T1. CONCEPTOS SOBRE SEGURIDAD INFORMÁTICA

1. Seguridad informática.

La Seguridad Informática es la disciplina que involucra técnicas, aplicaciones y dispositivos que aseguran la autenticidad, integridad y privacidad de la información contenida dentro de un sistema informático, así como su transmisión.

Técnicamente resulta muy difícil desarrollar un sistema informático que garantice la completa seguridad de la información, sin embargo, el avance de la tecnología ha posibilitado la disposición de mejores medidas de seguridad para evitar daños y problemas que puedan ser aprovechados por los intrusos. Dentro de la seguridad informática se pueden mencionar dos tipos:

Seguridad lógica: Conjunto de medidas de seguridad y herramientas informáticas de control de acceso a los sistemas informáticos. Software.

Seguridad física: Controles externos al ordenador, que tratan de protegerlo contra amenazas de naturaleza física como incendios, inundaciones, etc. Hardware.

2. Fiabilidad, confidencialidad, integridad y disponibilidad.

Un sistema informático seguro se caracteriza por lo siguiente:

2.1 . Fiabilidad.

La fiabilidad se define como la probabilidad de que un bien funcione adecuadamente durante un período determinado bajo condiciones operativas específicas (por ejemplo, condiciones de presión, temperatura, velocidad, tensión o forma de una onda eléctrica, nivel de vibraciones, etc.).

Un sistema fiable debe tener entre otras: la capacidad de evitar fallos, tolerancia a defectos y capacidad de recuperación (tanto prestaciones como datos afectados).

2.2 . Confidencialidad.

La confidencialidad es la cualidad que debe poseer un documento o archivo para que este solo se entienda de manera comprensible o sea leído por la persona o sistema que esté autorizado.

De esta manera se dice que un documento (o archivo o mensaje) es confidencial si y sólo si puede ser comprendido por la persona o entidad a quien va dirigida o esté autorizada. En el caso de un mensaje esto evita que exista una intercepción de este y que pueda ser leído por una persona no autorizada.

Por ejemplo: si queremos enviar un mensaje a una persona y queremos que sólo dicha persona pueda leer el mensaje, podemos cifrar este mensaje con una clave de tal forma que la persona a la cual va dirigida el mensaje sea la única que puede descifrarlo, así nos aseguramos de que nadie más pueda leer el mensaje.

2.3 . Integridad.

La integridad es la cualidad que posee un documento o archivo que no ha sido alterado y que además permite comprobar que no se ha producido manipulación alguna en el documento original. Aplicado a las bases de datos sería la correspondencia entre los datos y los hechos que refleja.

2.4 . Disponibilidad.

La disponibilidad es la característica, cualidad o condición de la información de encontrarse a disposición de quienes deben acceder a ella, ya sean personas, procesos o aplicaciones.

En el caso de los sistemas informáticos utilizados para almacenar y procesar la información, los controles de seguridad utilizados para protegerlo, y los canales de comunicación protegidos que se utilizan para acceder a ella deben estar funcionando correctamente. El objetivo de la Alta Disponibilidad de sistemas es que debe seguir estando disponible en todo momento, evitando interrupciones del servicio debido a cortes de energía, fallos de hardware, y actualizaciones del sistema.

Video: Security and Data Protection in a Google Data Center

https://www.youtube.com/watch?&v=cLory3qLoY8

3. Elementos vulnerables en el sistema informático: hardware, software y datos.

En seguridad informática, la palabra *vulnerabilidad* hace referencia a una debilidad en un sistema permitiendo a un atacante violar la confidencialidad, integridad, disponibilidad, control de acceso y consistencia del sistema o de sus datos y aplicaciones.

Las amenazas siempre están presentes, pero sin la identificación de una vulnerabilidad, no podrán causar ningún impacto.

3.1 . Hardware.

Las vulnerabilidades de hardware representan la probabilidad de que las piezas físicas del sistema fallen (ya sea por mal uso, descuido, mal diseño etc.) dejando al sistema desprotegido o inoperable.

También trata sobre las formas en que el hardware puede ser usado por personas para atacar la seguridad del sistema, por ejemplo el sabotaje de un sistema al sobrecargarlo deliberadamente con componentes de hardware que no han sido diseñados correctamente para funcionar en el sistema.

Mal diseño: es cuando los componentes de hardware del sistema no son apropiados y no cumplen los requerimientos necesarios, en otras palabras, dicha pieza del módulo no fue diseñada correctamente para trabajar en el sistema.

Errores de fabricación: es cuando las piezas de hardware son adquiridas con desperfectos de fabricación y posteriormente fallan al momento de intentar usarse. Aunque la calidad de los componentes de hardware es responsabilidad del fabricante, la organización que los adquiere es la más afectada por este tipo de amenaza.

Suministro de energía: las variaciones de voltaje dañan los dispositivos, por ello es necesario verificar que las instalaciones de suministro de energía funcionen dentro de los parámetros requeridos. Dichas instalaciones también deben proporcionar el nivel de voltaje especificado por el fabricante para no acortar su vida útil.

Desgaste: el uso constante del hardware produce un desgaste considerado, con el tiempo este desgaste reduce el funcionamiento óptimo del dispositivo hasta dejarlo inutilizable.

Descuido y mal uso: todos los componentes deben ser usados dentro de los parámetros establecidos por los fabricantes, esto incluye tiempos de uso, periodos y procedimientos adecuados de mantenimiento, así como un apropiado almacenamiento. No seguir estas prácticas provoca un desgaste mayor y la consiguiente reducción de la vida útil de los recursos.

3.2. Software.

Cada programa, sea externo o propio al sistema operativo, puede ser usado como medio para atacar a un sistema más grande; esto se puede ser debido a errores de programación, de diseño o porque simplemente no fueron considerados determinados aspectos: controles de acceso, seguridad, implantación, etc.. Estos factores hacen susceptible al sistema a las denominadas amenazas de software.

Código malicioso(malware): es cualquier software que entra en un sistema de cómputo sin ser invitado e intenta romper las reglas, esto incluye caballos de Troya, virus, gusanos informáticos, bombas lógicas y otras amenazas programadas.

Virus: este tipo de código malicioso tiene como principal característica la capacidad de duplicarse a sí mismo usando recursos del sistema infectado, propagando su infección rápidamente dentro de un mismo sistema anfitrión.

Troyanos: este tipo de código se presenta escondido en otros programas de aplicación aparentemente inofensivos para posteriormente activarse de manera discreta cumpliendo su propósito malicioso. La mejor forma de expandir un software malicioso es compartir software popular que una víctima potencial desee instalarse.

Gusanos: es muy similar a los virus con la diferencia fundamental que éstos aprovechan más los recursos de los sistemas infectados, atacando diferentes programas y posteriormente replicándose para redistribuirse utilizando la red.

Errores de programación y diseño: Los errores de programación y fallas generales que puede tener un software de aplicación también representan una amenaza.

Amenazas informáticas. Malware:
https://www.youtube.com/watch?v=BMrtJGxgzFY

3.3. Datos

Las redes pueden llegar a ser lugares muy vulnerables para los datos al tratarse de una serie de equipos conectados entre sí compartiendo recursos. Es posible atacar a toda la red para obtener la información que se comparte en la misma penetrando primero en uno de los equipos vulnerables y posteriormente expandiéndose al resto.

En una red la prioridad es la transmisión de la información, así que todas las vulnerabilidades están relacionadas directamente con la posible intercepción de la información por personas no autorizadas y con fallas en la disponibilidad del servicio, así como la pérdida de privacidad o robo de información.

La información (datos) es el elemento más sensible de todo el sistema informático, por lo que conlleva el riesgo de accesos no autorizados, que utilicen esa información o que la modifiquen, lo que puede ser mucho más grave.

3.4. Análisis de las principales vulnerabilidades del sistema informático.

Existen diferentes vulnerabilidades que, dependiendo de sus características, las podemos clasificar e identificar en los siguientes tipos:

De configuración

Una vulnerabilidad se produce cuando la configuración por defecto del sistema es insegura, por ejemplo una aplicación recién instalada que cuenta de base con usuarios por defecto (un usuario por defecto sería como dejar una puerta abierta).

Validación de entrada

Este tipo de vulnerabilidad se produce cuando la entrada que procesa un sistema no es comprobada adecuadamente de forma que una vulnerabilidad puede ser aprovechada por una cierta secuencia de entrada (p. ej., una fecha mal introducida puede abortar una aplicación)

Salto de directorio

Ésta aprovecha la falta de seguridad de un servicio de red para desplazarse por el árbol de directorios hasta la raíz del volumen del sistema. El atacante podrá entonces desplazarse a través de las carpetas de archivos del sistema operativo para ejecutar una utilidad de forma remota (p.ej., acortar la url para probar).

Secuencias de comandos en sitios cruzados (XSS)

Este tipo de vulnerabilidad abarca cualquier ataque que permita ejecutar código de "scripting", como VBScript o javascript, en el contexto de otro dominio. Estos errores se pueden encontrar en cualquier aplicación HTML, no se limita a sitios web, ya que puede haber aplicaciones locales vulnerables a XSS, o incluso el navegador en sí. El problema está en que normalmente no se validan correctamente los datos de entrada que son usados en cierta aplicación.

Inyección de comandos en el sistema operativo

Hablamos de este tipo de vulnerabilidad para referirnos a la capacidad de un usuario, que controla la entrada de comandos (bien a través de un terminal de Unix/Linux o del interfaz de comando de Windows), para ejecutar instrucciones que puedan comprometer la integridad del sistema (equipo que permita la posibilidad de abrir la consola).

Inyección SQL

Inyección SQL es una vulnerabilidad informática en el nivel de base de datos de una aplicación. El origen es el filtrado incorrecto de las variables utilizadas en las partes del programa con código SQL.

Una inyección de código SQL sucede cuando se inserta un trozo de código SQL dentro de otro código SQL con el fin de modificar su comportamiento, haciendo que ejecute el código malicioso en la base de datos.

El hecho de que un servidor pueda verse afectado por las inyecciones SQL se debe a la falta de medidas de seguridad por parte de sus diseñadores/programadores, especialmente por una mala filtración de las entradas (por formularios, cookies o parámetros).

Video: Inyección SQL

https://www.youtube.com/watch?v=ciNHn38EyRc

Formato de cadena

Nos referimos a este tipo de vulnerabilidad cuando se produce a través de cadenas de formato controladas externamente, como el tipo de funciones "printf" en el lenguaje "C" que pueden conducir a provocar desbordamientos de búfer o problemas en la representación de los datos.

Revelación/Filtrado de información

Un filtrado o escape de información puede ser intencionado o no intencionado. En este aspecto los atacantes pueden aprovechar esta vulnerabilidad para descubrir el directorio de instalación de una aplicación, la visualización de mensajes privados, etc. La severidad de esta vulnerabilidad depende del tipo de información que se puede filtrar (p.ej., una aplicación que muestre al usuario dónde se encuentra instalada otra aplicación).

Condición de carrera

Una condición de carrera se produce cuando varios procesos tratan de acceder y manipular los mismos datos simultáneamente. Los resultados de la ejecución dependerán del orden particular en que el acceso se lleva a cabo. Una condición de carrera puede ser interesante para un atacante cuando ésta puede ser utilizada para obtener acceso al sistema.

Desbordamiento de buffer

Un búfer es una ubicación de la memoria en una computadora o en un instrumento digital reservada para el almacenamiento temporal de información digital, mientras que está esperando ser procesada.

Errores de programación en la gestión del buffer pueden provocar que se intente almacenar más información de la que soporta, produciendo un overflow.

Errores numéricos

El desbordamiento de entero (integer overflow): un desbordamiento del número entero ocurre cuando una operación aritmética procura crear un valor numérico que sea más grande del que se puede representar dentro del espacio de almacenaje disponible. Por ejemplo, la adición de 1 al valor más grande que puede ser representado constituye un desbordamiento del número entero.

Error en la gestión de recursos

El sistema o software que adolece de este tipo de vulnerabilidad permite al atacante provocar un consumo excesivo en los recursos del sistema (disco, memoria y CPU). Esto puede causar que el sistema deje de responder y provocar denegaciones de servicio.

Falsificación de petición en sitios cruzados (CSRF)

Este tipo de vulnerabilidad afecta a las aplicaciones web con una estructura de invocación predecible. El agresor puede colocar en la página cualquier código, el cual posteriormente puede servir para la ejecución de operaciones no planificadas por el creador del sitio web, por ejemplo, capturar archivos cookies sin que el usuario se percate.

El tipo de ataque CSRF más popular se basa en el uso del marcador HTML <img>, el cual sirve para la visualización de gráficos. En vez del marcador con la URL del archivo gráfico, el agresor pone un tag que lleva a un código JavaScript que es ejecutado en el navegador de la víctima (todo se basa en la posibilidad de que el atacante pueda ingresar código HTML en la web que va a visitar la víctima).

Artículo

https://www.elconfidencial.com/tecnologia/2019-10-09/whatsapp-fallo-seguridad-incibe-app-620_2275762/

4. Medidas de Protección

Podemos encontrar dos tipos de técnicas de seguridad para proteger de nuestro sistema informático:

- Seguridad activa
- Seguridad pasiva

La seguridad activa y pasiva son muy importantes ya que con ellas podemos asegurar que nuestro sistema no sufra ataques y con ello poder asegurar la disponibilidad, fiabilidad, confidencialidad e integridad de nuestra información.

4.1 Medidas activas

La seguridad activa se encarga de evitar que los sistemas informáticos sufran algún daño, y por lo general implican la supervisión del administrador del sistema. Consiste en realizar, entre otras, las siguientes acciones:

- Emplear contraseñas seguras: Para que una contraseña sea segura, debe contener más de ocho caracteres, mezclando letras mayúsculas y minúsculas, números y otros caracteres. No se deben emplear como contraseñas la fecha de nacimiento o el nombre de la mascota.

- Cifrar los datos importantes: O lo que es lo mismo, cifrar los datos para que sólo puedan ser leídos si se conoce la clave de cifrado. La encriptación se hace con programas especiales.

- Instalar y configurar software de seguridad: como antivirus, antiespías, cortafuegos.

etc.

4.2 Medidas pasivas

El objetivo de las técnicas de seguridad pasiva es minimizar los efectos o desastres causados por un accidente, un usuario o un malware a los sistemas informáticos. ejemplos de prácticas de seguridad pasiva recomendables podrían ser:

- El uso de hardware adecuado frente a accidentes y averías (refrigeración del sistema, conexiones eléctricas adecuadas, dispositivos SAI...)

- La realización de copias de seguridad de los datos y del sistema operativo en más de un soporte y en distintas ubicaciones físicas.

- Creación de respaldos de la información en discos y/o servidores externos, particiones lógicas en el disco duro para poder almacenar archivos y copias de seguridad(backup) en una unidad distinta a la del sistema operativo., etc.

5. Seguridad física y ambiental.

La seguridad física es uno de los aspectos más olvidados a la hora del diseño de un sistema informático. Si bien algunos de los aspectos de seguridad física básicos se prevén, otros, como la detección de un atacante interno a la empresa que intenta acceder físicamente a una sala de cómputo de la misma, no.

Esto puede derivar en que para un atacante sea más fácil lograr tomar y copiar una cinta de backup de la sala de ordenadores, que intentar acceder vía lógica a la misma. Así, la Seguridad Física consiste en la "aplicación de barreras físicas y procedimientos de control, como medidas de prevención y contramedidas ante amenazas al sistema informático

5.1. Amenazas Físicas.

Es muy importante ser consciente que por más que nuestra empresa sea la más segura desde el punto de vista de ataques externos (hackers, virus, ataques de DoS, etc.); la seguridad de la misma será nula si no se ha previsto como combatir un incendio o cualquier otro tipo de desastre natural y no tener presente políticas claras de recuperación.

Las principales amenazas que se prevén en la seguridad física son:

1. Desastres naturales, incendios accidentales, tormentas e inundaciones.

2. Amenazas ocasionadas por el hombre.

3. Disturbios, sabotajes internos y externos deliberados.

5.2. Protección ante las amenazas físicas

5.2.1. Ubicación y protección física de los equipos y servidores.

Para minimizar el impacto de un posible problema físico tendremos que imponer condiciones de seguridad para los equipos y sistemas de la organización. Por otra lado, para que los equipos informáticos funcionen correctamente deben de encontrarse bajo ciertas condiciones. Los servidores dado que su funcionamiento ha de ser continuo deben de situarse en un lugar que cumpla las condiciones óptimas para el funcionamiento de estos, además debe estar bajo llave en un armario rack y estar en un lugar con acceso restringido al cual sólo acceda personal autorizado.

Para asegurar los sistemas y equipos que han de mantenerse siempre operativos se crean lugares que se conocen como "*Centro de Procesamiento de Datos*" o por sus siglas **CPD**. En estos CPD se deben de cumplir una serie de requisitos para protegerlos de posibles desastres:

- No debe haber conducciones cercanas de agua, gas o calefacción, para evitar fugas, humedades, etc.

- Deben contar con un doble suelo para evitar cortocircuitos en caso de inundación

- Se debe evitar el polvo y la electricidad estática.

- La temperatura debe ser continua las 24 horas los 365 días al año.

- Se debe evitar el uso de techos falsos.

- Deben disponer de sistemas de alimentación ininterrumpida.

- En zonas de riesgo sísmico deben contar con la protección adecuada.

- Se deben mantener bajo llave, las cuales serán asignadas solo al personal autorizado.

5.2.2 Protección ante fallos de cableado

Con mayor frecuencia de la deseable, los cables de red o las interfaces de red de los dispositivos pueden sufrir daños y deteriorar la calidad de la transmisión hasta el punto de imposibilitarla por completo. Todo administrador de sistemas debe contar con latiguillos, conectores, bobinas y herramientas específicas para realizar reparaciones de este tipo. Sin embargo, centrándonos en el cableado interno del CPD, puede ser inaceptable el tiempo de parada (downtime) que sufra el sistema en caso del fallo de un cable. Por ello es habitual utilizar métodos de combinación de dos o más cables físicos redundantes que, a todos los efectos, se comportan como un único cable virtual.

Esta tecnología recibe diversos nombres, según el fabricante de hardware: link aggregation, IEEE 802.3x, LAG (Link Aggregation Group). NIC bonding, port trunking. NIC teaming, etc. El concepto es utilizado no solo con cableado Ethernet, sino en enlaces wifi haciendo uso de múltiples bandas de frecuencia.

5.2.3. Protección ante humedades e inundaciones

Casi cualquier medio (máquinas, cintas, routers ...) que entre en contacto con el agua queda automáticamente inutilizado, bien por el propio líquido o bien por los cortocircuitos que genera en los sistemas electrónicos. Contra ellas podemos instalar **sistemas de detección que apaguen los sistemas si se detecta agua** y corten la corriente en cuanto estén apagados.

Respecto a la humedad, un CPD debe mantenerse en un rango de humedad entre 45-55%. Bajar del 30% o subir de 70% puede resultar peligroso para los equipos.

5.2.4. Protección ante incendios y altas temperaturas

El fuego y los humos en general provendrán del incendio de equipos por sobrecarga eléctrica. Contra ellos emplearemos **sistemas de extinción**, que aunque pueden dañar los equipos que apaguemos aunque actualmente son más o menos inocuos), nos evitarán males mayores.

Además del fuego, también el humo es perjudicial para los equipos (incluso el del tabaco), al ser un abrasivo que ataca a todos los componentes, por lo que es recomendable mantenerlo lo más alejado posible de los equipos.

Las temperaturas extremas, ya sea un calor excesivo o un frío intenso, perjudican gravemente a todos los equipos. En general es recomendable que los equipos operen **entre 10 y 32 grados Celsius**.

Para controlar la temperatura emplearemos **aparatos de aire acondicionado**.

5.2.5. Protección ante terremotos

Los terremotos son el desastre natural menos probable en la mayoría de organismos ubicados en España, por lo que no se harán grandes inversiones en prevenirlos, aunque hay varias cosas que se pueden hacer sin un desembolso elevado y que son útiles para prevenir problemas causados por pequeñas vibraciones:

- No situar equipos en sitios altos para evitar caídas.
- No colocar elementos móviles sobre los equipos para evitar que caigan sobre ellos.
- Separar los equipos de las ventanas para evitar que caigan por ellas o qué objetos lanzados desde el exterior los dañen.
- Utilizar fijaciones para elementos críticos.
- Colocar los equipos sobre plataformas de goma para que esta absorba las vibraciones.

5.2.6. Protección ante problemas de suministro eléctrico

Quizás los problemas derivados del entorno de trabajo más frecuentes son los relacionados con el sistema eléctrico que alimenta nuestros equipos; cortocircuitos, picos de tensión, cortes de flujo, etc.

Para corregir los problemas con las subidas de tensión podremos instalar **tomas de tierra o filtros reguladores de tensión**.

El ruido eléctrico suele ser generado por motores o por maquinaria pesada, pero también puede serlo por otros ordenadores o por multitud de aparatos, y se transmite a través del espacio o de líneas eléctricas cercanas a nuestra instalación.

Para prevenir los problemas que puede causar el ruido eléctrico lo más barato es intentar no situar el hardware cerca de los elementos que pueden causar el ruido. En caso de que fuese necesario hacerlo, siempre podemos **instalar filtros o apantallar las cajas** de los equipos.

Para los cortes podemos emplear Sistemas de Alimentación Ininterrumpida (SAI), que además de proteger ante cortes mantienen el flujo de corriente constante, evitando las subidas y bajadas de tensión.

Por último indicar que además de los problemas del sistema eléctrico también debemos preocuparnos de la corriente estática, que puede dañar los equipos. Para evitar problemas se pueden emplear sprays antiestáticos o ionizadores y tener cuidado de no tocar componentes metálicos, evitar que el ambiente esté excesivamente seco, etc.

Sistemas de alimentación ininterrumpida.

Un sistema de alimentación ininterrumpida, SAI (en inglés Uninterruptible Power Supply, UPS), es un dispositivo que gracias a sus baterías, puede proporcionar energía eléctrica tras un

apagón a todos los dispositivos que tenga conectados. Otra de las funciones de los UPS es la de mejorar la calidad de la energía eléctrica que llega a las cargas, filtrando subidas y bajadas de tensión y eliminando armónicos de la red en el caso de usar corriente alterna.

Los UPS dan energía eléctrica a equipos llamados cargas críticas, como pueden ser aparatos médicos, industriales o informáticos, incluso se utilizan en servidores y ordenadores de casi cualquier oficina o empresa, que requieren tener siempre alimentación y que ésta sea de calidad, debido a la necesidad de estar en todo momento operativos y sin fallos (picos o caídas de tensión).

Los cortes en el suministro eléctrico, pueden producir en nuestro sistema informático:

- Destrucción de la información.
- Daño en las infraestructuras (ordenadores, servidores...).
- Estrés y desmotivación de las personas que lo utilizan.
- Afecta a la productividad.
- Genera pérdidas.

Un SAI está formado por una o varias baterías y un convertidor de corriente que transforma la energía continua en alterna, y la eleva hasta obtener una tensión de 220V. Los SAI disponen de unos conectores que se enchufan a los equipos a alimentar.

Los SAI normalmente tienen una autonomía de unos 10 minutos, aunque existen modelos de gran autonomía de servicios. Esta autonomía está directamente relacionada con el consumo que tengan los dispositivos conectados al SAI.

A la hora de elegir un SAI debemos tener en cuenta la potencia que necesitamos para alimentar los dispositivos que queremos proteger, en función de eso compraremos un SAI de una potencia algo superior a la que necesitamos.

Fallos comunes en el suministro de energía eléctrica

El papel del UPS es suministrar potencia eléctrica en ocasiones de fallo de suministro, en un intervalo de tiempo "corto". (Si es un fallo en el suministro de la red, hasta que comiencen a funcionar los sistemas aislados de emergencia). Sin embargo, muchos sistemas de alimentación ininterrumpida son capaces de **corregir** otros fallos de suministro:

- Corte de energía: pérdida total de tensión de entrada.
- Sobretensión: tiene lugar cuando la tensión supera el 110% del valor nominal. Caída de tensión: cuando la tensión es inferior al 85-80% de la nominal.
- Picos de tensión.
- Ruido eléctrico.
- Inestabilidad en la frecuencia.
- Distorsión armónica, cuando la onda sinusoidal suministrada no tiene esa forma.

Tipos de SAI.

Podemos distinguir tres tipos de SAI según su tipo de alimentación:

- **Off-line**: la alimentación viene de la red eléctrica y en caso de fallo de suministro el dispositivo empieza a generar su propia alimentación. Debido a que no son activos, hay un pequeño tiempo en el que no hay suministro eléctrico (entre 10 y 15 milisegundos). Típicamente generan una forma de onda que no es sinusoidal, por lo que no son adecuados para proteger dispositivos delicados o sensibles a la forma de onda de su alimentación. Su uso más común es en la protección de dispositivos domésticos como ordenadores, monitores, televisores, etc.

- **In-line**: también conocido como de "línea interactiva". Es similar al off-line, pero dispone de filtros activos que estabilizan la tensión de entrada. Sólo en caso de fallo de tensión o anomalía grave empiezan a generar su propia alimentación. Al igual que los SAI de tipo off-line tienen un pequeño tiempo de conmutación en el que no hay suministro eléctrico (entre 2 y 6 milisegundos). Típicamente generan una forma de onda pseudo-sinusoidal o sinusoidal de mayor calidad que los SAI off-line. Su uso más común es en la protección de dispositivos en pequeños comercios o empresas, tales como ordenadores, monitores, servidores, cámaras de seguridad y videograbadores, etc.

- **On-line**: el más sofisticado de todos. El dispositivo genera una alimentación limpia con una onda sinusoidal perfecta en todo momento a partir de sus baterías. Para evitar que se descarguen las cargas al mismo tiempo que genera la alimentación. Por tanto, en caso de fallo o anomalía en el suministro los dispositivos protegidos no se ven afectados en ningún momento porque no hay un tiempo de conmutación. Su principal inconveniente es que las baterías están constantemente trabajando, por lo que deben sustituirse con más frecuencia. Su uso más común es en la protección de dispositivos delicados o de mucho valor en empresas, tales como servidores, electrónica de red, ordenadores de monitorización, videograbadores y cámaras de seguridad, etc.

A la hora de elegir un SAI es necesario fijarse en dos características clave:

- Potencia máxima que es capaz de proporcionar (en el conjunto de sus tomas de salida). Se mide en Watios o Voltios Amperios. Debemos adquirir uno cuya potencia máxima iguale la suma de las potencias de consumo de los equipos que van a ser conectados (más un margen de tolerancia del 15-20%)

1 watio = 1 voltio amperio x F.P. (factor de potencia)

(El factor de potencia suele rondar 0,8 o 0,9 en todos los SAI profesionales y 0,6 en los básicos)

Por ejemplo, para un SAI cuya potencia en VA sea de 500 tendremos una potencia máxima en W de 300 o 350 vatios respectivamente, en un SAI para el hogar.

- Tiempo de autonomía (runtime). Dependerá del nivel de carga de las baterías, del número de éstas, y de la potencia de suministro aportada. Existen fórmulas complejas para calcular el

tiempo de autonomía de un SAI, según la potencia a suministrar, aunque los fabricantes suelen suministrar esa información.

Prueba a elegir un SAI para el hogar y uno para un CPD.

https://www.apc.com/shop/es/es/tools/ups_selector

5.2.7. Protección ante accesos no autorizados y robos.

Las computadoras son posesiones valiosas de las empresas y están expuestas, de la misma forma que lo están las piezas de stock e incluso el dinero. La información importante o confidencial puede ser fácilmente copiada. Muchas empresas invierten millones de dólares en programas y archivos de información, a los que dan menor protección que la que otorgan a una máquina de escribir o una calculadora. El software, es una propiedad muy fácilmente sustraíble y las cintas y discos son fácilmente copiados sin dejar ningún rastro.

El control de acceso no sólo requiere la capacidad de identificación, sino también asociarla a la apertura o cerramiento de puertas, permitir o negar acceso basado en restricciones de tiempo, área o sector dentro de una empresa o institución. Algunos de los controles y medidas antirrobo que podemos realizar son:

- Utilización de Guardias
- Utilización de Detectores de Metales
- Verificación Automática de Firmas (VAF)
- Seguridad con Animales
- Uso de candados antirrobo
- Sistemas de alarma y videovigilancia...

Sistemas de control de acceso:

- Llaves tradicionales
- Contraseñas: con su correspondiente política de contraseñas.
- Tarjetas magnéticas.
- Sistemas biométricos.
- Sistemas de control de temperatura.

Sistemas Biométricos.

La biometría *es el estudio de métodos automáticos para el reconocimiento único de humanos basados en uno o más rasgos conductuales o físicos intrínsecos*. Es decir, la biometría es un sistema que fundamenta sus decisiones de reconocimiento mediante una característica personal que puede ser reconocida o verificada de manera automatizada. El término se deriva de las palabras griegas "bios" de vida y "metron" de medida.

La "biometría informática" es la aplicación de técnicas matemáticas y estadísticas sobre los rasgos físicos o de conducta de un individuo, para “verificar” identidades o para “identificar” individuos.

En las tecnologías de la información (TI), la autentificación biométrica se refiere a las tecnologías para medir y analizar las características físicas y del comportamiento humanas con propósito de autentificación.

Las huellas dactilares, las retinas, el iris, los patrones faciales, de venas de la mano o la geometría de la palma de la mano, representan ejemplos de características físicas (estáticas), mientras que entre los ejemplos de características del comportamiento se incluye la firma, el paso y el tecleo(dinámicas). La voz se considera una mezcla de características físicas y del comportamiento, pero todos los rasgos biométricos comparten aspectos físicos y del comportamiento.

Biometrics vs passwords

https://www.youtube.com/watch?v=ZPG3XQhZVII

6. Análisis Forense en Sistemas Informáticos.

La auditoría de seguridad informática

Muchas compañías contratan a empresas especializadas en seguridad informática, llamadas **auditoras de seguridad informática** (o peritos en seguridad informática si se trata de trabajadores autónomos), para que evalúen el sistema informático mediante técnicas de *pentesting* (“test de penetración”, consiste en atacar un sistema informático para identificar fallos, vulnerabilidades y demás errores de seguridad existentes, para así poder prevenir los ataques externos), encuentren vulnerabilidades y aconsejen medidas de seguridad a aplicar. Para evaluar las principales amenazas cuentan con **hackers éticos**, los cuales intentan penetrar en el sistema como lo haría cualquier hacker pero bajo un contrato de confidencialidad y de no agresión. Estas auditorías reciben el nombre de **análisis forense de sistemas informáticos** si se aplican después de la vulneración del sistema, y pueden tener validez como pruebas en un proceso judicial.

Una auditoría de seguridad supone una *fase inicial en el proceso de implantación de medidas de seguridad activa*: una vez realizada y presentado el consiguiente informe, la empresa decidirá cuáles de las medidas recomendadas desea (y se puede permitir) implantar.

El contenido mínimo de un informe de auditoría de seguridad está definido en la norma ISO 19011, “Directrices para la auditoría de Sistemas de Gestión", y debería ser:

1. **Objetivo** de la auditoría. Si se trata de una auditoría periódica o una auditoría de seguimiento de acciones correctivas.

2. **Alcance** de la auditoría, incluyendo procesos, departamentos, delegaciones, etc., así como periodo de tiempo a evaluar, si procede.

3. **Equipo auditor**, con nombres, apellidos y cargo que ocupa en el equipo.

4. **Fechas y lugares** de la auditoría. Es importante detallar y poder demostrar el marco temporal en que se realizan las auditorías

5. **Criterios** de la auditoría. ¿Qué procesos se han auditado y siguiendo qué estándar?

6. **Resultados** de la auditoría. ¿Cuales son los resultados de las evidencias que se encontraron? Algunas organizaciones distinguen entre **principales hallazgos** (donde hay un fallo sistemático) y **hallazgos menores** (como uno o varios errores que se cometieron pero que no eran genéricos), pero esto no es necesariamente así. Otras organizaciones incluyen también los resultados positivos y mejores prácticas que pueden ser compartidos con toda la organización. Es importante incluir los elementos probatorios de los hallazgos.

7. **Conclusiones** de la auditoría. ¿Cuál es el resumen de los resultados de la auditoría? ¿Había demasiados hallazgos para determinar si el proceso se llevó a cabo correctamente?

La UNE (Asociación Española de Normalización, www.une.org) también elabora normas equivalentes a las ISO orientadas al territorio nacional, muchas veces basadas en normas ISO.

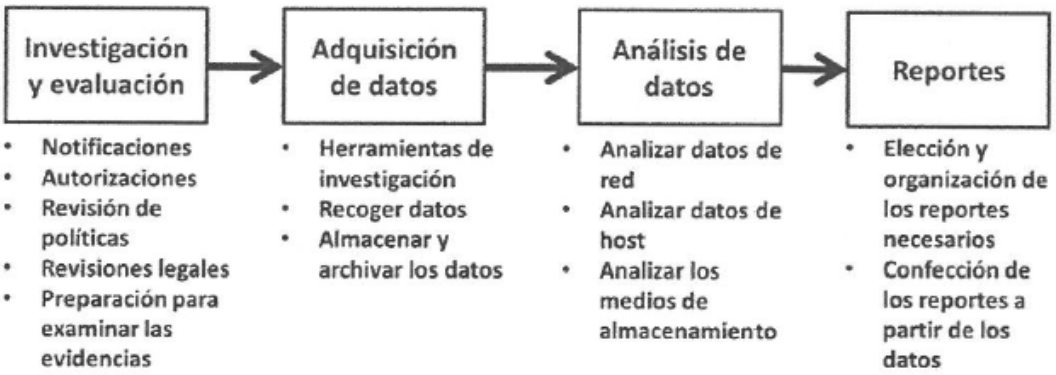
Por ejemplo, la **UNE 197001:2019**, "Criterios generales para la elaboración de informes y dictámenes periciales", establece un informe pericial con unos apartados muy similares a los arriba descritos. Para la recopilación de pruebas que puedan tener validez en un proceso judicial existen las normas:

UNE 71505:2013, "Sistema de Gestión de Evidencias Electrónicas (SGEE)".

UNE 71506:2013, "Metodología para el análisis forense de las evidencias electrónicas".

6.1. Fases del análisis forense

El procedimiento utilizado para llevar a cabo un análisis forense es el siguiente:



1. **Investigación o estudio previo**. En esta fase se realiza un estudio inicial mediante entrevistas y documentación entregada por el cliente con el objetivo de tener una idea inicial del problema que nos vamos a encontrar
2. **Adquisición de datos**. Se realiza una obtención de los datos e informaciones esenciales para la investigación. Se duplican o clonan los dispositivos implicados para un posterior análisis, y

se establece una férrea cadena de custodia para garantizar la integridad de las pruebas. Las fuentes de información que se utilizan, entre otras, son:

- Ficheros log del cortafuegos.
- Ficheros log del sistema de control de incidencias, si existe.
- Ficheros log del sistema operativo, servidor, equipos, etc.
- Ficheros log proporcionados por el proveedor de internet (IPS).
- Correos electrónicos.
- Historial del navegador.
- Entrevistas con el administrador del sistema o con los usuarios.
- Listados de vulnerabilidades.

3. **Análisis de datos e investigación**. Se realiza un estudio con los datos adquiridos en la fase anterior.
4. **Realización del informe**. En esta fase se elabora el informe que será remitido a la dirección de la empresa. Como hemos dicho, este informe podrá ser utilizado para acompañar la denuncia que se pueda realizar a la autoridad competente. Debe procurar ser redactado con un lenguaje entendible y sin tecnicismos, añadiendo un glosario con la definición de aquellos que resulte inevitable utilizar.

Las vulnerabilidades utilizadas por los atacantes, si están identificadas, aparecen en listados públicos como el proporcionado por Security Focus (www.securityfocus.com), identificados por un código CVE (Common Vulnerabilities and Exposures)

6.2. Herramientas para el análisis forense

Las herramientas utilizadas en análisis forense de sistemas informáticos abarcan multitud de categorías, como pueden ser clonación de unidades de almacenamiento, análisis de dispositivos de almacenamiento, análisis de ficheros log, análisis de conexiones de red, etc. Las más conocidas son las siguientes:

- Digital Forensics Framework (DFF), herramienta de código abierto y con licencia GPL. https://tools.kali.org/forensics/dff.
- Open Computer Forensics Architecture, (OCFA), creado originalmente por la Agencia Nacional de Policía holandesa. http://ocfa.sourceforge.net.
- Computer Forensics Linux Live Distro, también conocida como Computer Aided Investigative Environment, distribución Linux basada en Ubuntu creada expresamente para análisis forense. https://www.caine-live.net.
- SANS Investigative Forensic Toolkit. http://sans.org/community/downloads
- The Sleuth Kit, https://www.sleuthkit.org

- Volatility Foundation, https://www.volatilityfoundation.org.
- OpenSCAP, https://www.open-scap.org.

No debemos confundir las herramientas de pentesting con las de análisis forense. Las primeras están orientadas a la penetración en sistemas, mientras que las segundas pretenden recabar información de un sistema previamente infiltrado. Algunas distribuciones de pentesting, sin embargo incluyen también herramientas forenses, como es el caso de Kali Linux con su arranque en modo forense (sin montar ninguna unidad, ni siquiera la partición swap) y su Digital Forensic Framework.

6.3. Registro log centralizado

Por las mismas razones por las que es conveniente sincronizar la hora en toda la red, puede ser conveniente mantener un registro log centralizado, al cual todos los servicios y dispositivos envíen sus eventos, en lugar de que cada uno de ellos los almacene en ficheros locales. Esto se consigue mediante rsyslog (término que hace referencia tanto al servidor, como al protocolo utilizado para enviar los eventos al registro central de dicho servidor) en sistemas Unix/Linux, o con la redirección de eventos en sistemas WIndows.

Entornos Linux

El **protocolo syslog** está implementado en el mundo Linux con el paquete rsyslog, que viene instalado por defecto en todos los sistemas. El daemon rsyslogd es el encargado de recibir eventos de todas las aplicaciones del sistema, principalmente del kernel, y los va almacenando en ficheros log, pero puede ser configurado para, además, recibir eventos de equipos remotos (dicha configuración se encuentra en /etc/rsyslog.conf), así como para almacenar la información en múltiples formatos, incluyendo bases de datos MySQL o PostgreSQL. Una de las formas de almacenar la información es redirigirla (forward) a otro equipo, que es, precisamente, la forma de configurar un equipo para enviar información a un servidor centralizado. Dicho de otro modo, el mismo daemon rsyslogd es utilizado en clientes y servidores.

Dado que la mayoría de los routers, NAS y dispositivos de red en general están, internamente, basados en Linux, suelen incluir la capacidad de enviar eventos a un servidor Syslog o incluso de funcionar como servidor Syslog para recibir los eventos del resto de la red.

Entornos Windows

La **redirección de eventos** (WEF) funciona exactamente de la misma forma que syslog: un servidor central, denominado recopilador, es el que recibe los eventos del resto de equipos, llamados *fuentes*. Para ello hace uso del protocolo WinRM de intercambio de información entre equipos, proporcionado por el servicio "Administración remota de Windows (WS-Management)", que deberá ser habilitado en todos los equipos del sistema. El equipo recopilador, además, deberá habilitar el servicio “Recopilador de eventos de Windows".

Los reenvíos se configuran en lo que se denomina suscripciones de eventos, dentro del visor de eventos del sistema recopilador.

MAPA CONCEPTUAL DE LA UNIDAD