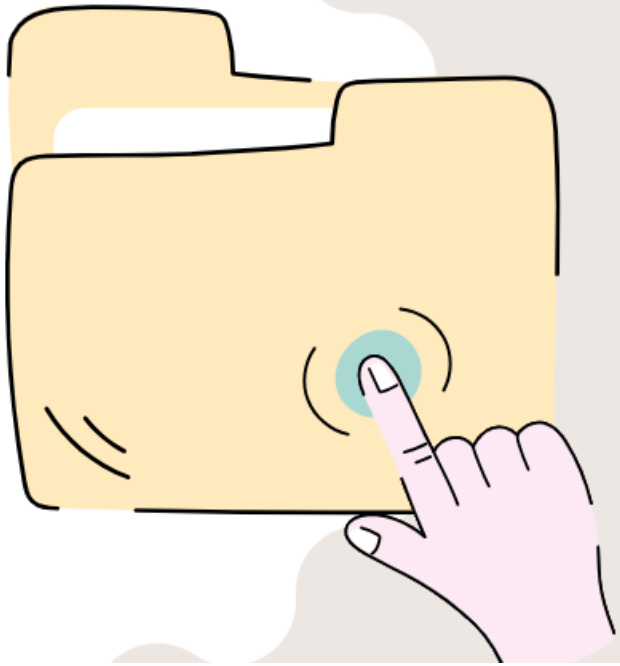
Informatica Forense



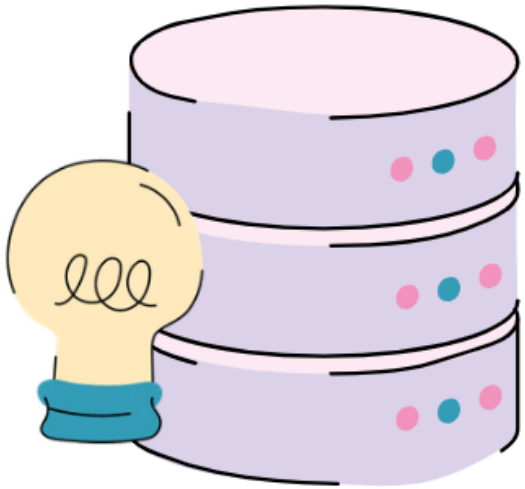
La informática forense es el uso de métodos y técnicas científicas probadas, con el fin de **identificar, recuperar, preservar, validar, analizar, interpretar, documentar y presentar** evidencia digital obtenida a partir de fuentes de información digital, con el propósito de facilitar la reconstrucción de hechos en una investigación legal, o ayudar a prevenir acciones en contra de la ley.

Objetivos de la Informática Forense

- Diseño de procesos para garantizar la autenticidad de evidencia digital.
- Recuperación, análisis y preservación de material digital y tecnológico.
- Adquisición y recuperación de datos y documentos eliminados.
- Preservar la evidencia de informática forense siguiendo la cadena de custodia.
- Identificar ciberdelincuentes y los motivos detrás de sus crímenes.

Principios de la informática Forense

En marzo de 1998, la IOCE (International Organization on Computer Evidence) se encargó de elaborar principios internacionales de informática forense para asegurar la estructura de los procesos de extracción de evidencia digital entre los países.



1. Cuando se trata de recolectar evidencia digital, todos los principios y procedimientos generales de la criminalística deberán ser aplicados.

2. Si se ocupa evidencia digital, ninguna acción realizada podrá cambiar la evidencia.

3. Cuando sea necesario que una persona acceda a la evidencia original, deberá ser un profesional forense.

4. Toda actividad relacionada con la ocupación, acceso, almacenamiento o transferencia de evidencia digital debe ser totalmente documentada, preservada y disponible para su revisión.

5. Se establece la responsabilidad individual de todas las acciones realizadas mientras la evidencia digital esté en posesión del individuo.

6. Cualquier agencia que ocupe, acceda, almacene o transfiera evidencia digital es responsable del cumplimiento de estos principios.

Hacker

Se trata de una persona que dispone de los conocimientos informáticos suficientes como para acceder a un determinado sistema o dispositivo y realizar cambios y modificaciones desde dentro.

versus

Cracker

Alguien que irrumpió en los sistemas informáticos, eludió contraseñas o licencias en programas informáticos o violó intencionalmente la seguridad informática de otras formas. Están motivados por intenciones maliciosas, con fines de lucro o simplemente porque el desafío está ahí.

Tipos de hacker

White Hat

Conocido comúnmente como hacking ético, el hacking de sombrero blanco siempre se usa para el bien. Utilizan casi los mismos métodos que cualquier otro hacker, pero lo hacen siempre con el permiso del propietario del sistema.

Grey Hat

El hacking de sombrero gris está en algún lugar entre lo ético y lo inmoral. Como norma, los hackers de sobrero gris nunca son completamente maliciosos, aunque algunos de sus movimientos pueden ser interpretados como tales. Por ejemplo, pueden entrar en una red sin el permiso de los propietarios para buscar vulnerabilidades. Después de eso, normalmente se pondrán en contacto con el propietario y preguntarán por una pequeña suma para reparar el problema.

Black Hat

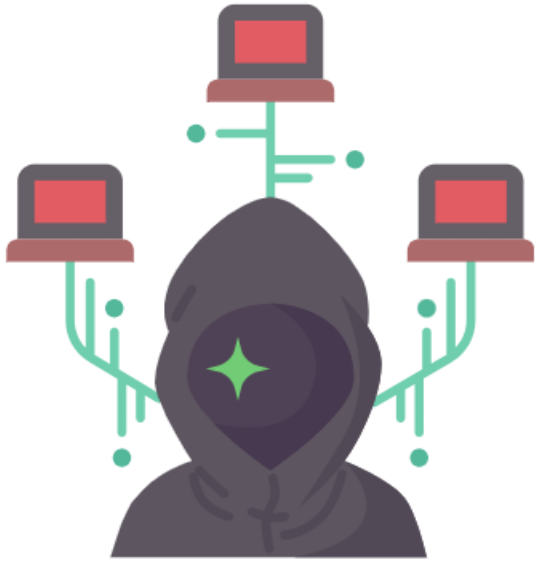
La hacking de sombrero negro es lo contrario al hacking de sombrero blanco, por eso se le denomina inmoral. Los ataques de sombrero negro normalmente están motivados por ganancias personales o económicas, aunque pueden estar motivados por muchos otros factores. Como no tienen permiso explícito del propietario para atacar su sistema, usan emails de phishing y páginas comprometidas para descargar e instalar software malicioso en el ordenador de la potencial víctima y lo usan para robar su información personal.

¿Qué es un ataque?

Un ataque cibernético es una **acción delictiva y malintencionada** que se realiza para acceder a información privada, bien para apropiarse de ella o bien para inutilizarla y pedir dinero a cambio de liberarla.

Detrás de estos **ataques cibernéticos** están delincuentes informáticos o hackers, cuyo objetivo es **apropiarse de la información o extorsionar** a la empresa o persona atacada.

Cualquier empresa que almacene, manipule o transmita datos se encuentra expuesta a un ciberataque.



Malware

Malware es un término genérico utilizado para describir una variedad de software hostil o intrusivo: virus informáticos, gusanos, caballos de Troya, etc.

Puede tomar la forma de código ejecutable, scripts, contenido activo y otro software.

El malware también puede hacer:

- encriptar o eliminar datos confidenciales
- modificar o desviar las funciones básicas del ordenador
- espiar la actividad informática de los usuarios

Firewall

Firewall o cortafuegos, es un sistema de seguridad que esencialmente actua como una frontera.
Esta frontera monitorea todos los paquetes, y solo deja entrar los que tengan ciertas caracteristicas.
Este sistema puede ser configurado de una infinidad de formas, se pueden poner "reglas" como **no permitir la entrada de paquetes que contengan x información o que provengan de x dirección.**

Ingeniería Social

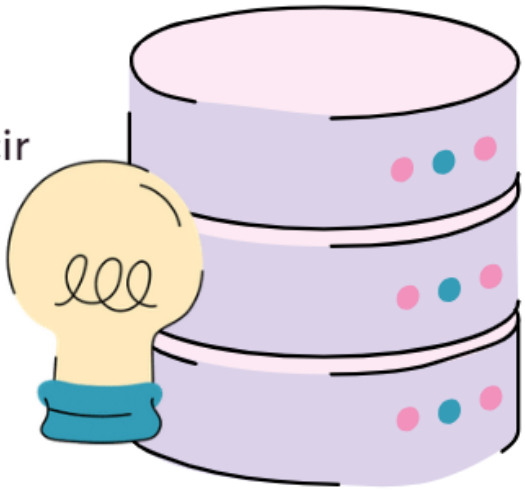
Es la metodología no-técnica de manipular a las personas por medios de sus defectos para llegar a un objetivo, usualmente malicioso.

A pesar de ser una metodología no-técnica, sigue cierta metodología para llegar a un objetivo, y se toman en cuenta varias "fallas" típicas que tenemos inherentemente los humanos.

Todos queremos ayudar

El primer movimiento siempre es de confianza

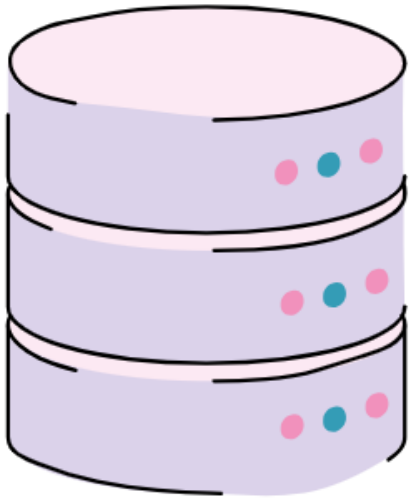
No nos gusta decir no

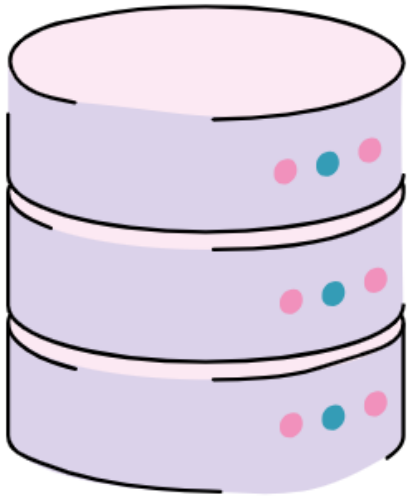


A todos nos gusta que nos alaben

Criptografía

Es la practica y estudio de las técnicas que se utilizan para comunicación segura contra los "adversarios", tiene mas de un siglo de ser utilizado para proteger la integridad, confidencialidad y disponibilidad de canales de comunicación.





Esteganografía

Es la otra forma de ocultar información, sin embargo, en vez de ponerle un candado a la información, la ocultas en algo de forma que nadie sepa que esta allí.

Podríamos decir que criptografía seria como ocultar algo en una caja fuerte a la vista, y esteganografía seria como un camufle eso mismo a plena vista, pero que nadie reconozca.

Seguridad de la Información

La Seguridad de la Información reúne un conjunto de medidas preventivas y procedimientos para controlar el tratamiento de los datos que se utilizan en una empresa.
El objetivo de proteger los datos es garantizar un entorno seguro y cuidar de que los datos personales no estén expuestos a riesgos.
Comprender qué significa lleva consigo realizar un estudio de las especialidades y las características propias de cada empresa y así poder intentar garantizar su protección.

Características

La **Seguridad de la Información** debe tener tres características para considerarse segura:

1. Confidencialidad

Solo la persona que tiene permiso de ver la información puede poder verla.

2. Integridad

La información solo debe de ser accedida o cambiada por la persona que tenga permiso de ellos.

3. Disponibilidad

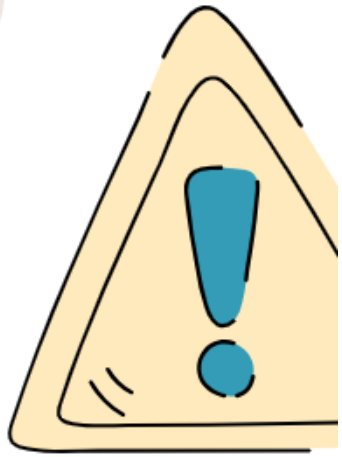
Debe de ser posible accder, en el momento que se requiere, por quien tiene permiso de accederla.

ISO 27001

Nos aportan un Sistema de Gestión de la Seguridad de la Información (SGSI), consistente en medidas orientadas a proteger la información, indistintamente del formato de la misma, contra cualquier amenaza, de forma que garanticemos en todo momento la continuidad de las actividades de la empresa.

Los Objetivos del SGSI son preservar la:

- **Confidencialidad**
- **Integridad**
- y **Disponibilidad** de la Información



CADENA DE CUSTODIA

La Cadena de Custodia es un sistema de control y registro que se aplica al material probatorio, desde el momento de su localización hasta que se presenta en juicio. El rompimiento de este sistema de control, se castiga con sanciones administrativas o sanciones penales y tiene consecuencias directas sobre el valor probatorio de los indicios hallados en la escena de los hechos.

Cualquier contaminación de las pruebas e indicios en la escena del crimen puede alterar el resultado en un proceso penal obligando al juez a condenar o absolver a la persona equivocada.

CADENA DE CUSTODIA

EVIDENCIA FISICA

Elemento material probatorio o evidencia física será entonces toda cosa u objeto que directa o indirectamente pueda aportar información acerca de uno o varios aspectos estructurales del delito o de la identidad del acusado, es decir, la cosa u objeto que por si solo tenga la cualidad demostrativa o probatoria de las circunstancias en que ocurrió un delito.

EVIDENCIA DIGITAL

La evidencia digital se define como información y datos de valor para una investigación almacenada, recibida o transmitida por un dispositivo electrónico. Esta evidencia se puede adquirir cuando se confiscan dispositivos electrónicos para su examen.


ETAPAS DE LA CADENA DE CUSTODIA
Procesamiento
Traslado
Analisis
Almacenamiento

Etapa inicial en la cual el policía de investigación, perito, servidor publico y/o el personal especializado detecta, preserva y conserva los indicios o elementos materiales probatorios digitales dentro del lugar de intervención, concluyendo con el traslado para su análisis.

PROCESAMIENTO

TRASLADO

El servidor publico que lleve a cabo el traslado tiene como encomienda, trasportar los indicios o elementos materiales probatorios digitales, debidamente embalados, sellados, etiquetados, firmados y con registro de Cadena de Custodia Digital, del lugar de intervención, hacia el lugar determinado por parte del Ministerio Público o el Órgano Jurisdiccional, dichos lugares pueden ser los servicios periciales, la bodega de indicios, las instituciones que cuenten con áreas forenses, o a algún otro lugar con condiciones de preservación o conservación, en cumplimiento a las recomendaciones de los especialistas.

ANÁLISIS

Dentro de una investigación donde se trabaja con indicios o elementos probatorios digitales, se debe considerar que ademas de recabarlos, se tiene que sumar las marcas de tiempo relacionadas con cada uno de ellos, esto incluye el momento en el que se modificaron por ultima vez o se accedió a ellos.

El personal especializado y/o perito deberá de seleccionar los archivos, datos o elementos que serán útiles para su intervención y, a su vez, excluir aquellos que no sean relevantes. Una manera de delimitar la información con la cual realizara su investigación sera excluyendo todo dato que pone en riesgo la información sensible de personas, instituciones o empresas.

ALMACENAMIENTO

Durante esta etapa se almacenan los indicios o elementos materiales probatorios digitales en alguna de las bodegas destinadas para dicho fin, previa autorización por parte del Ministerio Público, el cual designara al servidor público que sera encargado de realizar el traslado del indicio o elemento material probatorio digital, desde el lugar de intervención hasta su almacenamiento en la bodega de indicios.

ALMACENAMIENTO

Una vez que el servidor público arribe a la Bodega de indicios, el responsable de la misma recibirá los indicios o elementos materiales probatorios digitales, previa revisión de los mismos verificando que la información contenida en la Cadena de Custodia Digital coincida con el indicio o elemento material probatorio digital presentado.

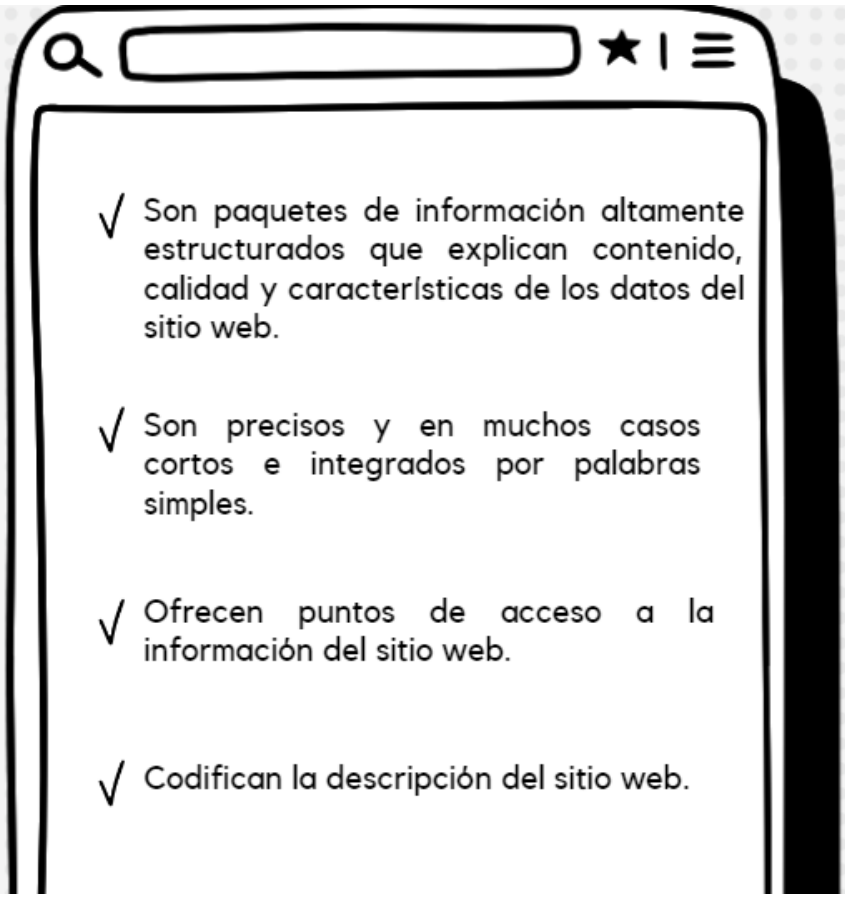
En caso de que sea necesario la salida de un indicio o elemento material probatorio, solo sera por dos razones:

- Salida temporal.
- Salida definitiva

METADATOS

Son datos sobre los datos. En otras palabras, es información que se usa para describir los datos contenidos en algo como una página web, documento o archivo. Otra forma de pensar en los metadatos es como una breve explicación o resumen de lo que son los datos.

Los metadatos se pueden crear manualmente para seleccionar y elegir lo que se incluye, pero también se pueden generar automáticamente en función de los datos.



- √ Son paquetes de información altamente estructurados que explican contenido, calidad y características de los datos del sitio web.
- √ Son precisos y en muchos casos cortos e integrados por palabras simples.
- √ Ofrecen puntos de acceso a la información del sitio web.
- √ Codifican la descripción del sitio web.

CARACTERÍSTICAS

¿PARA QUE SIRVEN LOS METADATOS?

- Los metadatos sirven para una variedad de propósitos, siendo el descubrimiento de recursos uno de los más comunes. Aquí, se puede comparar con una catalogación efectiva, que incluye identificar recursos, definirlos por criterios, reunir recursos similares y distinguir entre los que son diferentes.

- Otro uso de los metadatos es como un medio para facilitar la interoperabilidad y la integración de recursos. El uso de metadatos para describir recursos permite su comprensión tanto por humanos como por máquinas. Esto permite los niveles más efectivos de interoperabilidad, o cómo se intercambian datos entre muchos sistemas con plataformas operativas, estructuras de datos e interfaces dispares. A su vez, facilita la búsqueda de recursos en la red.

- Los metadatos también facilitan la identificación digital a través de números estándar que identifican de forma única el recurso que definen los metadatos.

- Finalmente, los metadatos son una forma importante de proteger los recursos y su accesibilidad futura. Es una preocupación crítica dada la fragilidad de la información digital y su susceptibilidad a la corrupción o alteración.

ARCHIVOS CIFRADOS Y ARCHIVOS BINARIOS

Archivos Cifrados

EL CIFRADO DE ARCHIVOS, ES UN PROCEDIMIENTO QUE VUELVE COMPLETAMENTE ILEGIBLES LOS DATOS DE UN DOCUMENTO O DE CUALQUIER ARCHIVO. DE ESTA MANERA, EL ARCHIVO SE VUELVE PRÁCTICAMENTE INSERVIBLE PARA UN USUARIO NO AUTORIZADO A LEERLO, YA QUE INCLUSO SI LO HA INTERCEPTADO O LO HA COPIADO, SI NO CUENTA CON EL PASSWORD CORRESPONDIENTE, NO PODRÁ LEERLO O VISUALIZARLO.

Archivos Binarios

LOS ARCHIVOS BINARIOS SON ARCHIVOS NORMALES QUE CONTIENEN INFORMACIÓN QUE EL SISTEMA PUEDE LEER. LOS ARCHIVOS BINARIOS PODRÍAN SER ARCHIVOS EJECUTABLES QUE INDICARAN AL SISTEMA QUE HA DE REALIZAR UN TRABAJO. LOS MANDATOS Y LOS PROGRAMAS SE ALMACENAN EN ARCHIVOS BINARIOS EJECUTABLES. LOS PROGRAMAS DE COMPILACIÓN ESPECIAL CONVIERTEN TEXTO ASCII EN CÓDIGO BINARIO.