiento de la información recopilada.

Establecer los requerimientos que se deben cumplir.

Identificar fuentes de información relevante.

¡CORRECTO!

2.4.- Herramientas OSINT.

Hay multitud de **herramientas y servicios** útiles a la hora de **implementar un sistema OSINT**. A continuación se mencionan algunos de ellos:

Buscadores habituales

Google, Bing, Yahoo, Ask. Permiten consultar toda la información que indexan. Asimismo, permiten especificar parámetros concretos (*Hacking* con buscadores: por ejemplo *"Google Hacking"* o *"Bing Hacking"*) de manera que se pueden realizar búsquedas con mucha mayor precisión que la que utilizan los usuarios habitualmente.

Dependiendo del buscador empleado se utilizan distintos parámetros, si bien algunos de ellos son comunes, como ocurre con las búsquedas parametrizadas:

- Ficheros con extensión pdf de un sitio web concreto.
- Exploración de sitios hackeados.

Mediante estos parámetros se puede obtener, entre otras cosas, **información sensible como nombres de usuarios y contraseñas procedentes de volcados de bases de datos**, localización de servidores vulnerables, acceso a dispositivos hardware online como webcams, cámaras de vigilancia o impresoras, o datos personales como DNI, cuentas bancarias, etc.

Buscadores especializados:

- **Shodan**: Permite entre otras cosas localizar ordenadores, webcams, impresoras, etc. basándose en el software, la dirección IP, la ubicación geográfica, etc. Mediante este servicio es posible localizar información de interés o de acceso a diversos sistemas, como por ejemplo: acceder a los sistemas de control de una Smart City y alterar su funcionamiento.
- **NameCHK:** es una herramienta que permite comprobar si un nombre de usuario está disponible en más de 150 servicios online. De este modo, se puede saber los servicios que utiliza un usuario en concreto, ya que habitualmente la gente mantiene dicho nombre para todos los servicios que utiliza. Además, disponen de una API que permite automatizar las consultas.
- **Knowem:** es una herramienta de similares características que NameCHK pero comprueba el nombre en más de 550 servicios, incluyendo dominios disponibles.
- **Tineye:** es un servicio que, partiendo de una imagen, indica en qué sitios web aparece. Es similar a la búsqueda por imagen que incorpora Google Imágenes.
- **Buscadores de información de personas:** permiten realizar búsquedas a través de diferentes parámetros como nombres, direcciones de correo o teléfonos. A partir de datos concretos localizan a usuarios en servicios como redes sociales, e incluyen posibles datos relacionados con ellos como números de teléfono o fotos. Algunos de los portales que incorporan este servicio son: Spokeo, Pipl, 123people o Wink.

Herramientas de recolección de metadatos:

- **Metagoofil:** permite la extracción de metadatos de documentos públicos (pdf, doc, xls, ppt, docx, pptx, xlsx). A partir de la información extraída se pueden obtener direcciones de correo electrónico del personal de una empresa, o el software utilizado para la creación de los documentos y, por tanto, poder buscar vulnerabilidades para dicho software, nombres de empleados, etc.
- **Libextractor:** es una aplicación similar a Metagoofil que soporta muchos más formatos, si bien la información obtenida no es de tanta utilidad.

Servicios para obtener información a partir de un dominio:

- **Domaintools:** es uno de los servicios referentes en este ámbito, ya que incorpora un gran número de funcionalidades. Cabe destacar que permite crear alertas a usuarios que registran dominios, monitorizar dominios e IPs, crear alertas para dominios nuevos que contengan ciertas palabras, e incluso un servicio de investigación de gran cantidad de amenazas como *spear phishing*, denegación de servicio, *spam*, fraude o malware.
- **Robtex**: muestra, entre otras cosas, la fiabilidad del dominio, su posición en el ranking Alexa, el listado de subdominios, los servidores de correo o el ISP que utiliza.
- **MyIPNeighbors**: permite obtener el listado de dominios que comparten servidor con el dominio indicado.

APIs de diferentes servicios como Facebook, Twitter o Youtube:

- Mediante los métodos que implementan se pueden **consultar de una manera automatizada los datos publicados**.

Herramientas Palantir y Maltego

Merecen una mención especial Palantir y Maltego al implementar un **gran número de funcionalidades** y ser unos de los **grandes referentes en la materia** de la inteligencia de las fuentes abiertas.

- **Palantir**: es una empresa que tiene como cliente a diferentes servicios del Gobierno de Estados Unidos (CIA, NSA y FBI) y que se centra en el desarrollo de **software contra el terrorismo y el fraude**, mediante la gestión y explotación de grandes volúmenes de información.
- **Maltego**: permite **visualizar de manera gráfica las relaciones** entre personas, empresas, páginas web, documentos, etc. a partir de información pública. La documentación completa de la herramienta se puede encontrar en la web oficial https://docs.maltego.com/support/home.

Otras herramientas de interés:

- **GooScan**: permite automatizar búsquedas en Google, pudiendo identificar de una manera sencilla subdominios de un dominio concreto, fugas de información o posibles vulnerabilidades.
- **SiteDigger**: al igual que GooScan permite automatizar búsquedas. Busca en la caché de Google para identificar vulnerabilidades, errores, problemas de configuración, etc.
- **OsintStalker (FBStalker y GeoStalker)**: utilizan diferentes redes sociales como Facebook, LinkedIn, Flickr, Instagram y Twitter para recolectar gran cantidad de información sobre una persona. Permiten localizar lugares y sitios web visitados con regularidad, amigos online, etc. y mostrar los datos en Google Maps.
- **Cree.py**: permite obtener datos de Twitter, Flickr e Instagram. A partir de la selección de una cuenta, extrae fechas e información GPS, y crea una base de datos en formato csv o kmz para visualizarlos.

- **TheHarvester**: esta herramienta obtiene emails, subdominios, host, nombres de empleados, puertos abiertos, etc. a través de diferentes servicios como Google, Bing, LinkedIn y Shodan.
- **DumpltBlue+**. Se trata de una extensión para Chrome que busca material en Facebook.
- **Osintgram** (https://github.com/Datalux/Osintgram). Herramienta para recopilar y analizar información de una cuenta de Instagram.
- **CrossLinked** (https://github.com/m8sec/CrossLinked). Muestra información acerca de los empleados asociados a una organización en Linkedin.
- **Treeverse** (https://treeverse.app/). Una extensión disponible en Chrome y Firefox que permite ver y navegar por distintos hilos de la red X (anteriormente Twitter).

A continuación, se muestran una serie de comandos/parámetros disponibles para utilizar en el motor de búsqueda Google (**Google Hacking**).

- Búsqueda de frases exactas. Utilizar entrecomillado " ". Ej.: "incidentes de ciberseguridad".
- Exlcluir una palabra de la búsqueda. Utilizar el guión -. Ej.: incidentes -seguridad. Buscaría "incidentes" pero sin "ciberseguridad".
- Búsqueda por sinónimos. Utilizar la virgulilla ~. Ej.: incidentes ~ciberseguridad.
- Comodín que vale cualquier texto. El asterisco *. Se puede combinar con las comillas en frases exactas. Ej.: "incidentes de ciberseguridad*20*".
- Búsqueda de páginas que contengan dos palabras separadas una distancia máxima: around(distancia). Ej.: integridad around(4) ciberseguridad.
- Búsqueda de un tipo de fichero con filetype:tipo de fichero. Ej.: filetype:pdf.
- Búsqueda de una extensión concreta con ext:extension. Ej.: ext:pdf.
- Búsqueda de páginas que contengan en algún lugar el texto indicado: intext:texto y también indicando varias palabras allintext:frase texto. Ej.: allintext:escenarios de riesgo de ciberseguridad.
- Búsqueda de páginas con un texto en la dirección url: inurl:texto y también indicando varias palabras con allinurl:texto.
- Búsqueda de páginas que contengan texto en el título intitle:texto y con varias palabras allintitle:texto. Ej.: allintitle:medidas de seguridad.
- Búsqueda de páginas que apuntan a una url concreta usando link. Ej.: link:incibe.es.
- Cuando se desee realizar búsqueda que satisfagan una u otra condición, se puede usar el operador OR (o barra vertical |). Ej: ext:txt OR ext:mp3.

También se pueden usar múltiples parámetros de manera conjunta, perfilando así aún más la búsqueda a realizar. Por ejemplo, podemos buscar páginas de una empresa que estén en dominios no seguros que pudieran ser fraudulentos: site:incibe.* -inurl:https.

Shodan es un buscador que permite indicar múltiples parámetros configurables para encontrar dispositivos conectados Internet. Se puede consultar el listado completo en la web oficial https://www.shodan.io/search/filters. Una serie de esos filtros personalizables de búsqueda son:

- after: se muestran los resultados después de la fecha indicada (dd/mm/aaaa).
- asn: número del sistema autónomo (red grande o grupo de redes que tiene una política de enrutamiento unificada).
- before: se muestran los resultados antes de la fecha indicada (dd/mm/aaaa).
- city: filtro por nombre de ciudad. Por ejemplo, city:Madrid.
- country: permite buscar en un país específico usando su código de dos letras. Por ejemplo, country:ES.
- has_screenshot: encuentra dispositivos que tienen una captura. Se utilizan los valores true o false.
- server: dispositivos o servidores específicos.
- hostname: nombre completo del host.
- http.tittle: que tengan un título específico. Por ejemplo, http.title:"Alojamiento".
- ip: dirección IP.
- isp: proveedor de internet.
- net: rango de red en notación CIDR. Por ejemplo, net:172.13.0.0/16.
- org: organización. Por ejemplo, org:google.
- os: sistema operativo. Por ejemplo, os:windows.

- port: número de puerto de un servicio. Por ejemplo, port:3389 para buscar máquinas windows con este puerto de escritorio remoto expuesto.
- product: nombre del software que está usando el servicio. Por ejemplo, producto:“Apache httpd”.
- region: región/estado/comunidad autónoma, usando su código de dos letras. Por ejemplo, region:AN buscaría en Andalucía.
- version: versión del producto.
- vuln: permite buscar dispositivos que presenten una vulnerabilidad concreta, haciendo uso de la nomenclatura de vulnerabilidades CVE (Common Vulnerabilities and Exposures). Este filtro solo está disponible en la versión de pago de Shodan.

Autoevaluación

¿Cuál de las siguientes herramientas OSINT se centra en el desarrollo de software contra el terrorismo?

Maltego

SiteDigger

TheHarvester

Palantir

GooScan

¡CORRECTO!

Para saber más

En el siguiente enlace se puede acceder a una red de herramientas OSINT gratuitas, organizadas y categorizadas:

https://osintframework.com/

3.- Clasificación, Valoración, Documentación, Seguimiento Inicial de Incidentes de Ciberseguridad.

La Gestión de Incidentes de Ciberseguridad

Francisco Artés - Elaboración Propia. *Detección Temprana y Análisis Forense* (CC0)

La gestión de incidentes se basa en disponer de un plan de acción para atender a los incidentes que vayan surgiendo. Además de resolverlos, dicho plan debe incorporar medidas de rendimiento que permitan conocer la calidad del sistema de protección y **detectar tendencias antes de que se conviertan en grandes problemas.**

Para ello, l**a estrategia más importante es la detección temprana de incidentes** mediante un IDS eficiente y su **análisis rápido** en varias etapas (preliminar, profundo, forense) para implementar **políticas de respuesta inmediata y programación IPS** (prevención de incidentes).

En el momento de detectarse un incidente, gracias al uso de herramientas IDS, se procederá a su registro y documentación en una base de datos, donde se almacenarán al menos los siguientes datos:

- Tipo de incidente. Haciendo uso de la taxonomía de Incibe vista en la unidad. Se pueden utilizar los subtipos necesarios.
- Fecha y hora del incidente.
- Descripción. Cómo ha ocurrido, en qué sistemas y quién o quiénes se han visto involucrados.
- Gravedad. Un nivel aproximado de peligrosidad y cómo afecta a la organización, para adecuar la respuesta. Las plataformas de gestión de incidentes son capaces de asignar un nivel de gravedad en función de distintos aspectos (sistemas y servicios implicados, datos afectados, periodo de tiempo, alcance, etc.).
- Estado. Un atributo que muestra en qué punto se encuentra el incidente (abierto, en proceso, pendiente, solucionado, etc.).

Esta información se registra, documenta y realiza seguimiento haciendo uso de múltiples posibles herramientas de registro de incidencias o herramientas de ticketing genéricas. Ej.: SysAid ITSM, Jira Service Management.

No obstante, también se pueden encontrar herramientas específicas enfocadas a la **gestión de incidentes de ciberseguridad** (como las *Security Orchestration Automation and Response*, SOAR). Estas herramientas permiten automatizar posibles tareas de respuesta a incidentes, preparar flujos de trabajo para su resolución así como mostrar información de bases de datos sobre amenazas y vulnerabilidades (por ejemplo, con MITRE ATT&CK®, https://attack.mitre.org). Ej.: TheHive, FIR (*Fast Incident Response*), IBM QRadar SOAR o Splunk SOAR.

Al final, gracias al IDS, IPS, base de datos de taxonomía oficial y la base de datos de incidentes (una base de datos del conocimiento), el núcleo del gestor de incidentes será capaz de tomar las decisiones oportunas para aprender de los nuevos incidentes y prevenir los anteriormente ocurridos realimentándose continuamente.

La **base del análisis de incidentes** está constituida principalmente por **dos categorías de herramientas**:

- El **SIEM**, que almacenará la información de los incidentes de forma estructurada, permitiendo a los expertos efectuar el correspondiente estudio y obtener conclusiones aplicables a la prevención.
- Si el incidente ya ha tenido lugar, sólo cabrá utilizar herramientas de **Análisis Forense** (por ejemplo, Volatility) con el mismo objetivo de fondo, esto es, obtener suficiente información como para efectuar la prevención adecuada, además de rescatar toda la información válida que sea posible.

Además de esto y de forma continua, se deberá efectuar un **análisis de rendimiento y solidez de los sistemas de protección**, de forma contrastada con las amenazas más frecuentes registradas o reportadas externamente, para reforzar las políticas preventivas.

Debes conocer

En el registro de incidentes es importante hacer constar la **gravedad** del mismo, para poder dar prioridad a los incidentes más críticos. Para obtener la gravedad de un incidente es necesario realizar una valoración de varios factores:

- Sistemas y servicios implicados. Sistemas o servicios expuestos o alterados su funcionamiento.
- Datos afectados. Naturaleza de los datos (personales, estructurales, etc.) y la cantidad.
- Periodo de tiempo. Cuánto tiempo ha durado (horas, días, semanas, años, etc.).
- Alcance. Tamaño de la organización, número de empresas/personas afectadas.

Conociendo la información asociada a esos factores, podemos realizar una ponderación del nivel de peligrosidad. El CCN-CERT, en su Guía CCN-STIC 817 sobre seguridad de las TIC, establece cinco niveles de peligrosidad de los ciberincidentes, a saber:

- Nivel 1: BAJO.
- Nivel 2: MEDIO.
- Nivel 3: ALTO.
- Nivel 4: MUY ALTO.
- Nivel 5: CRÍTICO.

En esa misma guía, se ofrecen unos **criterios de determinación de la peligrosidad** para asignar el nivel de peligrosidad al ciberincidente en función del tipo de ataque (cómo de peligroso es el atacante) y el objetivo del ataque (el impacto y alcance del ataque). En la siguiente figura se muestran dichos criterios:

Fuente: CCN-CERT. *Niveles de peligrosidad de un ciberincidente*

Ejercicio Resuelto

Muchos ciberataques tienen éxito, por tanto, la clave está en analizarlos bien y extraer las correspondientes conclusiones de cara a la prevención de futuros ataques de similar etiología.

En este ejercicio se efectuará un análisis forense preliminar utilizando la herramienta Volatility, con objeto de mostrar qué información se puede derivar de un estudio de la información con posterioridad a un ataque.

Ejercicio Resuelto (pdf - 866989 B)

Autoevaluación

¿Cuál es la estrategia más importante en la Gestión de Incidentes?

El análisis de rendimiento y solidez de los sistemas de protección

La implementación y mantenimiento de un Inventario de Activos

La Detección Temprana de incidentes

El Análisis Forense de los incidentes

¡CORRECTO!

BIBLIOGRAFIA

- https://www.incibe-cert.es/taxonomia.
- https://github.com/enisaeu/Reference-Security-Incident-Taxonomy-Task-Force/blob/master/working_copy/humanv1.md.
- https://www.incibe.es/incibe-cert/guias-y-estudios/guias/guia-nacional-de-notificacion-y-gestion-de-ciberincidentes.
- https://www.incibe.es/ed2026/talento-hacker/emplea-hacker/soy-hacker/soy-CISO.
- https://www.ccn-cert.cni.es/series-ccn-stic/800-guia-esquema-nacional-de-seguridad/988-ccn-stic-817-gestion-de-ciberincidentes/file.html.
- https://www.ccn-cert.cni.es/publico/seriesCCN-STIC/series/400-Guias_Generales/401-glosario_abreviaturas/index.html?n=844.html.
- https://www.incibe-cert.es/blog/osint-la-informacion-es-poder.
- https://ens.ccn.cni.es/es/.
- https://www.ccn-cert.cni.es/es/seguridad-al-dia/novedades-ccn-cert/12666-actualizada-la-guia-ccn-stic-825-sobre-el-esquema-nacional-de-seguridad-y-la-certificacion-27001.html.
- https://www.industriaconectada40.gob.es/difusion/Documents/Documento_Norma_UNE-EN_ISO-IEC_27001%20MINTUR.pdf.