

# 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](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.

[Mostrar retroalimentación](#)

## 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.

[Mostrar retroalimentación](#)

## Ejercicio - Vectores de Infección

"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.

[Mostrar retroalimentación](#)

# Autoevaluación

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

Sugerencia

- Contenido Abusivo
- Contenido Dañino
- Obtención de Información
- Intento de Intrusión
- Intrusión
- Disponibilidad
- Compromiso de la Información
- Fraude
- Vulnerabilidad

## 2.- Controles, Herramientas y Mecanismos.

¿Realmente se ha producido un incidente?



[INCIBE](#). Caja de Herramientas (CCO)

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 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>

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

---



[INCIBE. Detección y Alerta \(CCO\)](#)

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

- ✓ Un **preursor** 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.

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

---



[ISO. ISO 27001 \(CC0\)](#)

La seguridad física trata del **conjunto de medidas que protegen la documentación y equipos 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.

## 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.

## 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.

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

---



[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**.

## 2.4.- Herramientas OSINT.



DOMAINTOOLS

robtex



SHODAN



API  
facebook



Twitter API



YouTube

Data API v3



Palantir

MALTEGO

Francisco Artés - Elaboración Propia. Herramientas OSINT (CC0)

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.

## 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.

## Autoevaluación

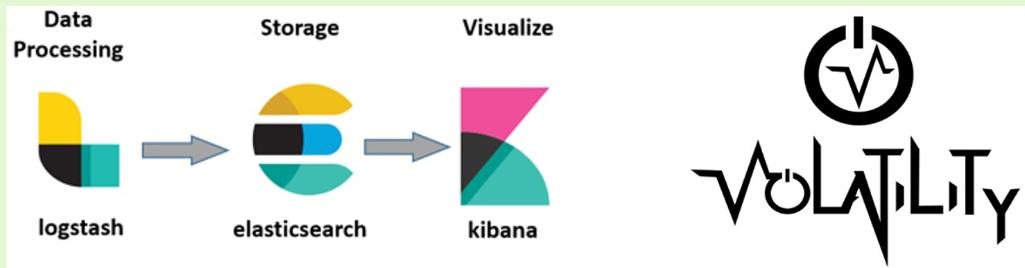
¿Cuál de las siguientes herramientas OSINT se centra en el desarrollo de software contra el terrorismo?

- Maltego
- SiteDigger
- TheHarvester
- Palantir
- GooScan



### **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, la 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).

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.

## 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.

[Mostrar retroalimentación](#)

## 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



## **4.- Bibliografía.**

---

[Bibliografía](#) (pdf - 37454 B)

# Condiciones y términos de uso de los materiales

Materiales desarrollados inicialmente por el Ministerio de Educación, Cultura y Deporte y actualizados por el profesorado de la Junta de Andalucía bajo licencia Creative Commons BY-NC-SA.



MINISTERIO  
DE EDUCACIÓN  
Y FORMACIÓN PROFESIONAL



Antes de cualquier uso leer detenidamente el siguiente [Aviso legal](#)

## Historial de actualizaciones

Versión: 01.00.01

Fecha de actualización: 20/10/23

Actualización de materiales y correcciones menores.

Versión: 01.00.00

Fecha de actualización: 04/07/23

Versión inicial de los materiales.