Seguridad y alta disponibilidad

En este libro se abarcara la asignatura de seguridad y alta disponibilidad del grado superior de informática.

Escrito por: Nicolás Madrid Gallego

Nicolás Madrid Gallego
IES GREGORIO PRIETO
Adopción de pautas de seguridad

ÍNDICE

UD1: "Adopción de pautas de seguridad informática".

1.-Fiabilidad, confidencialidad, integridad y disponibilidad.

Conceptos de Seguridad

Los conceptos confidencialidad, integridad o disponibilidad son muy comunes en el ámbito de la seguridad y aparecen como fundamentales en toda arquitectura de seguridad de la información, ya sea en el ámbito de la protección de datos, normativa vigente relacionada con la protección de datos de carácter personal, como de códigos de buenas prácticas o recomendaciones sobre gestión de la seguridad de la información y de prestigiosas certificaciones internacionales, éstas últimas, relacionadas con la auditoría de los sistemas de información. Suele referirse al grupo de estas características como **CIDAN**, nombre sacado de la inicial de cada característica.

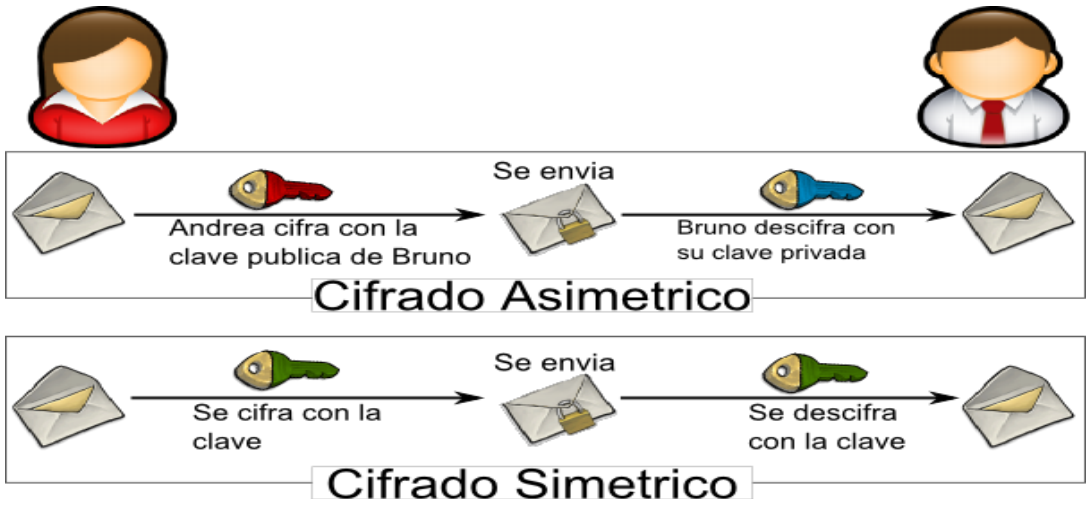
Por estos motivos es importante tener una idea clara de estos conceptos.

Confidencialidad

Se trata de 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 este autorizado.

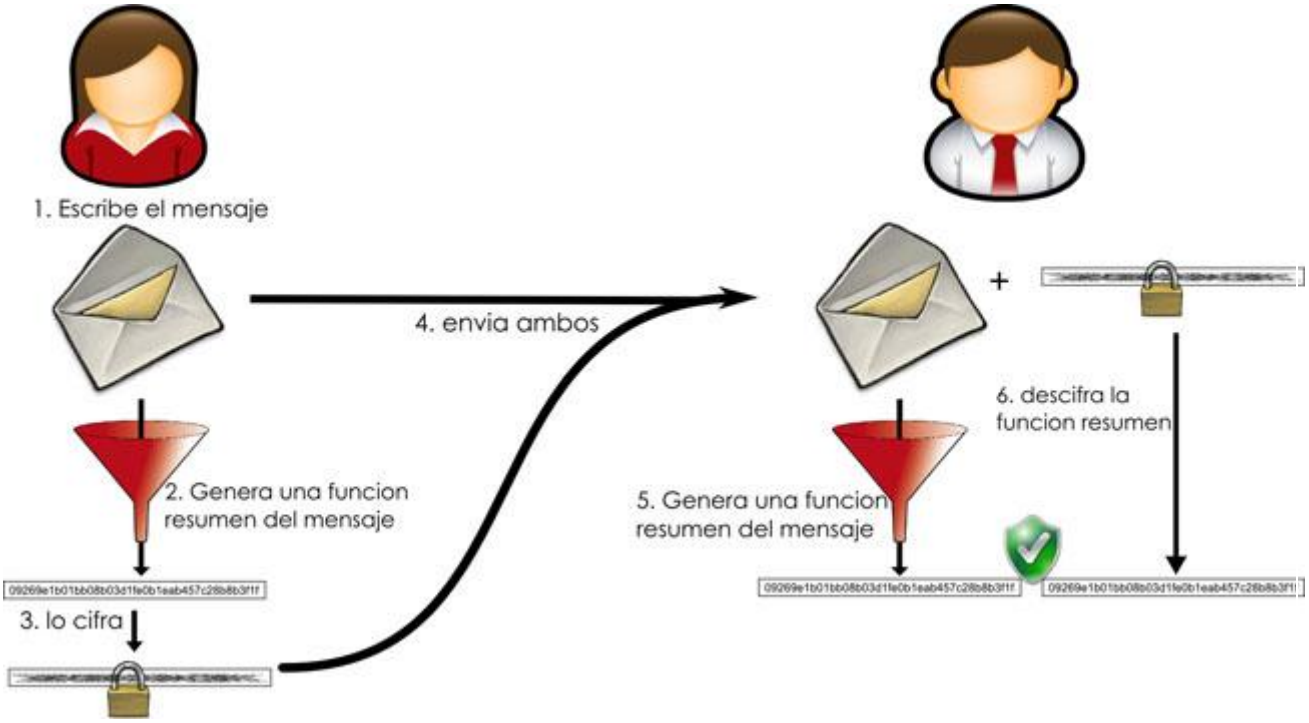
De esta manera se dice que un documento (o archivo o mensaje) es confidencial si y solo si puede ser comprendido por la persona o entidad a quien va dirigida o esté autorizada. En el caso de un mensaje esto evita que exista una intercepción de este y que pueda ser leído por una persona no autorizada.

Por ejemplo, si Andrea quiere enviar un mensaje a Bruno y que solo pueda leerlo Bruno, Andrea cifra el mensaje con una clave (simétrica o asimétrica), de tal modo que solo Bruno sepa la manera de descifrarlo, así ambos usuarios están seguros que solo ellos van a poder leer el mensaje.



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 seria la correspondencia entre los datos y los hechos que refleja.



Teniendo como muestra el ejemplo anterior. Finalmente Bruno compara ambas funciones resumen, que se trata de una función que produce un valor alfanumérico que identifica cualquier cambio que se produzca en el mensaje, y si éstas funciones son iguales, quiere decir que no ha existido manipulación del mensaje

Autenticación

La autenticación es la situación en la cual se puede verificar que un documento ha sido elaborado (o pertenece) a quien el documento dice.

Aplicado a la verificación de la identidad de un usuario, la autenticación se produce cuando el usuario puede aportar algún modo de que se pueda verificar que dicha persona es quien dice ser, a partir de ese momento se considera un usuario autorizado.

Otra manera de definirlo seria, la capacidad de determinar si una determinada lista de personas ha establecido su reconocimiento sobre el contenido de un mensaje.

Disponibilidad

Se trata de la capacidad de un servicio, de unos datos o de un sistema, a ser accesible y utilizable por los usuarios (o procesos) autorizados cuando estos lo requieran.

No repudio

El no repudio o irrenunciabilidad es un servicio de seguridad estrechamente relacionado con la autenticación y que permite probar la participación de las partes en una comunicación. La diferencia esencial con la autenticación es que la primera se produce entre las partes que establecen la comunicación y el servicio de no repudio se produce frente a un tercero, de este modo, existirán dos posibilidades:

- No repudio en origen: El emisor no puede negar que envío porque el destinatario tiene pruebas del envío, el receptor recibe una prueba infalsificable del origen del envío, lo cual evita que el emisor, de negar tal envío, tenga éxito ante el juicio de terceros. En este caso la prueba la crea el propio emisor y la recibe el destinatario
- No repudio en destino: El receptor no puede negar que recibió el mensaje porque el emisor tiene pruebas de la recepción. Este servicio proporciona al emisor la prueba de que el destinatario legítimo de un envío, realmente lo recibió, evitando que el receptor lo niegue posteriormente. En este caso la prueba irrefutable la crea el receptor y la recibe el emisor.

Si la autenticidad prueba quién es el autor de un documento y cual es su destinatario, el “no repudio” prueba que el autor envió la comunicación (no repudio en origen) y que el destinatario la recibió (no repudio en destino).

Relación de los servicios de seguridad

En la imagen superior se ilustra como se relacionan los diferentes servicios de seguridad, unos dependen de otros jerárquicamente, así si no existe el de mas abajo, no puede aplicarse el superior. De esta manera, la **disponibilidad** se convierte en el primer requisito de seguridad, cuando existe esta, se puede disponer de **confidencialidad**, que es imprescindible para conseguir **integridad**, para poder obtener **autenticación** es imprescindible la integridad y por ultimo el **no repudio** solo se obtiene si se produce previamente la autenticación.

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

Las amenazas son eventos que pueden causar alteraciones a la información de la organización ocasionándole pérdidas materiales, económicas, de información, y de prestigio.

Las amenazas se consideran como exteriores a cualquier sistema, es posible establecer medidas para protegerse de las amenazas, pero prácticamente imposible controlarlas y menos aún eliminarlas.

2.1.- Fuentes de amenaza

Aunque todas las amenazas tienen la característica de ser las posibles causantes de destrucción a los sistemas, las amenazas pueden tener diferentes orígenes. Existen varias categorías de amenazas, para esta investigación se clasificaran por su origen, de esta forma se dividirán en cinco tipos los cuales son: amenazas humanas, de hardware, de software, de red y desastres naturales.

2.1.2- Factor humano

Las personas son la principal fuente de amenaza que existe en los sistemas de información y son el tipo de amenaza en el que se invierten más recursos para controlarlos y contrarrestar sus efectos.

El Factor Humano(*)

conductas privadas, comportamiento colectivo

Abarca actos malintencionados, incumplimiento de las medidas de seguridad como consecuencia de actos negligentes o falta de controles adecuados.

2.1.2.1- Tipos de amenazas humanas.

Los actos humanos que pueden afectar la seguridad de un sistema son variados, entre los más comunes e importantes están:

Curiosos: se trata de personas que entran a sistemas (en algunos casos de manera accidental) a los que no están autorizados, motivados por la curiosidad, por el desafió personal, o por el deseo de aprender o averiguar.

Generalmente este tipo de intrusos no tienen los conocimientos apropiados para lograr causar daños, pero no por eso se les debe ignorar sin tomar las precauciones necesarias.

Aunque se afirma que no tienen intenciones maliciosas, su sola intrusión al sistema representa una peligrosa amenaza ya que pueden causar daños no intencionales o dejar expuesta la estructura y seguridad del sistema.

Intrusos remunerados: este tipo de atacante se encarga de penetrar a los sistemas a cambio de un pago. Aunque son menos comunes, en realidad son muy peligrosos ya que se trata de personas que poseen los conocimientos, experiencia y herramientas necesarias para penetrar en los sistemas, incuso en aquellos que tienen un nivel alto de seguridad.

Personal enterado: se trata de personas que tienen acceso autorizado o conocen la estructura del sistema de cierta organización. Por lo general es el mismo personal interno de una empresa o un exempleado, sus motivaciones van desde revanchas personales hasta ofertas y remuneraciones de organizaciones rivales.

Terroristas: tienen como objetivo causar daños con diferentes fines por ejemplo proselitistas o religiosos.

Robo: se refiere a la extracción física de la información por medio de unidades de almacenamiento secundario (diskettes, CD, cintas, etc.), robo físico de los componentes de hardware del sistema e incluso también se considera como robo el uso de los equipos para actividades diferentes a los que se les asigna en la organización,

Sabotaje: consiste en reducir la funcionalidad del sistema por medio de acciones deliberadas dirigidas a dañar los equipos, logrando la interrupción de los servicios e incluso la destrucción completa del sistema. Puede ser perpetuada por el personal interno o por opositores externos.

Fraude: estas actividades no tienen como principal fin la destrucción del sistema, si no aprovechar los recursos que se manejan para obtener beneficios ajenos a los objetivos de la organización.

Aun cuando los responsables del fraude sean identificados y detenidos, este tipo de actividad comúnmente se trata con suma discreción sin hacerle publicidad debido a que le da mala imagen a la organización implicada.

Ingeniería social: en el campo de la seguridad informática ingeniería social es la práctica de obtener información confidencial a través de la manipulación de

usuarios legítimos llevándolos a revelar información sensible, o bien a violar las políticas de seguridad típicas.

Con este método, los ingenieros sociales aprovechan la tendencia natural de la gente a confiar en su palabra, antes que aprovechar agujeros de seguridad en los sistemas informáticos. Generalmente se está de acuerdo en que “los usuarios son el eslabón débil” en seguridad; éste es el principio por el que se rige la ingeniería social.

2.1.3 Amenazas en el Hardware

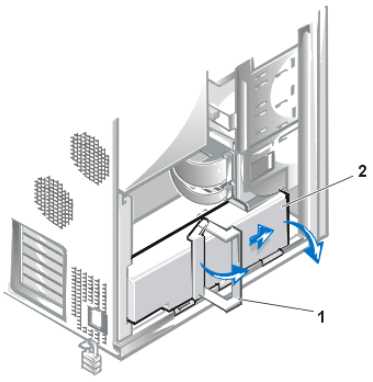
Se da la amenaza por fallas físicas que presente cualquiera de los elementos de hardware que conforman al sistema de cómputo. Estas fallas físicas pueden ser defectos de fabricación o mal diseño del hardware, pero también pueden ser el resultado de un mal uso y descuido en el mantenimiento.

2.1.3.1.-Tipos de amenazas de hardware

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. También debe procurarse que dichas instalaciones proporcionen los voltajes requeridos para hacer funcionar un dispositivo, pues existen componentes de hardware que necesitan ser energizados a ciertos niveles de voltaje especificados por los fabricantes, de lo contrario se acortara su vida útil.



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

Descuido y mal uso: todos los componente 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 que trae como consecuencia descomposturas prematuras y reducción del tiempo de vida útil de los recursos.

2.1.4.-Red de datos

Esta amenaza se presenta cuando la red de comunicación no está disponible para su uso, esto puede ser provocado por un ataque deliberado por parte de un intruso o un error físico o lógico del sistema mismo. Las dos principales amenazas que se presentan en una red de datos son, la no disponibilidad de la red, y la extracción lógica de información a través de ésta.

2.1.4.1.- Tipos

Topología seleccionada: la topología es la disposición física en la que se conectan los nodos de una red de ordenadores o servidores, cada una presenta una serie de ventajas y desventajas. Dependiendo el alcance y recursos compartidos en una red, puede ser más conveniente seleccionar una topología sobre otra, pero debe tomarse en cuenta que las desventajas de cada arquitectura no solo limitan la comunicación, incluso pueden dejar la red fuera de servicio.

Sistema operativo: aunque el modelo OSI permite la comunicación entre equipos con diferentes sistemas operativos, se dan casos en los que ciertas opciones de operación difieren entre sistemas operativos, haciendo difícil el compartir ciertos recursos.

También cada sistema operativo tiene un nivel de protección diferente que los hace más susceptibles a ataques que otros, y a partir de ahí el atacante puede tomar acciones contra otros sistemas operativos con mayor nivel de seguridad. Este último punto es considerado más una vulnerabilidad que una amenaza.

Incumplimiento de las normas de instalación de la red: la instalación del cableado físico de las redes de datos, deben seguir ciertas normas y estándares de diseño conocidos también como cableado estructurado.

2.1.5.- Amenazas Software

Las amenazas de software incluyen posibles fallas dentro del software de un sistema operativo, software mal desarrollado, mal diseñado o mal implantado, además de que existe software de uso malicioso que representa una amenaza directa contra un sistema.

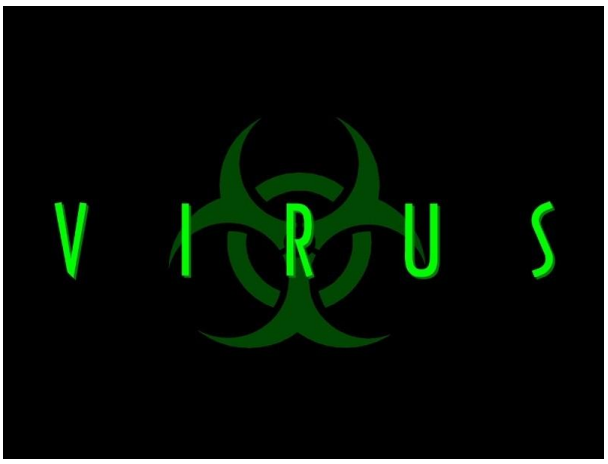
2.1.5.1.-Tipos

Software de desarrollo: es un tipo de software personalizado, puede ser creado con el fin de atacar un sistema completo o aprovechar alguna de sus características para violar su seguridad.

Software de aplicación: este software no fue creado específicamente para realizar ataques, pero tiene características que pueden ser usadas de manera maliciosa para atacar un sistema.

Código malicioso: 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 si mismo usando recursos del sistema infectado, propagando su infección rápidamente.



Troyanos: este tipo de código se presenta escondido en otros programas de aplicación aparentemente inofensivos, para posteriormente activarse de manera discreta cumpliendo su propósito nocivo.

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

Errores de programación y diseño: el software creado para cumplir alguna función dentro de la organización (Por ejemplo un sistema de transacciones financieras, sistema de nomina, sistemas operativos, etc.) también pueden causar perdida o modificación de la información. Esto ocurre cuando el software en cuestión no cumple con los estándares de seguridad requeridos pues nunca fue diseñado para dar soporte a una organización. Los errores de programación y fallas generales que puede tener un software de aplicación también representan una amenaza.

2.1.5.-Desastres naturales

Son eventos que tienen su origen en las fuerzas de la naturaleza. Estos desastres no solo afectan a la información contenida en los sistemas, sino también representan una amenaza a la integridad del sistema completo (infraestructura, instalación, componentes, equipos, etc.) pudiendo dejar al sistema incluso en un estado de intolerabilidad permanente. Este tipo de amenazas también incluye la falta de preparación.

2.1.5.1Tipos

Entre los tipos de desastres naturales que amenazan a un sistema de información, tenemos las inundaciones, los terremotos, incendios, huracanes, tormentas eléctricas, etc. Los cuales provocan cortos circuitos, destrucción total o parcial de los equipos de cómputo, o alteraciones físicas de las localidades, causando que ya no sean apropiadas para albergar un equipo de cómputo.

Por lo que es necesario considerar el punto geográfico en el que se llevara a cabo la instalación del equipo de cómputo, centro de servicios de información, centro de cómputo etc. y hacer un estudio que permita determinar las amenazas a las que serian susceptibles a fin de evitar ser víctimas de estos.

Adicionalmente considerar la importancia de un cableado no solo en la res de datos sino de las redes de energía eléctrica y suministro de aguas que de manera indirecta podrían causar algún desastre de este tipo y dañar la información de la organización.

3.-Analisis de las principales vulnerabilidades de un sistema informático.

Vulnerabilidades

Dependiendo del enfoque que se le de a la seguridad informática, un sistema informático está expuesto al peligro por medio de dos factores: Las amenazas y las vulnerabilidades.

Las vulnerabilidades constituyen el otro factor que pone en peligro la seguridad de un sistema, generalmente se cree que una vulnerabilidad es un punto débil de un sistema y aunque no es una definición incorrecta, tampoco expresa en su totalidad lo que es una vulnerabilidad.

3.1.-Definición

Una vulnerabilidad informática es un elemento de un sistema informático que puede ser aprovechado por un atacante para violar la seguridad, así mismo pueden causar daños por sí mismos sin tratarse de un ataque intencionado.

A las vulnerabilidades se les consideran un elemento interno del sistema, por lo que es tarea de los administradores y usuarios el detectarlos, valorarlos y reducirlos.

3.2.-Tipos de Vulnerabilidades

Las vulnerabilidades son el resultado de errores de programación (bugs), fallos en el diseño del sistema, incluso las limitaciones tecnológicas pueden ser aprovechadas por los atacantes.

Para esta investigación, se clasifican las vulnerabilidades en seis tipos: Físicas, naturales, de hardware, de software, de red y de factor humano.

Físicas

Está relacionada con el acceso físico al sistema. Es todo lo referente al acceso y de las instalaciones donde se tienen los equipos de cómputo que contienen la información o forman partes de los procesos esenciales del sistema.

Las vulnerabilidades de este tipo se pueden presentar en forma de malas prácticas de las políticas de acceso de personal a los sistemas y uso de medios físicos de almacenamiento de información que permitan extraer datos del sistema de manera no autorizada.

Naturales

Recordemos que las amenazas naturales son todo tipo de desastres causados por fuerzas naturales que causan daño a un sistema, por el lado de las amenazas naturales, estas se refieren al grado en que el sistema se puede ver afectado por este tipo de eventos.

Las vulnerabilidades de tipo natural se presentan principalmente en deficiencias de las medidas tomadas para afrontar los desastres, por ejemplo no disponer de reguladores, no-breaks, mal sistema de ventilación o calefacción, etc.

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.

Software

Cada programa (ya sea de paquetería o de sistema operativo) puede ser usado como medio para atacar a un sistema más grande, esto se da debido a errores de programación, o porque en el diseño no fueron considerados ciertos aspectos (por ejemplo controles de acceso, seguridad, implantación, etc.).

Ambos factores hacen susceptible al sistema a las amenazas de software.

Red

Las redes pueden llegar a ser sistemas muy vulnerables, al tratarse de una serie de equipos conectados entre sí compartiendo recursos, es posible atacar a toda la red penetrando primero en uno de los equipos y posteriormente expandirse 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.

Estos dos puntos hacen que las vulnerabilidades de las redes lleguen a ser una combinación de vulnerabilidades de hardware, software, físicas e incluso naturales.

Factor humano

Los elementos humanos de un sistema son los más difíciles de controlar lo que los convierte en constantes amenazas y al mismo tiempo una de las partes más vulnerables del sistema.

Las vulnerabilidades de origen humano más comunes son la falta de capacitación y concienciación, lo que puede dar lugar a la negligencia en el seguimiento de las políticas de seguridad, y mal uso del equipo de cómputo.

Los actos contra la seguridad realizados a conciencia por un elemento humano (Como el robo de información o la destrucción de los sistemas) pueden ser el resultado de una vulnerabilidad humana, ya sea por un usuario que accidentalmente revela las contraseñas de acceso o no revisa periódicamente las bitácoras de actividades de los equipo de cómputo a fin de buscar actividades sospechosas por citar algunos ejemplo.

Un usuario resentido o con poca lealtad a la organización es una amenaza y una vulnerabilidad humana al mismo tiempo, pues él puede convertirse en el autor directo de ataques al sistema o revelar intencionalmente información del sistema a personas no convenientes.

Finalmente es importante hacer una reflexionen el sentido de que las vulnerabilidades se pueden reducir, eliminar o controlar lo que ayuda entonces a contrarrestar la posibilidad de que una amenaza se materialice y llegue a convertirse en un ataque.

De manera que el riesgo es el daño potencial que puede surgir por un proceso presente o suceso futuro, es decir, es la posibilidad de que un peligro pueda materializarse.

4.-SEGURIDAD INFORMATICA

Podemos dar protección a nuestro sistemas dependiendo lo que se quiera proteger las medidas de seguridad muy superiores a lo normal serán muy costosas y pueden llegar a ser desfavorables pudiendo llamar la atención. La seguridad debe ser adecuada a la necesidad de protección de lo asegurado y a los recursos disponibles. Conviene hacer una valoración de riesgos y de los costos de la protección de forma que los costos no superen a los riesgos. Para evaluar los riesgos conviene describir: qué deseamos proteger cuál es su valor qué riesgos existen quién puede atacar.

Seguridad con respecto a la naturaleza de la amenaza:
Existen dos tipos de seguridad con respecto a la naturaleza de la amenaza:

Seguridad lógica: aplicaciones para seguridad, herramientas informáticas, etc.
Seguridad física: mantenimiento eléctrico, anti-incendio, humedad, etc.

4.1.-La seguridad lógica de un sistema informático incluye:

Restringir al acceso a programas y archivos mediante claves y/o encriptación. Asignar las limitaciones correspondientes a cada usuario del sistema informático. Esto significa, no darle más privilegios extras a un usuario, sino sólo los que necesita para realizar su trabajo. Asegurarse que los archivos y programas que se emplean son los correctos y se usan correctamente. Por ejemplo, el mal uso de una aplicación puede ocasionar agujeros en la seguridad de un sistema informático. Control de los flujos de entrada/salida de la información. Esto incluye que una determinada información llegue solamente al destino que se espera que llegue, y que la información llegue tal cual se envió.
Los controles anteriormente mencionados se pueden hacer a nivel sistema operativo, a nivel aplicación, a nivel base de datos o archivo, o a nivel firmware.

Ejemplos de barreras de seguridad a nivel software (seguridad lógica):

Encriptación:

Es el proceso mediante el cual una rutina es codificada de tal manera que no pueda ser interpretada fácilmente. Es una medida de seguridad utilizada para que al momento de transmitir la información ésta no pueda ser interceptada por intrusos.

Sistemas de protección de Cortafuegos o firewalls:

Un cortafuegos (o firewall en inglés), es un elemento de hardware o software utilizado en una red de computadoras para controlar las comunicaciones, permitiéndolas o prohibiéndolas según las políticas de red que haya definido la organización responsable de la red.

Antivirus: Es un software que se instala en tu ordenador y que permite prevenir que programas diseñados para producir daños, también llamados virus, dañen tu equipo. También tiene la misión de limpiar ordenadores ya infectados.

Antispam: Es un método de protección contra la publicidad no deseada de este modo se evita los molestos avisos publicitarios.

Antitroyanos: Un AntiTroyano es un programa desarrollado para combatir software malicioso -malware- como los llamados troyanos o backdoors.
Los troyanos son programas creados para a través de un archivo servidor abrir un puerto y luego ponerse a la escucha para que el atacante desde el programa cliente se conecte al servicio y pueda utilizar la computadora de la victima de forma remota.

Los mecanismos de seguridad física:

Deben resguardar de amenazas producidas tanto por el hombre como por la naturaleza.
Básicamente, las amenazas físicas que pueden poner en riesgo un sistema informático son:

-Desastres naturales, incendios accidentales,

humedad e inundaciones.

-Amenazas ocasionadas involuntariamente por personas.

-Acciones hostiles deliberadas como robo, fraude o sabojate.

Ejemplos de barreras de seguridad a nivel software (seguridad física):

SAI - UPS (Uninterruptible Power Supply)

Un SAI es un dispositivo que proporciona suministro eléctrico en el caso de que se produzca un fallo en el suministro eléctrico principal. Esto es, un sistema de respaldo del suministro eléctrico. También proporciona suministro estable, lo que previene de fallos eléctricos a los equipos.

Protección contra incendios

En un incendio en una sala de ordenadores, etc. además de los impactos por las pérdidas humanas y materiales, la alta temperatura causa daños directos en los elementos cercanos. Sin embargo, los daños de mayor importancia se producen por los humos y gases que son generados en el incendio, que se pueden propagar rápidamente, incluso a dependencias anexas.

Por lo tanto, es importante la implantación de un sistema eficaz de extinción de incendios que evite todos los daños descritos anteriormente.

Existen sistemas de extinción manuales, ampliamente conocidos, u otros automáticos.

Los elementos típicos y mínimos de una instalación de extinción automática son:

- Sistema de detección: constituido por iniciadores de incendio que captan y revelan la presencia del fuego, pudiendo estar integrados en el equipo (rociadores) o formar parte del sistema ajeno de detección automática de incendios.

- Central de alarma: procesa las señales recibidas de los equipos detectores y actúa en función de parámetros programados: comunicar la alarma, activar el mecanismo de disparo (en ciertos equipos -rociadores- está vinculado al detector directamente y en otros también es posible hacerlo manualmente), conectar otros sistemas, etc.

- Dispositivos de descarga: son los elementos que deben proyectar el agente extintor sobre el espacio incendiado (rociadores, difusores, emisores,...).
- Depósito de almacenamiento del agente extintor: dependiendo de éste se pueden contener en recipientes de características, formas y tamaños muy variados.

Los componentes de las instalaciones anteriormente descritos se disponen en sistemas de protección contra incendios configurados en función del agente extintor empleado para anular los efectos del fuego:

- Sistemas automáticos de rociadores de agua o sprinklers.
- Sistemas automáticos de extinción por agua: pulverizada, nebulizada o por aspersión.
- Sistemas de CO2 (anhídrido carbónico).
- Sistemas de extinción por espuma.
- Sistemas de extinción por polvo.
- Instalaciones fijas de gases inertes: emplean gases sustitutivos del halón: Inergen, S-lll, FM-200, FE-13, Argón,...).

Refrigeración

Se deberá instalar un sistema de refrigeración en las salas de servidores, que permitan mantener una temperatura idónea para el correcto funcionamiento de los equipos.

Lo más recomendable es poner los equipos sobre un falso suelo, por el que se impulsa aire que sube, refrigerando los equipos.

Ubicación y protección física de los equipos y servidores

Continuamos en el apartado de "Aplicación de medidas de seguridad pasiva" de estos apuntes de dirigidos para el "Módulo Profesional de Seguridad informática" que pertenece a el FP. de grado medio de "Técnico en Sistemas Microinformáticos y Redes".

5.-Ubicación y protección física de los equipos y servidores

Los incidentes de tipo físico que encontramos en los equipos y servidores se pueden dividir en dos tipos básicos.

•**Incidentes Naturales**: Incendios, inundaciones, temperatura, alimentación eléctrica, ...

•**Incidentes Humanos:** Robos, fraudes, sabotajes, ...

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 en bajo ciertas condiciones.

Como es lógico pensar no todos los equipos informáticos de una organización tienen el mismo valor. Para poder tener una buena seguridad debemos saber que equipos y datos son más importantes para la organización. Ej. Un servidor y un puesto de trabajo no tendrán las mismas medidas de seguridad, ni físicas ni lógicas.

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.

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.

Para poder asegurar un CPD lo primero que debemos hacer es asegurar el recinto con medidas de seguridad física. Ejemplos de medidas de seguridad:

•**Sistemas contra incendios.**

Existen varios tipos de sistemas de extinción de incendios, como: extracción de oxigeno, inserción de gases nobles o extintores especiales que eviten el riesgo de electrocución.

Es importante intentar evitar los sistemas contra incendios que usen materiales conductores, dado que, de lo contrario pueden perderse datos de los dispositivos.

•Sistemas de control de acceso.

•Sistemas de Llaves (tradicionales).

•Sistemas de contraseña.

Estos sistemas son los más usados por su simplicidad de uso y bajo coste. En estos tipos de sistemas se ha de establecer políticas de contraseñas. Por tanto la organización que implemente un sistema de contraseña tendrá que indicar a sus usuarios con que periodicidad son cambiadas y que características tienen que tener para ser seguras. Sobre las políticas de contraseñas hablaremos más adelante.

•Sistemas Tarjeta magnética.

Estos sistemas se componen de una tarjeta con una banda magnética que contiene un código para acceder.

•Sistemas RFID:

Son las siglas de identificación por radio frecuencia en Ingles (Radio Frequency IDentification), estos sistemas se componen de un elemento que reacciona ante una señal, devolviendo un resultado. Existen dispositivos RFID con identificadores únicos certificados por la casa de la moneda.

•Sistemas de Token.

Un sistema de token se compone de un elemento móvil llamado "Token" que genera claves aleatorias, para poder funcionar correctamente el token ha de estar sincronizado con el sistema de acceso. Para poder acceder el usuario ha de insertar la clave generada por el token en el sistema, este generará una clave usando el mismo algoritmo y la comparará. Actualmente se están usando sistemas de "Token" mediante el envío de un sms.

•Sistemas Biométricos.

Son sistemas que otorgan acceso mediante la identificación por elementos físicos de cada individuo, véase iris del ojo, huellas dactilares, voz, sistema de venas palmares, u otros rasgos únicos. Este tipos de sistemas son más complejos para ser saltados dado es muy complejo copiar este tipo de datos.

•Sistemas de control de temperatura.

Para que los sistemas informáticos funcionen correctamente los elementos físicos de los mismos han de encontrase a ciertas temperaturas.

Debido a que los equipos informáticos funcionan mediante semiconductores se tienen que mantener entre cierto valores de temperatura, de lo contrario los semiconductores pierden sus propiedades y dejan de funcionar adecuadamente. La temperatura adecuada de un CPD no debe de superar los 30º.

6.-SISTEMAS DE ALIMENTACIÓN ININTERRUMPIDA

QUE ES UN SAI Y COMO FUNCIONA.

Un SAI es un dispositivo que proporciona suministro eléctrico en el caso de que se produzca un fallo en el suministro eléctrico principal. Esto es, un sistema de respaldo del suministro eléctrico. También proporciona suministro estable, lo que previene de fallos eléctricos a los equipos.

Por lo tanto, un S.A.I es especialmente útil con equipos informáticos que pueden sufrir daños por cortes en el suministro eléctrico, o para aquellas empresas que trabajan con grandes cantidades de datos e información, pudiendo producirse pérdidas en los mismos en el caso de un corte de electricidad repentino.

El caso más evidente en el que es necesario un sistema de alimentación ininterrumpida es en el caso de los servidores.

Estos equipos sirven para proporcionar servicios que, normalmente, suelen ser necesarios en un ámbito 24x7, es decir, estos equipos están permanentemente conectados.

Con un sistema de alimentación ininterrumpida, la empresa se garantiza que el servidor se mantendrá funcionando, incluso cuando hay un corte en el suministro eléctrico habitual, lo que facilita que no se produzcan interrupciones en el trabajo, a la vez que se garantiza que no haya pérdidas en el contenido de los datos.

Los precios de estos dispositivos varían en función del sistema a mantener alimentado, y de la duración de ese suministro de respaldo:

Cuanto más grande sea el equipo que necesite ser mantenido en funcionamiento durante un corte en el suministro eléctrico, y cuanto más tiempo se necesite que dure esa alimentación eléctrica, más caro será el SAI.

TIPOS DE SAID

- **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**. 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**. 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 carga 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.

Otras **características habituales** de un SAI ó UPS:

- La mayoría de los SAI tienen dos **conectores RJ11 para proteger los equipos conectados a una línea telefónica**, en caso de que la línea reciba una sobretensión. En uno se conecta la línea de entrada y al otro se conectan los dispositivos a proteger. A veces se proporciona un conector RJ45, que es compatible con el RJ11 y permite proteger líneas de datos también.

- Del mismo modo, la mayoría de los SAI tienen una **salida RS-232 y/o USB para conectarlos a un ordenador**. Mediante el software adecuado, el ordenador es capaz de **conocer el estado del SAI y de autoapagarse** en caso de que tras un fallo de suministro prolongado, el ordenador vaya a quedarse sin alimentación. Esto es adecuado si cada ordenador se protege con un SAI, pero insuficiente si un SAI protege varios ordenadores al mismo tiempo.

- Algunos de nuestros SAI permiten la conexión de una **tarjeta de red** que permite extender la función anterior a los **ordenadores de toda una red**. De este modo, si un SAI protege varios ordenadores, todos ellos pueden conocer su estado y apagarse ordenadamente antes de quedarse sin suministro eléctrico. Esto es especialmente importante en servidores empresariales donde un fallo eléctrico podría ocasionar la pérdida de información.

7.-Sistemas biométricos: Funcionamiento. Estándares

La **biometría** es el estudio de métodos automáticos para el reconocimiento único de humanos basados en uno o más rasgos conductuales o físicos intrínsecos. 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.

FUNCIONAMIENTO

En un sistema de Biometria típico, la persona se registra con el sistema cuando una o más de sus características físicas y de conducta es obtenida, procesada por un algoritmo numérico, e introducida en una base de datos. Idealmente, cuando entra, casi todas sus características concuerdan; entonces cuando alguna otra persona intenta identificarse, no empareja completamente, por lo que el sistema no le permite el acceso. Las tecnologías actuales tienen tasas de error que varían ampliamente (desde valores bajos como el 60%, hasta altos como el 99,9%).

El rendimiento de una medida biométrica se define generalmente en términos de tasa de falso positivo (*False Acceptance Rate* o FAR), la tasa de falso negativo (*False NonMatch Rate* o FNMR, también *False Rejection Rate* o FRR), y el fallo de tasa de alistamiento (*Failure-to-enroll Rate*, FTR o FER).

En los sistemas biométricos reales el FAR y el FRR puede transformarse en los demás cambiando cierto parámetro. Una de las medidas más comunes de los sistemas biométricos reales es la tasa en la que el ajuste en el cual acepta y rechaza los errores es igual: la tasa de error igual (*Equal Error Rate* o EER), también conocida como la tasa de error de cruce (*Cross-over Error Rate* o CER). Cuanto más bajo es el EER o el CER, se considera que el sistema es más exacto.

Las tasas de error anunciadas implican a veces elementos idiosincrásicos o subjetivos. Por ejemplo, un fabricante de sistemas biométricos fijó el umbral de aceptación alto, para reducir al mínimo las falsas aceptaciones; en la práctica, se permitían tres intentos, por lo que un falso rechazo se contaba sólo si los tres intentos resultaban fallidos (por ejemplo escritura, habla, etc.), las opiniones pueden variar sobre qué constituye un falso rechazo.

Tabla comparativa de sistemas biométricos

o que sigue a continuación es una tabla en la que recogen las diferentes características de los sistemas biométricos:

	Ojo (Iris)	**Ojo (Retina)**	**Huellas dactilares**	**Vascular dedo**	**Vascular mano**	**Geometría de la mano**	**Escritura y firma**	**Voz**	**Cara 2D**	**Cara 3D**
Fiabilidad	Muy alta	Muy Alta	Muy Alta	Muy Alta	Muy Alta	Alta	Media	Alta	Media	Alta
Facilidad de uso	Media	Baja	Alta	Muy Alta	Muy Alta	Alta	Alta	Alta	Alta	Alta
Prevención de ataques	Muy alta	Muy Alta	Alta	Muy Alta	Muy Alta	Alta	Media	Media	Media	Alta
Aceptación	Media	Baja	Alta	Alta	Alta	Alta	Muy Alta	Alta	Muy alta	Muy alta
Estabilidad	Alta	Alta	Alta	Alta	Alta	Media	Baja	Media	Media	Alta

Estándares

En los últimos años se ha notado una preocupación creciente por las organizaciones regulatorias respecto a elaborar estándares relativos al uso de técnicas biométricas en el ambiente informático. Esta preocupación es reflejo del creciente interés industrial por este ámbito tecnológico, y a los múltiples beneficios que su uso aporta. No obstante ello, aún la estandarización continua siendo deficiente y como resultado de ello, los proveedores de soluciones biométricas continúan suministrando interfaces de software propietarios para sus productos, lo que dificulta a las empresas el cambio de producto o vendedor.

A nivel mundial el principal organismo que coordina las actividades de estandarización biométrica es el Sub-Comité 17 (SC17) del Joint Technical Committee on Information Technology (ISO/IEC JTC1), del International Organization for Standardization (ISO) y el International Electrotechnical Commission (IEC).

En Estados Unidos desempeñan un papel similar el Comité Técnico M1 del INCITS (InterNational Committee for Information Technology Standards), el National Institute of Standards and Technology (NIST) y el American National Standards Institute (ANSI).

Existen además otros organismos no gubernamentales impulsando iniciativas en materias biométricas tales como: Biometrics Consortium, International Biometrics Groups y BioAPI. Este último se estableció en Estados Unidos en 1998 compuesto por las empresas Bioscrypt, Compaq, Iridiam, Infineon, NIST, Saflink y Unisis. El Consorcio BioAPI desarrolló conjuntamente con otros consorcios y asociaciones, un estándar que promoviera la conexión entre los dispositivos biométricos y los diferentes tipos de programas de aplicación, además de promover el crecimiento de los mercados biométricos.

Algunos de los estándares más importantes son:

- Estándar ANSI X.9.84: creado en 2001, por la ANSI (American National Standards Institute) y actualizado en 2003, define las condiciones de los sistemas biométricos para la industria de servicios financieros haciendo referencia a la transmisión y almacenamiento seguro de información biométrica, y a la seguridad del hardware asociado.

- Estándar ANSI / INCITS 358: creado en 2002 por ANSI y BioApi Consortium, presenta una interfaz de programación de aplicación que garantiza que los productos y sistemas que cumplen este estándar son interoperables entre sí.
- Estándar NISTIR 6529: también conocido como CBEFF (Common Biometric Exchange File Format) es un estándar creado en 1999 por NIST y Biometrics Consortium que propone un formato estandarizado (estructura lógica de archivos de datos) para el intercambio de información biométrica.

- Estándar ANSI 378: creado en 2004 por la ANSI, establece criterios para representar e intercambiar la información de las huellas dactilares a través del uso de minucias. El propósito de esta norma es que un sistema biométrico dactilar pueda realizar procesos de verificación de identidad e identificación, empleando información biométrica proveniente de otros sistemas.
- Estándar ISO 19794-2: creado en 2005 por la ISO/IEC con propósitos similares a la norma ANSI 378, respecto a la que guarda mucha similitud.
- Estándar PIV-071006: creado en 2006 por el NIST y el FBI en el contexto de la norma FIPS 201 del gobierno de EE.UU, establece los criterios de calidad de imagen que deben cumplir los lectores de huellas dactilares para poder ser usados en procesos de verificación de identidad en agencias federales.

8.-Seguridad lógica: Copias de seguridad e imágenes de respaldo.

Una **Copia de Seguridad**, es un duplicado de nuestra información más importante, que realizamos para salvaguardar los documentos, archivos, fotos, etc., de nuestro ordenador, por si acaso ocurriese algún problema que nos impidiese acceder a los originales que tenemos en él.

Esta Copia de Seguridad también se denomina Copia de Respaldo e incluso, podremos encontrarnos con la denominación Backup en términos ingleses.

Podemos **perder nuestra información** o cuando menos **no poder acceder a ella** por motivos muy diversos, desde infecciones del sistema por virus y malware, fallos de hardware (cortes de corriente y picos de tensión, excesos de temperatura y daños en los dispositivos), apagados incorrectos del equipo, problemas motivados por algún programa, daños del usuario al borrar archivos por error, etc.

Tipos de copias de seguridad

En función de la cantidad de archivos que se salvaguardan a la hora de realizar la copia de seguridad, podemos distinguir tres tipos de copia:

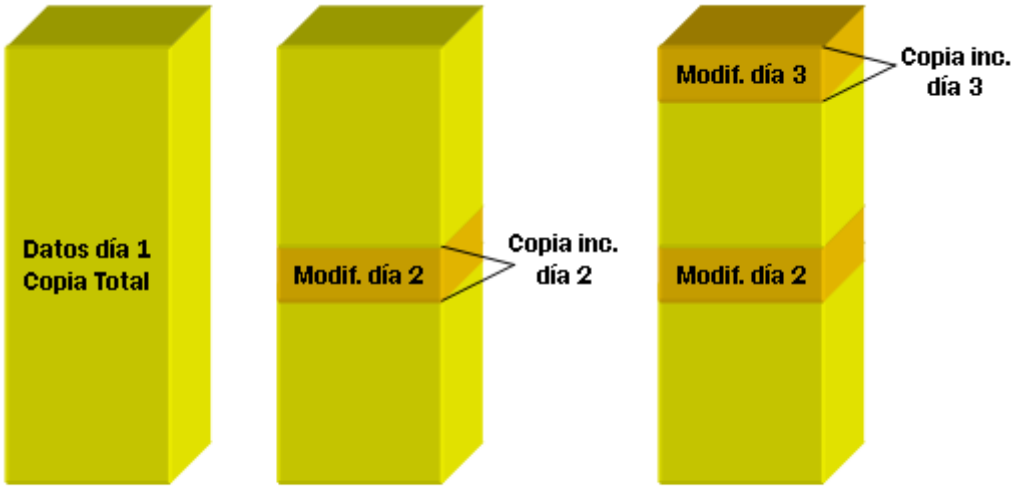
- Copia de seguridad total o íntegra
- Copia de seguridad incremental
- Copia de seguridad diferencial

Copia normal o copia total

Una copia de seguridad normal, es una copia de seguridad total de todos los archivos y directorios seleccionados.

Copia incremental

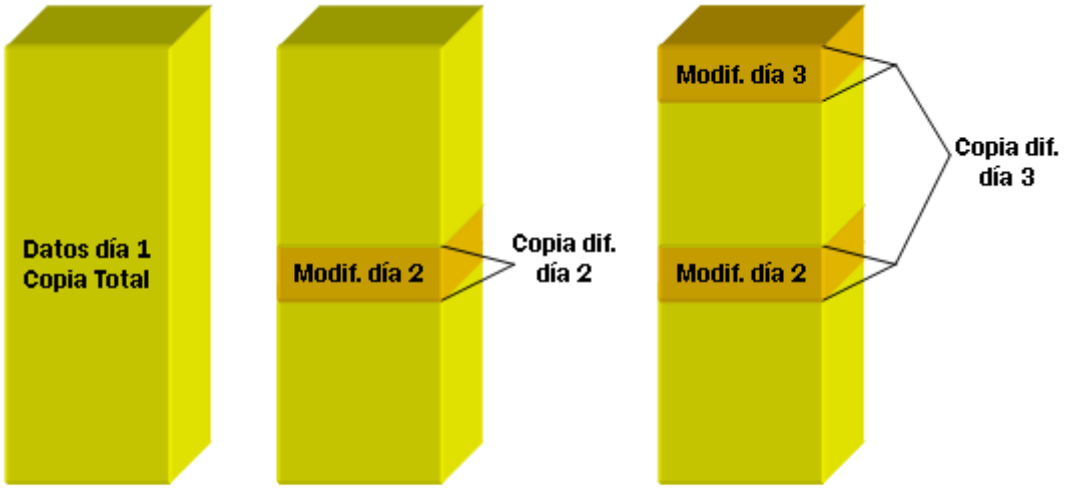
En un proceso de copia de seguridad incremental, se hace una copia de seguridad sólo de los archivos que han cambiado desde la última copia de seguridad realizada. Ejemplo, si hacemos copia de seguridad total el día 1 de cada mes y copia de seguridad incremental el resto de los días, cada copia incremental solo guardará los archivos que se hayan modificado ese día. Si tenemos que realizar la restauración de archivos **ante un desastre, debemos disponer de la copia total y de todas las copias incrementales que hayamos realizado desde la copia total.**



Las copias incrementales guardan solo los archivos modificados desde la última copia incremental

Copia diferencial

Una copia de seguridad diferencial es una copia de todos los archivos que han cambiado desde la última copia de seguridad total que hayamos hecho. Ejemplo, si hacemos copia de seguridad total el día 1 de cada mes y copia de seguridad diferencial el resto de los días, cada copia diferencial guardará los archivos que se hayan modificado desde el día 1. La ventaja es que se requiere menos espacio que la copia total y que **en el proceso de restauración únicamente necesitaremos la última copia total y la última copia diferencial.** Una copia diferencial anula a la copia diferencial anterior. Por el contrario, se consume más tiempo en realizar la copia y también más espacio que en el caso de copia incremental.



Las copias diferenciales guardan solo los archivos modificados desde la última copia total

Recomendación sobre el tipo de copia a efectuar

Si el volumen de datos de nuestra copia de seguridad no es muy elevado (menos de 4 GB), lo más práctico es realizar **siempre copias totales** ya que en caso de desastre, tan solo debemos recuperar la última copia.

Si el volumen de datos de nuestra copia de seguridad es muy elevado (mayor de 50 GB) pero el volumen de datos que se modifican no es elevado (sobre 4 GB), lo más práctico es realizar una primera copia total y posteriormente realizar **siempre copias diferenciales**. Así, en caso de desastre, tan solo debemos recuperar la copia total y la última diferencial. Periódicamente debemos realizar una copia total y así empezar de nuevo.

Si el volumen de datos de nuestra copia de seguridad es muy elevado (mayor de 50 GB) y el volumen de datos que se modifican también lo es, las copias diferenciales ocuparán mucho espacio, por lo tanto en este caso lo más práctico será realizar una primera copia total y posteriormente realizar **siempre copias incrementales** ya que son las que menos espacio ocupan. El problema es que en caso de desastre debemos recuperar la última copia total y todas las incrementales realizadas desde que se hizo la última copia total. En estos casos, conviene hacer copias totales más a menudo para no tener que mantener un número muy elevado de copias incrementales.

En grandes compañías donde la realización de copias de seguridad está perfectamente planificada, se suelen utilizar sistemas mixtos. Por ejemplo en un caso típico se realizarían las siguientes tareas:

- Todos los días 1 de cada mes, a las 23:00 horas: copia de seguridad total
- Todos los viernes a las 23:00 horas: copia de seguridad diferencial desde la copia de día 1
- Todos los días (excepto los viernes y el día 1) a las 23:00 horas: copia de seguridad incremental desde la copia del día anterior.

Con ésta planificación nos aseguramos disponer de copia de seguridad diaria. En caso de desastre deberíamos recuperar la copia total, la última diferencial y todas las incrementales desde la última diferencial.

En una política de este tipo se pueden utilizar por ejemplo 5 juegos diferentes de cintas de forma que se almacenen las copias de seguridad diarias de los últimos 3 meses. Luego se van reutilizando pero no más de 20 veces ya que las cintas se deterioran y la fiabilidad disminuye.

Imagen de respaldo

Una imagen del Sistema, llamada también "imagen Ghost" o "Ghost" a causa de un programa bastante conocido, es una copia de respaldo de todo el contenido de una partición (incluso de un conjunto de particiones). Ninguna distinción es hecha en el contenido. Se puede decir que una imagen del sistema es una "copia fiel" de la partición en un instante T (siendo T la hora del respaldo).

Debemos hacer una distinción entre imagen del sistema y copia de respaldo de datos. Por lo general, las copias de respaldo son hechas de forma continua o de manera muy regular, seleccionando los directorios a respaldar y casi siempre de forma incremental.

En cambio, el sistema cambia muy poco por lo que no hay necesidad de crear una imagen frecuentemente. Para crear una imagen, debemos elegir la partición y no los directorios. La copia de seguridad incremental consiste en hacer una copia de respaldo de todo lo que se especificó la primera vez, luego solamente de los archivos modificados posteriormente, guardando aparte una copia del archivo original. Por lo tanto, copia de respaldo e imagen del sistema son dos cosas muy distintas en cuanto a sus objetivos y métodos.

Para qué hacer una imagen del sistema

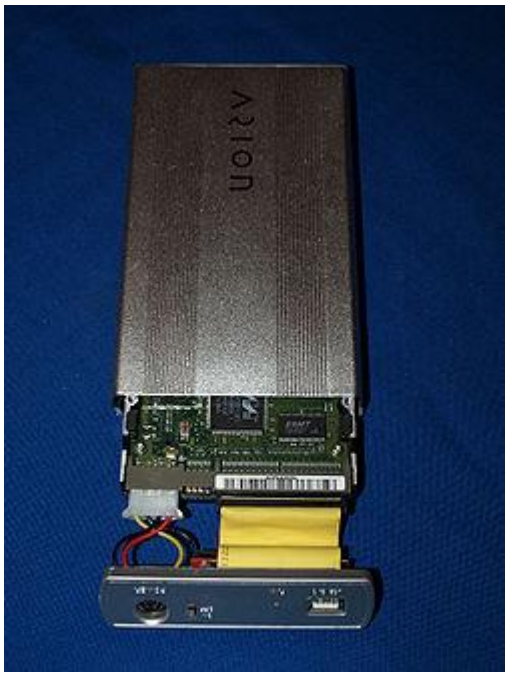
Una a imagen del sistema se realiza principalmente para poder restaurar nuestro sistema operativo cuando este haya sufrido daños; evitando así tener que instalar de nuevo sistema operativo. La principal ventaja de una imagen es que una vez restaurada el ordenador tendrá la misma configuración y los mismos archivos que tenía en el momento de la realización de la imagen.

•Seguridad lógica:
Medios de almacenamiento.

- Soportes de almacenamiento.

9.-Dispositivos de almacenamiento de datos

Disco duro



Los discos duros tienen una gran capacidad de almacenamiento de información, pero al estar alojados normalmente dentro del armazón de la computadora (discos internos), no son extraíbles fácilmente. Para intercambiar información con otros equipos (si no están conectados en red) necesitamos utilizar unidades de disco, como los disquetes, los discos ópticos (CD, DVD), los discos magneto-ópticos, memorias USB, memorias flash, etc.

El disco duro almacena casi toda la información que manejamos al trabajar con una computadora. En él se aloja, por ejemplo, el sistema operativo que permite arrancar la máquina, los programas, archivos de texto, imagen, vídeo, etc. Dicha unidad puede ser interna (fija) o externa (portátil), dependiendo del lugar que ocupe en el gabinete o caja de computadora.

Un disco duro está formado por varios discos apilados sobre los que se mueve una pequeña cabeza magnética que graba y lee la información.

Este componente, al contrario que el micro o los módulos de memoria, no se pincha directamente en la placa, sino que se conecta a ella mediante un cable. También va conectado a la fuente de alimentación, pues, como cualquier otro componente, necesita energía para funcionar.

Las características principales de un disco duro son:

- Capacidad: Se mide en gigabytes (GB). Es el espacio disponible para almacenar secuencias de 1 byte. La capacidad aumenta constantemente desde cientos de MB, decenas de GB, cientos de GB y hasta TB.
- Velocidad de giro: Se mide en revoluciones por minuto (RPM). Cuanto más rápido gire el disco, más rápido podrá acceder a la información la cabeza lectora. Los discos actuales giran desde las 4.200 a 15.000 RPM, dependiendo del tipo de ordenador al que estén destinadas.
- Capacidad de transmisión de datos: De poco servirá un disco duro de gran capacidad si transmite los datos lentamente. Los discos actuales pueden alcanzar transferencias de datos de 3 GB por segundo.

También existen discos duros externos que permiten almacenar grandes cantidades de información. Son muy útiles para intercambiar información entre dos equipos. Normalmente se conectan al PC mediante un conector USB.

Cuando el disco duro está leyendo, se enciende en la carcasa un LED (de color rojo, verde u otro). Esto es útil para saber, por ejemplo, si la máquina ha acabado de realizar una tarea o si aún está procesando datos.

Disquetera

La unidad de 3,5 pulgadas permite intercambiar información utilizando disquetes magnéticos de 1,44 MB de capacidad. Aunque la capacidad de soporte es muy limitada si tenemos en cuenta las necesidades de las aplicaciones actuales se siguen utilizando para intercambiar archivos pequeños, pues pueden borrarse y reescribirse cuantas veces se desee de una manera muy cómoda, aunque la transferencia de información es bastante lenta si la comparamos con otros soportes, como el disco duro o un CD-ROM.

Para usar el disquete basta con introducirlo en la ranura de la disquetera. Para expulsarlo se pulsa el botón situado junto a la ranura, o bien se ejecuta alguna acción en el entorno gráfico con el que trabajamos (por ejemplo, se arrastra el símbolo del disquete hasta un icono representado por una papelera).

La unidad de disco se alimenta mediante cables a partir de la fuente de alimentación del sistema. Y también va conectada mediante un cable a la placa

base. Un diodo LED se ilumina junto a la ranura cuando la unidad está leyendo el disco, como ocurre en el caso del disco duro.

En los disquetes solo se puede escribir cuando la pestaña esta cerrada.

Cabe destacar que el uso de este soporte en la actualidad es escaso o nulo, puesto que se ha vuelto obsoleto teniendo en cuenta los avances que en materia de tecnología se han producido.

Unidad de CD-ROM o "lectora"

La unidad de CD-ROM permite utilizar discos ópticos de una mayor capacidad que los disquetes de 3,5 pulgadas: hasta 700 MB. Ésta es su principal ventaja, pues los CD-ROM se han convertido en el estándar para distribuir sistemas operativos, aplicaciones, etc.

El uso de estas unidades está muy extendido, ya que también permiten leer los discos compactos de audio.

Para introducir un disco, en la mayoría de las unidades hay que pulsar un botón para que salga una especie de bandeja donde se deposita el CD-ROM. Pulsando nuevamente el botón, la bandeja se introduce.

En estas unidades, además, existe una toma para auriculares, y también pueden estar presentes los controles de navegación y de volumen típicos de los equipos de audio para saltar de una pista a otra, por ejemplo.

Una característica básica de las unidades de CD-ROM es la velocidad de lectura, que normalmente se expresa como un número seguido de una «x» (40x, 52x,..). Este número indica la velocidad de lectura en múltiplos de 128 kB/s. Así, una unidad de 52x lee información de 128 kB/s × 52 = 6,656 kB/s, es decir, a 6,5 MB/s.

Unidad de CD-RW (regrabadora) o "grabadora"

Las unidades de CD-ROM son de sólo lectura. Es decir, pueden leer la información en un disco, pero no pueden escribir datos en él.

Una regrabadora puede grabar y regrabar discos compactos. Las características básicas de estas unidades son la velocidad de lectura, de grabación y de regrabación. En los discos regrabables es normalmente menor que en los discos que sólo pueden ser grabados una vez. Las regrabadoras

que trabajan a 8X, 16X, 20X, 24X, etc., permiten grabar los 650, 700 o más megabytes (hasta 900 MB) de un disco compacto en unos pocos minutos. Es habitual observar tres datos de velocidad, según la expresión ax bx cx (*a*:velocidad de lectura; *b*: velocidad de grabación; *c*: velocidad de regrabación).

Unidad de DVD-ROM o "lectora de DVD"

Las unidades de DVD-ROM son aparentemente iguales que las de CD-ROM, pueden leer tanto discos DVD-ROM como CD-ROM. Se diferencian de las unidades lectoras de CD-ROM en que el soporte empleado tiene hasta 17 GB de capacidad, y en la velocidad de lectura de los datos. La velocidad se expresa con otro número de la «x»: 12x, 16x... Pero ahora la x hace referencia a 1,32 MB/s. Así: 16x = 21,12 MB/s.

Las conexiones de una unidad de DVD-ROM son similares a las de la unidad de CD-ROM: placa base, fuente de alimentación y tarjeta de sonido. La diferencia más destacable es que las unidades lectoras de discos DVD-ROM también pueden disponer de una salida de audio digital. Gracias a esta conexión es posible leer películas en formato DVD y escuchar seis canales de audio separados si disponemos de una buena tarjeta de sonido y un juego de altavoces apropiado (subwoofer más cinco satélites).

Lector de tarjetas de memoria

El lector de tarjetas de memoria es un periférico que lee o escribe en soportes de memoria flash. Actualmente, los instalados en computadores (incluidos en una placa o mediante puerto USB),marcos digitales, lectores de DVD y otros dispositivos, suelen leer varios tipos de tarjetas.

Una tarjeta de memoria es un pequeño soporte de almacenamiento que utiliza memoria flash para guardar la información que puede requerir o no baterías (pilas), en los últimos modelos la batería no es requerida, la batería era utilizada por los primeros modelos. Estas memorias son resistentes a los rasguños externos y al polvo que han afectado a las formas previas de almacenamiento portátil, como los CD y los disquetes.

Otros dispositivos de almacenamiento

Otros dispositivos de almacenamiento son las memorias flash o los dispositivos de almacenamiento magnéticos de gran capacidad.

- Memoria flash: Es un tipo de memoria que se comercializa para el uso de aparatos portátiles, como cámaras digitales o agendas electrónicas. El aparato correspondiente o bien un lector de tarjetas, se conecta a la computadora a través del puerto USB o Firewire.

- Discos y cintas magnéticas de gran capacidad: Son unidades especiales que se utilizan para realizar copias de seguridad o respaldo en empresas y centros de investigación. Su capacidad de almacenamiento puede ser de cientos de gigabytes.

- Almacenamiento en línea: Hoy en día también debe hablarse de esta forma de almacenar información. Esta modalidad permite liberar espacio de los equipos de escritorio y trasladar los archivos a discos rígidos remotos provistos que garantizan normalmente la disponibilidad de la información. En este caso podemos hablar de dos tipos de almacenamiento en línea: un almacenamiento de corto plazo normalmente destinado a la transferencia de grandes archivos vía web; otro almacenamiento de largo plazo, destinado a conservar información que normalmente se daría en el disco rígido del ordenador personal.

Restauración de datos

La información almacenada en cualquiera de estos dispositivos debe de disponer de algún mecanismo para restaurar la información, es decir restaurar la información a su estado original en caso de que algún evento no nos permita poder acceder a la información original, siendo necesario acudir a la copia que habíamos realizado anteriormente. Para esta restauración de datos existen diferentes métodos, desde un simple copiar pasando por comandos como el "copy" de DOS, el "cp" de sistemas Linux y Unix, o herramientas de diversos fabricantes..

Recuperación de datos

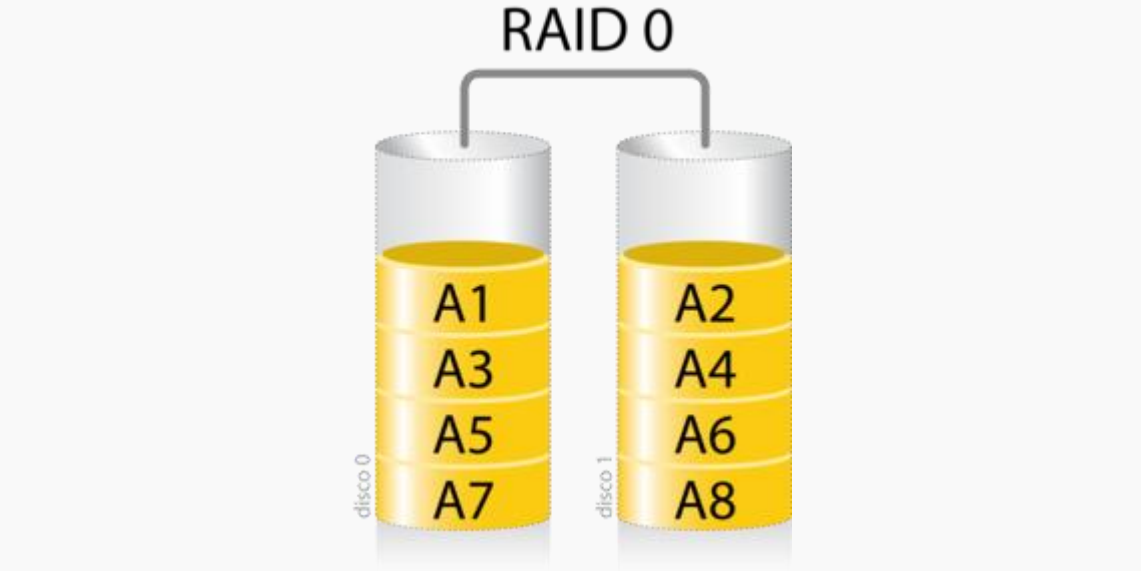
En casos en los que no es posible acceder a la información original, y no disponemos de copia de seguridad o no podemos acceder a ella, existen empresas especializadas que pueden rescatarnos la información de nuestros dispositivos de almacenamiento de información dañados. Estas empresas reparan el medio con el fin de extraer de el la información y después volcarla a otro medio en correcto estado de funcionamiento.

10- Almacenamiento redundante y distribuido: RAID y Centros de Respaldo.

En informática, el acrónimo **RAID**, «conjunto redundante de discos independientes», anteriormente conocido como ***Redundant Array of Inexpensive Disks***, «conjunto redundante de discos baratos») hace referencia a un sistema de almacenamiento que usa múltiples discos duros o SSD entre los que se distribuyen o replican los datos. Dependiendo de su configuración (a la que suele llamarse «nivel»), los beneficios de un RAID respecto a un único disco son uno o varios de los siguientes: mayor integridad, mayor tolerancia a fallos, mayor *throughput* (rendimiento) y mayor capacidad. En sus implementaciones originales, su ventaja clave era la habilidad de combinar varios dispositivos de bajo coste y tecnología más antigua en un conjunto que ofrecía mayor capacidad, fiabilidad, velocidad o una combinación de éstas que un solo dispositivo de última generación y coste más alto.

RAID 0 (Data Striping)

RAID 0 proporciona la fragmentación de discos en todas las unidades del subsistema RAID.
RAID 0 no ofrece redundancia de datos, aunque garantiza el mayor rendimiento de todos los niveles de RAID. RAID 0 divide los datos en bloques más pequeños y a continuación graba cada uno de los bloques en una unidad distinta de la matriz. El tamaño de cada bloque viene determinado por el parámetro de tamaño de franja, que se ha establecido durante la creación del conjunto RAID. RAID 0 ofrece un gran ancho de banda.



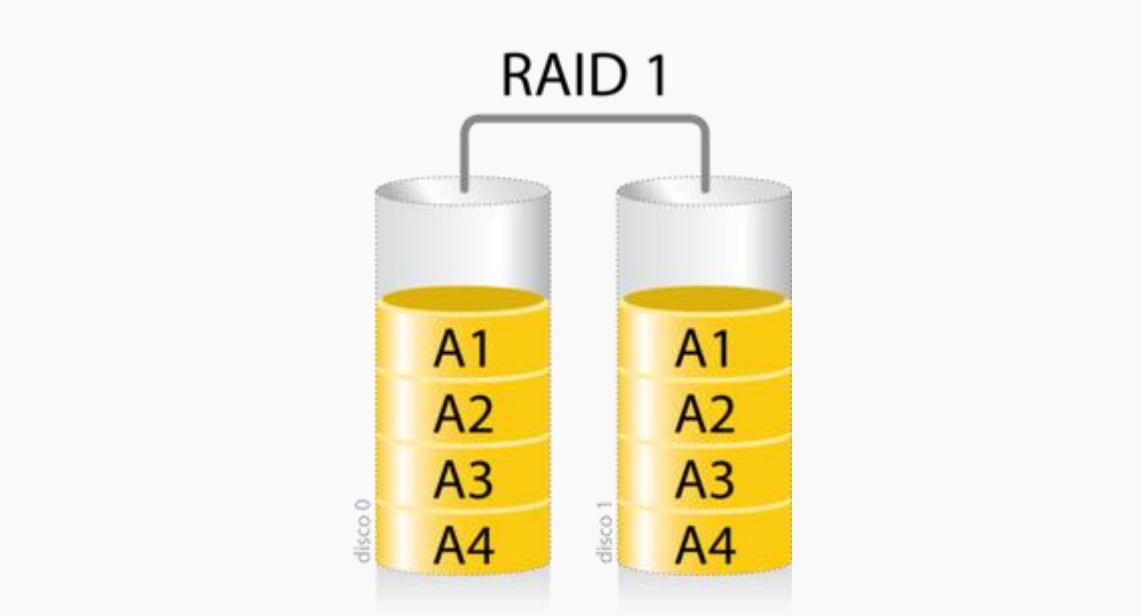
Al dividir un archivo de gran tamaño en bloques más pequeños, PERC4/Di puede utilizar varias unidades para leer o grabar el archivo más rápidamente.

RAID 0 no incluye cálculos de paridad que compliquen la operación de grabación. Esto hace que RAID 0 resulte ideal para aplicaciones que requieren un gran ancho de banda pero que no exigen tolerancia de fallas. RAID 0 también se utiliza para indicar una unidad única o "independiente".

Utilización	RAID 0 ofrece una producción de datos elevada, especialmente en el caso de los archivos de gran tamaño. En cualquier entorno que no requiera tolerancia de fallas.
Ventajas	Proporciona una mejor productividad de los datos en archivos grandes. No hay penalización por pérdida de la capacidad por paridad.
Inconvenientes	No ofrece tolerancia de fallas. En caso de fallo de alguna unidad, todos los datos se pierden.
Unidades	1 a 20

RAID 1

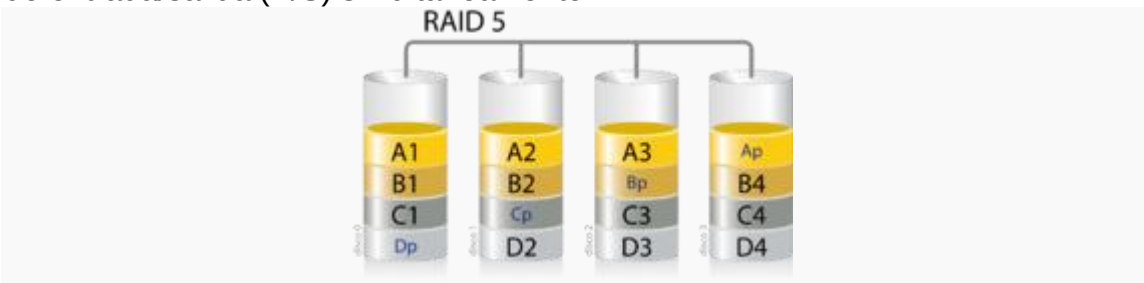
En RAID 1, PERC4/Di duplica todos los datos de una unidad en una segunda unidad. RAID 1 ofrece una redundancia de datos completa, pero a costa de doblar la capacidad de almacenamiento de datos necesaria.



Utilización	Utilice RAID 1 para bases de datos pequeñas o cualquier otro entorno en el que sea necesaria una tolerancia de fallas y una capacidad reducida.
Ventajas	RAID 1 proporciona una redundancia de datos completa. RAID 1 resulta ideal para cualquier aplicación que requiera tolerancia de fallas y una capacidad mínima.
Inconvenientes	RAID 1 requiere el doble de unidades de disco. El rendimiento se deteriora durante la reconstrucción de unidades.
Unidades	2

RAID 5

RAID 5 incluye la fragmentación de discos en el nivel de bloque y la paridad. En RAID 5, la información de paridad se graba en varias unidades. RAID 5 es apto para redes que realizan con frecuencia pequeñas transacciones aleatorias de entrada/salida (E/S) simultáneamente.

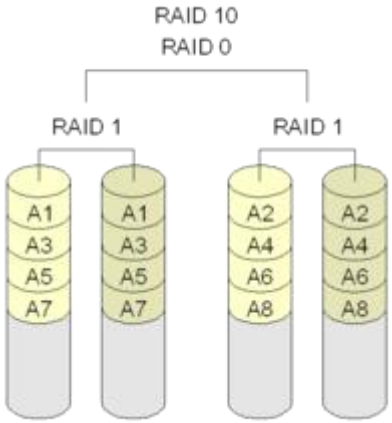


El rendimiento dependerá de la tasa de lectura/escritura: cuanto mayor sea la tasa, mayor será el rendimiento.

Utilización	RAID 5 ofrece una producción de datos elevada, especialmente en el caso de acceso aleatorio limitado. RAID 5 resulta ideal para aplicaciones de procesamiento de transacciones porque cada unidad puede llevar a cabo las operaciones de lectura y grabación independientemente. Si una unidad falla, el controlador RAID utiliza la unidad de paridad para volver a crear toda la información que falta. También se utiliza en ofimática y para servicios al cliente en línea que requieren tolerancia de fallas. Finalmente, se utiliza para cualquier aplicación que necesite una alta velocidad de lectura y menor velocidad de grabación.
Ventajas	Proporciona redundancia de datos y buen rendimiento en la mayoría de entornos.
Inconvenientes	El rendimiento de grabación es considerablemente inferior que RAID 0 o RAID 1. El rendimiento de la unidad de disco se verá reducido cuando otra unidad se esté reconstruyendo. Los entornos que comprenden pocos procesos no tienen tan buen rendimiento porque los gastos de RAID no se compensan con las ganancias del rendimiento derivadas del manejo de procesos simultáneos.
Unidades	3 a 20

RAID 10

RAID 10 es una combinación de RAID 0 y de RAID 1. RAID 10 está formado por franjas a lo largo de unidades duplicadas. RAID 10 divide los datos en bloques más pequeños y, a continuación, fragmenta los bloques de datos para cada conjunto RAID de RAID 1. Cada conjunto RAID de RAID 1 duplica los datos en la otra unidad. El tamaño de cada bloque se determina por el parámetro de tamaño de franja, que se establece durante la creación del conjunto RAID. RAID 10 puede sufrir de uno a cuatro fallos en la unidad y mantener la integridad de los datos si cada disco que ha fallado se encuentra en una matriz RAID 1 diferente. En la tabla 5 se muestra una visión general de RAID 10.



Utilización	RAID 10 funciona mejor con el almacenamiento de datos que obligatoriamente ha de tener un 100% de redundancia de matrices duplicadas además del rendimiento mejorado de E/S de RAID 0 (matrices con franjas). RAID 10 funciona bien con bases de datos de tamaño medio o cualquier entorno que precise de un alto grado de tolerancia de fallas y una capacidad entre moderada y media.
Ventajas	RAID 10 proporciona una alta velocidad de transferencia de datos y una redundancia de datos completa.
Inconvenientes	RAID 10 necesita el doble de unidades que los demás niveles de RAID excepto RAID 1.
Unidades	2n, donde n es mayor que 1. El número máximo de unidades es 16.

11.-Centro de respaldo

Un centro de respaldo es un centro de procesamiento de datos (CPD) específicamente diseñado para tomar el control de otro CPD principal en caso de contingencia.

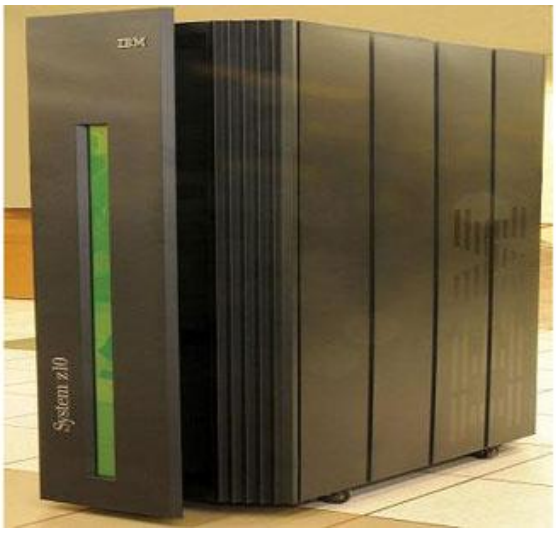
Motivación

Grandes organizaciones, tales como bancos o Administraciones Públicas, no pueden permitirse la pérdida de información ni el cese de operaciones ante un desastre en su centro de proceso de datos. Terremotos, incendios o atentados en estas instalaciones son infrecuentes, pero no improbables. Por este motivo, se suele habilitar un centro de respaldo para absorber las operaciones del CPD principal en caso de emergencia.

Diseño de un centro de respaldo

Un centro de respaldo se diseña bajo los mismos principios que cualquier CPD, pero bajo algunas consideraciones más. En primer lugar, debe elegirse una localización totalmente distinta a la del CPD principal con el objeto de que no se vean ambos afectados simultáneamente por la misma contingencia. Es habitual situarlos entre 20 y 40 kilómetros del CPD principal. La distancia está limitada por las necesidades de telecomunicaciones entre ambos centros.

En segundo lugar, el equipamiento electrónico e informático del centro de respaldo debe ser absolutamente compatible con el existente en el CPD principal. Esto no implica que el equipamiento deba ser exactamente igual. Normalmente, no todos los procesos del CPD principal son críticos. Por este motivo no es necesario duplicar todo el equipamiento. Por otra parte, tampoco se requiere el mismo nivel de servicio en caso de emergencia. En consecuencia, es posible utilizar hardware menos potente. La pecera de un centro de respaldo recibe estas denominaciones en función de su equipamiento:



- **Sala blanca:** cuando el equipamiento es exactamente igual al existente en el CPD principal.
- **Sala de back-up:** cuando el equipamiento es similar pero no exactamente igual.

En tercer lugar, el equipamiento software debe ser idéntico al existente en el CPD principal. Esto implica exactamente las mismas versiones y parches del software de base y de las aplicaciones corporativas que estén en explotación

en el CPD principal. De otra manera, no se podría garantizar totalmente la continuidad de operación.

Por último, pero no menos importante, es necesario contar con una réplica de los mismos datos con los que se trabaja en el CPD original. Este es el problema principal de los centros de respaldo, que se detalla a continuación.

El sincronismo de datos

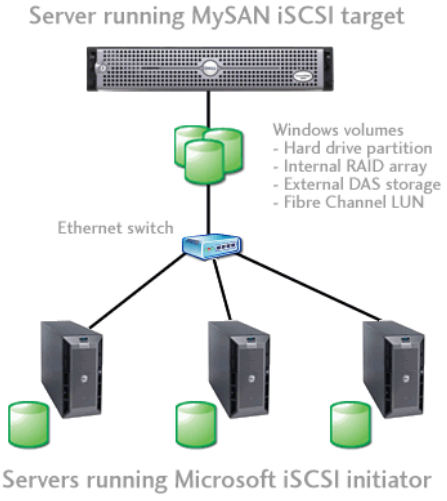
Existen dos políticas o aproximaciones a este problema:

- Copia síncrona de datos: Se asegura que todo dato escrito en el CPD principal también se escribe en el centro de respaldo antes de continuar con cualquier otra operación.
- Copia asíncrona de datos: No se asegura que todos los datos escritos en el CPD principal se escriban inmediatamente en el centro de respaldo, por lo que puede existir un desfase temporal entre unos y otros.

La copia asíncrona puede tener lugar fuera de línea. En este caso, el centro de respaldo utiliza la última copia de seguridad existente del CPD principal. Esto lleva a la pérdida de los datos de operaciones de varias horas (como mínimo) hasta días (lo habitual). Esta opción es viable para negocios no demasiado críticos, donde es más importante la continuidad del negocio que la pérdida de datos. Por ejemplo, en cadenas de supermercados o pequeños negocios. No obstante, es inviable en negocios como la banca, donde es impensable la pérdida de una sola transacción económica.

En los demás casos, la política de copia suele descansar sobre la infraestructura de almacenamiento corporativo. Generalmente, se trata de redes SAN y cabinas de discos con suficiente inteligencia como para implementar dichas políticas.

Tanto para la copia síncrona como asíncrona, es necesaria una extensión de la red de almacenamiento entre ambos centros. Es decir, un enlace de telecomunicaciones entre el CPD y el centro de respaldo. En caso de copia asíncrona es imprescindible que dicho enlace goce de baja latencia. Motivo por el que se suele emplear un enlace de fibra óptica, que limita la distancia máxima a decenas de kilómetros. Existen dos tecnologías factibles para la copia de datos en centros de respaldo:



- iSCSI.
- Fibre Channel.

La copia síncrona es esencial en negocios como la banca, donde no es posible la pérdida de ninguna transacción. La copia asíncrona es viable en la mayoría de los casos, ya que el desfase temporal de la copia se limita a unos pocos minutos.

El centro de respaldo en contexto

Un centro de respaldo por sí sólo no basta para hacer frente a una contingencia grave. Es necesario disponer de un Plan de Contingencias corporativo. Este plan contiene tres subplanes que indican las medidas técnicas, humanas y organizativas necesarias en tres momentos clave:

- Plan de respaldo: Contempla las actuaciones necesarias antes de que se produzca un incidente. Esencialmente, mantenimiento y prueba de las medidas preventivas.
- Plan de emergencia: Contempla las actuaciones necesarias durante un incidente.
- Plan de recuperación: Contempla las actuaciones necesarias después de un incidente. Básicamente, indica cómo volver a la operación normal.

12.- Almacenamiento remoto: SAN, NAS y almacenamiento clouding.

SAN

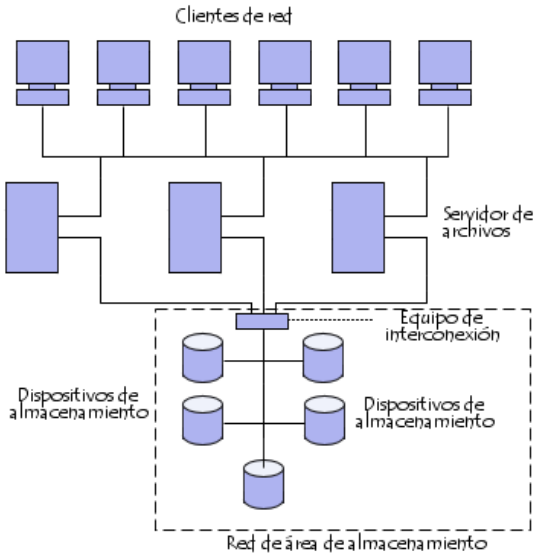
Introducción a SAN

Una "**SAN**" (*Red de área de almacenamiento*) es una red de almacenamiento integral. Se trata de una arquitectura completa que agrupa los siguientes elementos:

- Una red de alta velocidad de canal de fibra o SCSI
- Un equipo de interconexión dedicado (conmutadores, puentes, etc.)
- Elementos de almacenamiento de red (discos duros)

Presentación de una SAN

Una SAN es una red dedicada al almacenamiento que está conectada a las redes de comunicación de una compañía. Además de contar con interfaces de red tradicionales, los equipos con acceso a la SAN tienen una interfaz de red específica que se conecta a la SAN.



Ventajas y desventajas

El rendimiento de la SAN está directamente relacionado con el tipo de red que se utiliza. En el caso de una red de canal de fibra, el ancho de banda es de aproximadamente 100 megabytes/segundo (1.000 megabits/segundo) y se puede extender aumentando la cantidad de conexiones de acceso.

La capacidad de una SAN se puede extender de manera casi ilimitada y puede alcanzar cientos y hasta miles de terabytes.

Una SAN permite compartir datos entre varios equipos de la red sin afectar el rendimiento porque el tráfico de SAN está totalmente separado del tráfico de usuario. Son los servidores de aplicaciones que funcionan como una interfaz entre la red de datos (generalmente un canal de fibra) y la red de usuario (por lo generalEthernet).
Por otra parte, una SAN es mucho más costosa que una NAS ya que la primera es una arquitectura completa que utiliza una tecnología que todavía es muy cara. Normalmente, cuando una compañía estima el TCO (Coste total de

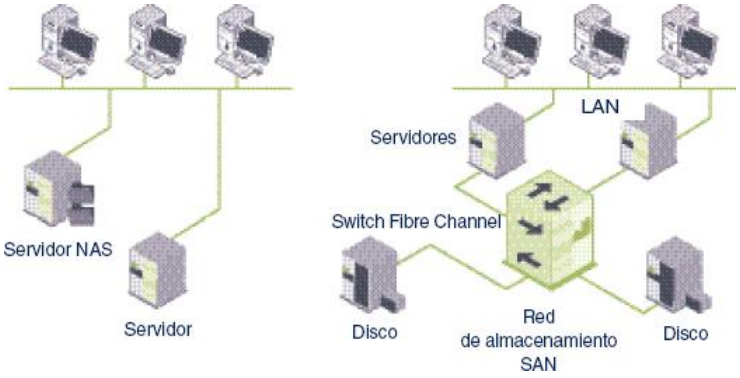
propiedad) con respecto al coste por byte, el coste se puede justificar con más facilidad.

NAS

Introducción al NAS

Un "**NAS**" (*Almacenamiento conectado a red*) es un dispositivo de almacenamiento de red. Un NAS es un servidor de almacenamiento que se puede conectar fácilmente a la red de una compañía para asistir al servidor de archivos y proporcionar espacio de almacenamiento tolerante a fallas.

Presentación de un NAS



Un NAS es un servidor separado que tiene su propio sistema operativo y un software de configuración parametrizado con valores predeterminados que se adaptan a la mayoría de los casos.
Por lo general, posee su propio sistema de archivos que aloja al sistema operativo, así como también una serie de discos independientes que se utilizan para alojar los datos que se van a guardar.

Alojamiento web en la nube (*cloud hosting*)

El alojamiento web en la "nube" (*cloud hosting*) está basado en las tecnologías más innovadoras que permiten a un gran número de máquinas actuar como un sistema conectadas a un grupo de medios de almacenamiento, tiene ventajas considerables sobre las soluciones de *web hosting* tradicionales tal como el uso de recursos. La seguridad de un sitio web alojado en la "nube" (*cloud*) está garantizada por numerosos servidores en lugar de sólo uno. La tecnología de computación en la nube también elimina cualquier limitación física para el crecimiento en tiempo real y hace que la solución sea extremadamente flexible.

Principales servicios de clouding:

En los últimos años el desarrollo de nuevas tecnologías y la continua expansión de internet ha permitido la aparición de las llamadas aplicaciones en la nube que, por definirlas de una manera sencilla, se trata de aplicaciones ofrecidas desde internet (que por tanto no requiere de ningún tipo de instalación ni de conocimiento previo por parte del usuario) y a través del navegador.

Una de las opciones más interesantes, en cuanto a aplicaciones en la nube se refiere, son las enfocadas al respaldo y sincronización de datos. En este monográfico hablaremos de cinco servicios distintos de almacenamiento en la nube:

1. Dropbox.
2. Windows Live Mesh/Skydrive.
3. Ubuntu One.
4. ZumoDrive.
5. ADrive.

13.- Políticas de almacenamiento.

No es ninguna novedad el valor que tiene la información y los datos para nuestros negocios. Lo que resulta increíble de esto es la falta de precauciones que solemos tener al confiar al núcleo de nuestros negocios
al sistema de almacenamiento de lo que en la mayoría de los casos resulta ser una computadora pobremente armada tanto del punto de vista
de hardware como de software.

Si el monitor, la memoria e incluso la CPU de nuestro computador dejan de funcionar, simplemente lo reemplazamos, y no hay mayores dificultades. Pero si falla el disco duro, el daño puede ser irreversible, puede significar la pérdida total de nuestra información. Es principalmente por esta razón, por la que debemos respaldar la información importante. Imaginémonos ahora lo que pasaría si esto le sucediera a una empresa, las pérdidas económicas podría ser cuantiosas. Los negocios de todos los tipos y tamaños confían en la información computarizada para facilitar su operación. La pérdida de información provoca un daño de fondo:

- Pérdida de oportunidades de negocio
- Clientes decepcionados
- Reputación perdida
- Etc.

La tecnología no está exenta de fallas o errores, y los respaldos de información son utilizados como un plan de contingencia en caso de que una falla o error se presente.

Asimismo, hay empresas, que por la naturaleza del sector en el que operan (por ejemplo Banca) no pueden permitirse la más mínima interrupción informática.

Las interrupciones se presentan de formas muy variadas: virus informáticos, fallos de electricidad, errores de hardware y software, caídas de red, hackers, errores humanos, incendios, inundaciones, etc. Y aunque no se pueda prevenir cada una de estas interrupciones, la empresa sí puede prepararse para evitar las consecuencias que éstas puedan tener sobre su negocio. Del tiempo que tarde en reaccionar una empresa dependerá la gravedad de sus consecuencias.

Riesgo a los cuales se encuentran inmersos los Sistemas de Información

Fuente: IBM

Además, podríamos recordar una de las leyes de mayor validez en la informática, la "Ley de Murphy":

- Si un archivo puede borrarse, se borrará.
- Si dos archivos pueden borrarse, se borrará el más importante.
- Si tenemos una copia de seguridad, no estará lo suficientemente actualizada.

La única solución es tener copias de seguridad, actualizarlas con frecuencia y esperar que no deban usarse.

Respaldar la información significa copiar el contenido lógico de nuestro sistema informático a un medio que cumpla con una serie de exigencias:

1. Ser confiable: Minimizar las probabilidades de error.
Muchos medios magnéticos como las cintas de respaldo, los disquetes, o discos duros tienen probabilidades de error o son particularmente sensibles a campos magnéticos, elementos todos que atentan contra la información que hemos respaldado allí.
Otras veces la falta de confiabilidad se genera al rehusar los medios magnéticos. Las cintas en particular tienen una vida útil concreta. Es común que se subestime este factor y se reutilicen más allá de su vida útil, con resultados nefastos, particularmente porque vamos a descubrir su falta de confiabilidad en el peor momento: cuando necesitamos RECUPERAR la información.

2. Estar fuera de línea, en un lugar seguro: Tan pronto se realiza el respaldo de información, el soporte que almacena este respaldo debe ser desconectado de la computadora y almacenado en un lugar seguro tanto desde el punto de vista de sus requerimientos técnicos como humedad, temperatura, campos

magnéticos, como de su seguridad física y lógica. No es de gran utilidad respaldar la información y dejar el respaldo conectado a la computadora donde potencialmente puede haber un ataque de cualquier índole que lo afecte.

3. La forma de recuperación sea rápida y eficiente*:* Es necesario probar la confiabilidad del sistema de respaldo no sólo para respaldar sino que también para recuperar. Hay sistemas de respaldo que aparentemente no tienen ninguna falla al generar el respaldo de la información pero que fallan completamente al recuperar estos datos al sistema informático. Esto depende de la efectividad y calidad del sistema que realiza el respaldo y la recuperación.

Esto nos lleva a que un sistema de respaldo y recuperación de información tiene que ser probado y eficiente.

Seguridad física y lógica:

Puede llegar a ser necesario eliminar los medios de entrada/salida innecesarios en algunos sistemas informáticos, tales como disqueteras y cdroms para evitar posible infecciones con virus traídos desde el exterior de la empresa por el personal, o la extracción de información de la empresa.

Las copias de seguridad son uno de los elementos más importantes y que requieren mayor atención a la hora de definir las medidas de seguridad del sistema de información, la misión de las mismas es la recuperación de los ficheros al estado inmediatamente anterior al momento de realización de la copia.

La realización de las copias de seguridad se basará en un análisis previo del sistema de información, en el que se definirán las medidas técnicas que puedan condicionar la realización de las copias de seguridad, entre los que se encuentran:

Control de acceso lógico:

14.- Identificación, autenticación y autorización

Identificación

La identificación es el proceso por el cual se comprueba que un usuario está autorizado a acceder a una serie de recursos. Este proceso de identificación se realiza normalmente mediante un nombre de usuario y contraseña; aunque actualmente también se utilizan los sistemas biométricos para realizar los procesos de identificación.

Autenticación

La autenticación es la situación en la cual se puede verificar que un documento ha sido elaborado (o pertenece) a quien el documento dice.

Aplicado a la verificación de la identidad de un usuario, la autenticación se produce cuando el usuario puede aportar algún modo de que se pueda verificar que dicha persona es quien dice ser, a partir de ese momento se considera un usuario autorizado.

Otra manera de definirlo seria, la capacidad de determinar si una determinada lista de personas ha establecido su reconocimiento sobre el contenido de un mensaje.

Autorización

En ingeniería de seguridad y seguridad informática, la **autorización** es una parte del sistema operativo que protege los recursos del sistema permitiendo que sólo sean usados por aquellos consumidores a los que se les ha concedido autorización para ello. Los recursos incluyen archivos y otros objetos de dato, programas, dispositivos y funcionalidades provistas por aplicaciones. Ejemplos de consumidores son usuarios del sistema, programas y otros dispositivos.

15- Política de contraseñas.

Contraseñas

Al conectarse a un sistema informático, generalmente se debe ingresar: un **nombre de registro** o **nombre de usuario** y una **contraseña** para acceder. Este par *nombre de registro/contraseña* forma la clave para tener acceso al sistema.
Mientras que al nombre de registro generalmente lo brinda el sistema o el administrador de forma automática, el usuario casi siempre tiene la libertad de elegir la contraseña. La mayoría de los usuarios, como piensan que no tienen ninguna información secreta que proteger, usan una contraseña fácil de recordar (por ejemplo, su nombre de registro, el nombre de su pareja o su fecha de nacimiento).

Y aunque los datos en la cuenta de un usuario puedan no ser estratégicos, tener acceso a la cuenta puede significar una puerta abierta a todo el sistema. Cuando un hacker tiene acceso a la cuenta de un equipo, puede extender su campo de acción al obtener la lista de usuarios autorizados a conectarse al equipo. Un hacker puede probar un gran número de contraseñas generadas al azar con herramientas destinadas a tal fin o con un diccionario (o puede combinar ambos). Si consigue la contraseña del administrador, obtiene todos los permisos sobre el equipo.

Además, es posible que el hacker tenga acceso a la red local desde la red de un equipo, lo que significa que puede trazar un mapa de los otros servidores al trabajar desde el equipo al que tiene acceso.

Las contraseñas de los usuarios son la primera línea de defensa contra los ataques, por eso es necesario definir una política de contraseñas para que los usuarios elijan contraseñas lo suficientemente seguras.

Métodos de ataque

Muchos sistemas están configurados para bloquear transitoriamente la cuenta de un usuario después de haber intentado conectarse sin éxito una cierta cantidad de veces. En consecuencia, es difícil para un hacker infiltrarse en un sistema de esta manera.

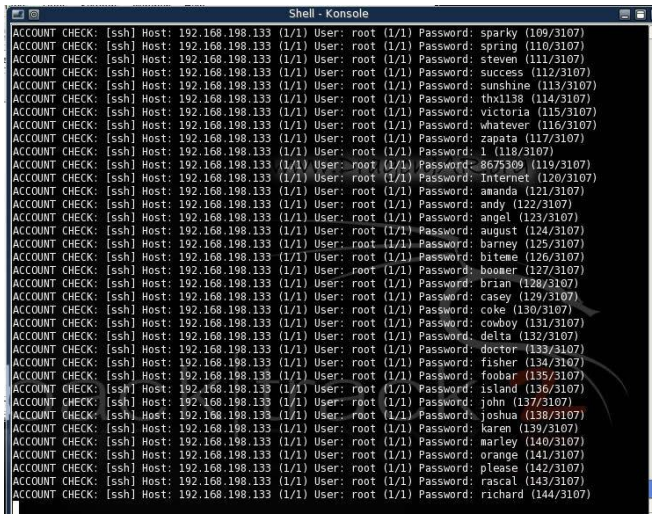
Sin embargo, puede usar este mecanismo de autodefensa para bloquear todas las cuentas de usuario para accionar una denegación de servicio.

En la mayoría de los sistemas, las contraseñas se guardan cifradas en un archivo o una base de datos.

Sin embargo, si un hacker tiene acceso al sistema y a este archivo, puede tratar de craquear una contraseña de usuario en particular o las contraseñas de todas las cuentas de usuario.

Ataque de fuerza bruta

El término "**ataque de fuerza bruta**" se usa para referirse al craqueo de una contraseña al probar todas las posibles combinaciones. Existe una variedad de herramientas para todos los sistemas operativos que permite realizar este tipo de procedimiento. Los administradores de sistema usan estas herramientas para probar la solidez de sus contraseñas de usuario, pero a veces los hackers las usurpan para infiltrarse en sus sistemas informáticos.



Ataque de diccionario

Las herramientas para el ataque de fuerza pueden demorar horas o hasta días de cálculos, incluso con equipos que cuentan con potentes procesadores. Una solución alternativa es llevar a cabo un "**ataque de diccionario**". En la práctica, los usuarios generalmente eligen contraseñas que tengan un significado. Con este tipo de ataque, tales contraseñas se pueden craquear en sólo unos minutos.

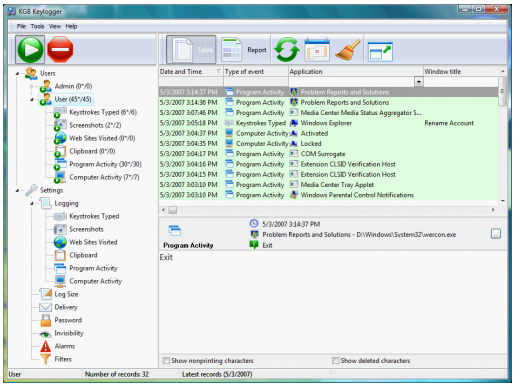
Ataque híbrido

El último ataque de este tipo, el "**ataque híbrido**", específicamente apunta a contraseñas compuestas por una palabra tradicional seguida de un número o una letra (como "marshal6"). Es una combinación entre el ataque de fuerza bruta y el de diccionario.

Existen métodos que también permiten que un hacker obtenga contraseñas de usuario:

- Los registradores de pulsaciones son programas de software que, al instalarlos en la estación de trabajo del usuario, registran lo que se pulsa en el teclado. Los sistemas operativos recientes presentan búfers protegidos

que permiten retener la contraseña durante un tiempo y a los que sólo el sistema puede acceder.



- La ingeniería social consiste en aprovecharse de la ingenuidad de la gente para obtener información. Así, un hacker puede acceder a la contraseña de una persona al hacerse pasar por un administrador de red o, a la inversa, puede contactar al soporte técnico y pedir reinicializar la contraseña usando como pretexto una situación de emergencia.
- El **espionaje** es el método más antiguo utilizado. En este caso, un pirata sólo tiene que observar los papeles que estén alrededor de la pantalla o debajo del teclado del usuario para obtener la contraseña. Si el pirata es alguien en quien la víctima confía, sólo tiene que mirar sobre el hombro de esa persona cuando ingrese la contraseña para verla o adivinarla.

Para gestionar correctamente la seguridad de las contraseñas, desde el Instituto Nacional de Tecnologías de la Comunicación (INTECO) se recomienda a los usuarios tener en cuenta las siguientes pautas para la creación y establecimiento de contraseñas seguras:

Política y acciones para construir contraseñas seguras:

1. Se deben utilizar al menos 8 caracteres para crear la clave. Según un estudio de la Universidad de Wichita, el número medio de caracteres por contraseña para usuarios entre 18 y 58 años habituales de Internet es de 7. Esto conlleva el peligro de que el tiempo para descubrir la clave se vea reducido a minutos o incluso segundos. Sólo un 36% de los encuestados indicaron que utilizaban un número de caracteres de 7 o superior.

2. Se recomienda utilizar en una misma contraseña dígitos, letras y caracteres especiales.

3. Es recomendable que las letras alternen aleatoriamente mayúsculas y minúsculas. Hay que tener presente el recordar qué letras van en mayúscula y cuáles en minúscula. Según el mismo estudio, el 86% de los usuarios utilizan sólo letras minúsculas, con el peligro de que la contraseña sea descubierta por un atacante casi instantáneamente.

4. Elegir una contraseña que pueda recordarse fácilmente y es deseable que pueda escribirse rápidamente, preferiblemente, sin que sea necesario mirar el teclado.

5. Las contraseñas hay que cambiarlas con una cierta regularidad. Un 53% de los usuarios no cambian nunca la contraseña salvo que el sistema le obligue a ello cada cierto tiempo. Y, a la vez, hay que procurar no generar reglas secuenciales de cambio. Por ejemplo, crear una nueva contraseña mediante un incremento secuencial del valor en relación a la última contraseña. P. ej.: pasar de “01Juitnx” a “02Juitnx”.

6. Utilizar signos de puntuación si el sistema lo permite. P. ej.: “Tr-.3Fre”. En este caso de incluir otros caracteres que no sean alfa-numéricos en la contraseña, hay que comprobar primero si el sistema permite dicha elección y cuáles son los permitidos.
Dentro de ese consejo se incluiría utilizar símbolos como: ! " # $ % & ' ( ) * + , - . / : ; < = > ? @ [\ ] ^ _ ` { | } ~

7. Existen algunos trucos para plantear una contraseña que no sea débil y se pueda recordar más fácilmente. Por ejemplo se pueden elegir palabras sin sentido pero que sean pronunciables, etc. Nos podemos ayudar combinando esta selección con números o letras e introducir alguna letra mayúscula. Otro método sencillo de creación de contraseñas consiste en elegir la primera letra de cada una de las palabras que componen una frase conocida, de una canción, película, etc. Con ello, mediante esta sencilla mnemotecnia es más sencillo recordarla. Vg: de la frase “Comí mucho chocolate el domingo 3, por la tarde”, resultaría la contraseña: “cmCeD3-:xLt”. En ella, además, se ha introducido alguna mayúscula, se ha cambiado el “por” en una “x” y, si el sistema lo permite, se ha colocado algún signo de puntuación (-).

Acciones que deben evitarse en la gestión de contraseñas seguras:

1. Se debe evitar utilizar la misma contraseña siempre en todos los sistemas o servicios. Por ejemplo, si se utilizan varias cuentas de correo, se debe recurrir a contraseñas distintas para cada una de las cuentas. Un 55% de los usuarios indican que utilizan siempre o casi siempre la misma contraseña para múltiples sistemas, y un 33% utilizan una variación de la misma contraseña.

2. No utilizar información personal en la contraseña: nombre del usuario o de sus familiares, ni sus apellidos, ni su fecha de nacimiento. Y, por supuesto, en ninguna ocasión utilizar datos como el DNI o número de teléfono.

3. Hay que evitar utilizar secuencias básicas de teclado (por ejemplo: ”qwerty”, “asdf” o las típicas en numeración: “1234” ó “98765”)

4. No repetir los mismos caracteres en la misma contraseña. (ej.: “111222”).

5. Hay que evitar también utilizar solamente números, letras mayúsculas o minúsculas en la contraseña.

6. No se debe utilizar como contraseña, ni contener, el nombre de usuario asociado a la contraseña.

7. No utilizar datos relacionados con el usuario que sean fácilmente deducibles, o derivados de estos. (ej: no poner como contraseña apodos, el nombre del actor o de un personaje de ficción preferido, etc.).

8. No escribir ni reflejar la contraseña en un papel o documento donde quede constancia de la misma. Tampoco se deben guardar en documentos de texto dentro del propio ordenador o dispositivo (ej: no guardar las contraseñas de las tarjetas de débito/crédito en el móvil o las contraseñas de los correos en documentos de texto dentro del ordenador),

9. No se deben utilizar palabras que se contengan en diccionarios en ningún idioma. Hoy en día existen programas de ruptura de claves que basan su ataque en probar una a una las palabras que extraen de diccionarios: Este método de ataque es conocido como “ataque por diccionario”.

10. No enviar nunca la contraseña por correo electrónico o en un sms. Tampoco se debe facilitar ni mencionar en una conversación o comunicación de cualquier tipo.

11. Si se trata de una contraseña para acceder a un sistema delicado hay que procurar limitar el número de intentos de acceso, como sucede en una tarjeta de crédito y cajeros, y que el sistema se bloquee si se excede el número de intentos fallidos permitidos. En este caso debe existir un sistema de recarga de la contraseña o “vuelta atrás”.

12. No utilizar en ningún caso contraseñas que se ofrezcan en los ejemplos explicativos de consucción de contraseñas robustas.

13. No escribir las contraseñas en ordenadores de los que se desconozca su nivel de seguridad y puedan estar monitorizados, o en ordenadores de uso público (bibliotecas, cibercafés, telecentros, etc.). tr

14. Cambiar las contraseñas por defecto proporcionadas por desarrolladores/fabricantes.

Auditorias de seguridad informática.

16- Concepto. Tipos de auditorias.

La auditoría en informática es la revisión y la evaluación de los controles, sistemas, procedimientos de informática; de los equipos de cómputo, su utilización, eficiencia y seguridad, de la organización que participan en el procesamiento de la información, a fin de que por medio del señalamiento de cursos alternativos se logre una utilización más eficiente y segura de la información que servirá para una adecuada toma de decisiones.

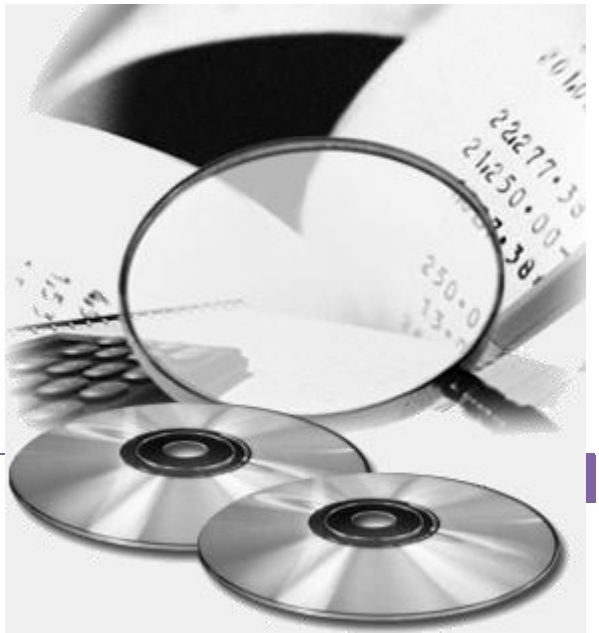
La auditoría en informática deberá comprender no sólo la evaluación de los equipos de cómputo, de un sistema o procedimiento específico, sino que además habrá de evaluar los sistemas de información en general desde sus entradas, procedimientos, controles, archivos, seguridad y obtención de información.

La auditoría en informática es de vital importancia para el buen desempeño de los sistemas de información, ya que proporciona los controles necesarios para que los sistemas sean confiables y con un buen nivel de seguridad. Además debe evaluar todo (informática, organización de centros de información, hardware y software).

Tipos de Auditoría informática

Dentro de la auditoría informática destacan los siguientes tipos (entre otros):

- **Auditoría de la gestión:** la contratación de bienes y servicios, documentación de los programas, etc.
- **Auditoría legal del Reglamento de Protección de Datos**: Cumplimiento legal de las medidas de seguridad exigidas por el Reglamento de desarrollo de la Ley Orgánica de Protección de Datos.
- **Auditoría de los datos**: Clasificación de los datos, estudio de las aplicaciones y análisis de los flujogramas.
- **Auditoría de las bases de datos**: Controles de acceso, de actualización, de integridad y calidad de los datos.



- **Auditoría de la seguridad**: Referidos a datos e información verificando disponibilidad, integridad, confidencialidad, autenticación y no repudio.
- **Auditoría de la seguridad física**: Referido a la ubicación de la organización, evitando ubicaciones de riesgo, y en algunos casos no revelando la situación física de esta. También está referida a las protecciones externas (arcos de seguridad, CCTV, vigilantes, etc.) y protecciones del entorno.
- **Auditoría de la seguridad lógica**: Comprende los métodos de autenticación de los sistemas de información.
- **Auditoría de las comunicaciones**. Se refiere a la auditoria de los procesos de autenticación en los sistemas de comunicación.
- **Auditoría de la seguridad en producción**: Frente a errores, accidentes y fraudes.

17- Pruebas y herramientas de auditoria informática.

Las herramientas tecnológicas son ampliamente utilizadas en el proceso de auditoría y la captación de evidencias, actualmente en el mundo profesional es impredecible el uso de tecnología informática.

HERRAMIENTAS TECNOLOGICAS

El procesamiento electrónico de datos sirve al contador público para la determinación de la calidad de la información, permite realizar un procesos de contabilización, revisión y auditoria más selectivo y penetrante de las actividades y procedimientos relativos aun copioso volumen de transacciones.

ACL

ACL es la herramienta de software preferida por los profesionales de lasfinanzas y auditoría para extraer y analizar datos, detectar fraudes y lograr unmonitoreo continuo

VENTAJAS DE ACL

Análisis datos más rápido y eficientemente.
Produce informes claros.
Identifica tendencias, indica de excepciones con toda precisión
Localiza errores y posibles fraudes.

Identifica problemas de control y garantiza el cumplimiento de los estándares.
Análisis interactivo, con resultados inmediatos.
Rapidez y facilidad de uso, lo que permite el análisis de grandes volúmenes de información

AUTOAUDIT

Es una herramienta dirigida al departamento de auditoría, que permite realizar una planificación de Auditorías en función de Evaluación de Riesgos, siguiendo metodologías de evaluación vertical y/o por proceso. Soportando todo el proceso y flujo de trabajo, desde la fase de planificación, pasando por el trabajo de campo, hasta la preparación del informe final.

BackTrack

BackTrack es una distribución GNU/Linux en formato LiveCD pensada y diseñada para la auditoría de seguridad y relacionada con la seguridad informática en general.

Apex SQL Audit provee

Apex SQL Audit provee una herramienta de auditoría activa para empresas que necesitan auditar bases de datos Microsoft SQL Server.
Apex SQL Audit, es la solución perfecta de auditoría activa para SQL Server.

AUDITOR ASSISTANT

Un completo sistema integrado de administración de auditorías que le ayuda a realizar, revisar y controlar su actividad de auditoría de manera más eficiente.

El entorno flexible de Auditor Assistant se puede adaptar para adecuarse al proceso de auditoría y el cambiante ambiente corporativo.

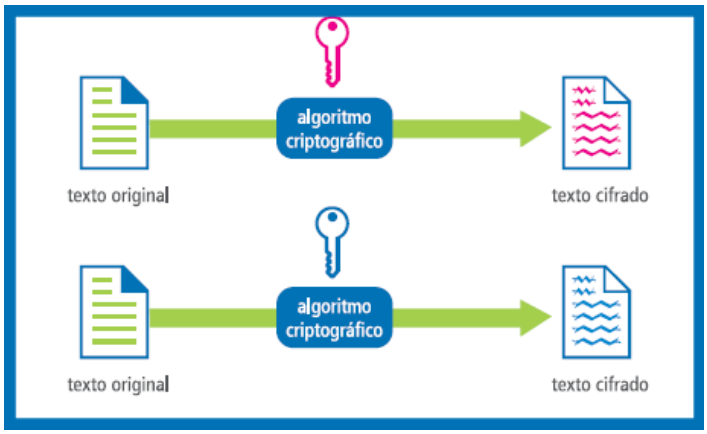
Criptografía.

18- Objetivos. Conceptos. Historia.

Objetivo de la criptografia

En esencia la criptografía trata de enmascarar las representaciones caligráficas de una lengua, de forma discreta. Si bien, el área de estudio científico que se encarga de ello es la Criptología.

Para ello existen distintos métodos. Por ejemplo enmascarar las referencias originales de la lengua por un método de conversión gobernado por un algoritmo que permita el proceso inverso o descifrado de la información. El uso de esta u otras técnicas, permite un intercambio de mensajes que sólo puedan ser leídos por los destinatarios designados como 'coherentes'. Un destinatario coherente es la persona a la que el mensaje se le dirige con intención por parte del remitente. Así pues, el destinatario coherente conoce el discretismo usado para el enmascaramiento del mensaje. Por lo que, o bien posee los medios para someter el mensaje criptográfico al proceso inverso, o puede razonar e inferir el proceso que lo convierta en un mensaje de acceso público. En ambos casos, no necesita usar técnicas criptoanalíticas.



Un ejemplo cotidiano de criptografía es el que usamos cuando mandamos una carta. El mensaje origen queda enmascarado por una cubierta denominada sobre, la cual declara el destinatario coherente, que además conoce el proceso inverso para hacer público el mensaje contenido en el sobre.

Hay procesos más elaborados que, por decirlo de alguna manera, el mensaje origen trata de introducir cada letra usada en un 'sobre' distinto. Por ejemplo, la frase 'texto de prueba', pudiera estar representada por la siguiente notación cifrada: CF, F0, 114, 10E, 106, 72, F3, F6, 75, 10C, 111, 118, FB, F6, F5. El 'sobre' usado es de notación hexadecimal, si bien, el cálculo hexadecimal es de acceso público, no se puede decir que sea un mensaje discreto, ahora, si el resultado de la notación hexadecimal (como es el caso para el ejemplo) es consecuencia de la aplicación de un 'método' de cierre del 'sobre' (como lo es la cola de sellado, o el lacre en las tradicionales cartas), el destinatario debe de conocer la forma de abrirlo sin deteriorar el mensaje origen. En otras palabras, debe de conocer la contraseña. Para el ejemplo, la contraseña es '12345678'.

Conceptos

La palabra criptografía es un término genérico que describe todas las técnicas que permiten cifrar mensajes o hacerlos ininteligibles sin recurrir a una acción específica. El verbo asociado es cifrar.

La criptografía se basa en la aritmética: En el caso de un texto, consiste en transformar las letras que conforman el mensaje en una serie de números (en forma de bits ya que los equipos informáticos usan el sistema binario) y luego realizar cálculos con estos números para:

•Modificarlos y hacerlos incomprensibles. El resultado de esta modificación (el mensaje cifrado) se llama texto cifrado, en contraste con el mensaje inicial, llamado texto simple.

•Asegurarse de que el receptor pueda descifrarlos. El hecho de codificar un mensaje para que sea secreto se llama cifrado. El método inverso, que consiste en recuperar el mensaje original, se llama descifrado.

El cifrado normalmente se realiza mediante una clave de cifrado y el descifrado requiere una clave de descifrado. Las claves generalmente se dividen en dos tipos:

1.-Las claves simétricas: son las claves que se usan tanto para el cifrado como para el descifrado. En este caso hablamos de cifrado simétrico o cifrado con clave secreta.

2.-Las claves asimétricas: son las claves que se usan en el caso del cifrado asimétrico (también llamado cifrado con clave pública). En este caso, se usa una clave para el cifrado y otra para el descifrado. En inglés, el término decryption (descifrado) también se refiere al acto de intentar descifrar en forma ilegítima el mensaje (ya conozca o no el atacante la clave de descifrado). Cuando el atacante no conoce la clave de descifrado, hablamos de criptanálisis o criptoanálisis (también se usa el término decodificación).

La criptología es la ciencia que estudia los aspectos científicos de estas técnicas, es decir, combina la criptografía y el criptoanálisis.

Las dos técnicas más sencillas de *cifrado*, en la criptografía clásica, son la *sustitución* (que supone el cambio de significado de los elementos básicos

del mensaje -las letras, los dígitos o los símbolos-) y la *transposición* (que supone una reordenación de los mismos); la gran mayoría de las *cifras* clásicas son combinaciones de estas dos operaciones básicas.

El *descifrado* es el proceso inverso que recupera el *texto plano* a partir del *criptograma* y la *clave*. El *protocolo criptográfico* especifica los detalles de cómo se utilizan los *algoritmos* y las *claves* (y otras operaciones primitivas) para conseguir el efecto deseado. El conjunto de *protocolos*, *algoritmos de cifrado*, procesos de gestión de claves y actuaciones de los usuarios, es lo que constituyen en conjunto un *criptosistema*, que es con lo que el usuario final trabaja e interactúa.

Existen dos grandes grupos de *cifras*: los algoritmos que usan una única *clave* tanto en el proceso de *cifrado* como en el de *descifrado*, y los que emplean una *clave* para *cifrar* mensajes y una clave distinta para *descifrarlos*. Los primeros se denominan *cifras simétricas*, de *clave simétrica* o de *clave privada*, y son la base de los algoritmos de cifrado clásico. Los segundos se denominan *cifras asimétricas*, de *clave asimétrica* o de *clave pública* y forman el núcleo de las técnicas de cifrado modernas.

En el lenguaje cotidiano, la palabra *código* se usa de forma indistinta con *cifra*. En la jerga de la criptografía, sin embargo, el término tiene un uso técnico especializado: los *códigos* son un método de criptografía clásica que consiste en sustituir unidades textuales más o menos largas o complejas, habitualmente palabras o frases, para ocultar el mensaje; por ejemplo, "cielo azul" podría significar «atacar al amanecer». Por el contrario, las *cifras* clásicas normalmente sustituyen o reordenan los elementos básicos del mensaje -letras, dígitos o símbolos-; en el ejemplo anterior, «rcnm arcteeaal aaa» sería un criptograma obtenido por *transposición*. Cuando se usa una técnica de códigos, la información secreta suele recopilarse en un *libro de códigos*.

Con frecuencia los procesos de cifrado y descifrado se encuentran en la literatura como *encriptado* y *desencriptado*, aunque ambos son neologismos erróneos —anglicismos de los términos ingleses*encrypt* y *decrypt*— todavía sin reconocimiento académico. Hay quien hace distinción entre *cifrado/descifrado* y *encriptado/desencriptado* según estén hablando de criptografía simétrica o asimétrica, pero la realidad es que la mayoría de los expertos hispanohablantes prefieren evitar ambos neologismos hasta el punto de que el uso de los mismos llega incluso a discernir a los aficionados y novatos en la materia de aquellos que han adquirido más experiencia y profundidad en la misma.

Las funciones de la criptografía

La criptografía se usa tradicionalmente para ocultar mensajes de ciertos usuarios. En la actualidad, esta función es incluso más útil ya que las comunicaciones de Internet circulan por infraestructuras cuya fiabilidad y confidencialidad no pueden garantizarse. La criptografía se usa no sólo para proteger la confidencialidad de los datos, sino también para garantizar su integridad y autenticidad.

Para que sirve la criptografía

Los seres humanos siempre han sentido la necesidad de ocultar información, mucho antes de que existieran los primeros equipos informáticos y calculadoras.

Desde su creación, Internet ha evolucionado hasta convertirse en una herramienta esencial de la comunicación. Sin embargo, esta comunicación implica un número creciente de problemas estratégicos relacionados con las actividades de las empresas en la Web. Las transacciones que se realizan a través de la red pueden ser interceptadas y, sobretodo, porque actualmente resulta difícil establecer una legislación sobre Internet. La seguridad de esta información debe garantizarse: éste es el papel de la criptografía.

Historia de la criptografía

La historia de la criptografía es larga y abunda en anécdotas. Ya las primeras civilizaciones desarrollaron técnicas para enviar mensajes durante las campañas militares, de forma que si el mensajero era interceptado la información que portaba no corriera el peligro de caer en manos del enemigo.El primer método de criptografía fue en el siglo V a.C, era conocido como "Escítala". El segundo criptosistema que se conoce fue documentado por el historiador griego Polibio: un sistema de sustitución basado en la posición de las letras en una tabla. También los romanos utilizaron sistemas de sustitución, siendo el método actualmente conocido como César, porque supuestamente Julio César lo empleó en sus campañas, uno de los más conocidos en la literatura (según algunos autores, en realidad Julio César no usaba este sistema de sustitución, pero la atribución tiene tanto arraigo que el nombre de este método de sustitución ha quedado para los anales de la historia). Otro de los métodos criptográficos utilizados por los griegos fue la escítala espartana, un método de trasposición basado en un cilindro que servía como clave en el que se enrollaba el mensaje para poder cifrar y descifrar.

En 1465 el italiano Leon Battista Alberti inventó un nuevo sistema de sustitución polialfabética que supuso un gran avance de la época. Otro de los criptógrafos más importantes del siglo XVI fue el francés Blaise de Vigenère que escribió un importante tratado sobre "la escritura secreta" y que diseñó una cifra que ha llegado a nuestros días asociada a su nombre.
A Selenus se le debe la obra criptográfica "Cryptomenytices et Cryptographiae" (Luneburgo, 1624). Durante los siglos XVII, XVIII y XIX, el interés de los monarcas por la criptografía fue notable. Las tropas de Felipe II emplearon durante mucho tiempo una cifra con un alfabeto de más de 500 símbolos que los matemáticos del rey consideraban inexpugnable. Cuando el matemático francés François Viète consiguió criptoanalizar aquel sistema para el rey de Francia, a la sazón Enrique IV, el conocimiento mostrado por el rey francés impulsó una queja de la corte española ante del papa Pío V acusando a Enrique IV de utilizar magia negra para vencer a sus ejércitos. Por su parte, la reina María Estuardo, reina de Escocia, fue ejecutada por su prima Isabel I de Inglaterra al descubrirse un complot de aquella tras un criptoanálisis exitoso por parte de los matemáticos de Isabel.

Durante la Primera Guerra Mundial, los Alemanes usaron el cifrado ADFGVX. Este método de cifrado es similar a la del tablero de ajedrez Polibio. Consistía en una matriz de 6 x 6 utilizado para sustituir cualquier letra del alfabeto y los números 0 a 9 con un par de letras que consiste de A, D, F, G, V, o X.

Desde el siglo XIX y hasta la Segunda Guerra Mundial, las figuras más importantes fueron la del holandés Auguste Kerckhoffs y la del prusiano Friedrich Kasiski. Pero es en el siglo XX cuando la historia de la criptografía vuelve a experimentar importantes avances. En especial durante las

dos contiendas bélicas que marcaron al siglo: la Gran Guerra y la Segunda Guerra Mundial. A partir del siglo XX, la criptografía usa una nueva herramienta que permitirá conseguir mejores y más seguras cifras: las máquinas de cálculo. La más conocida de las máquinas de cifrado posiblemente sea la máquina alemana Enigma: una máquina de rotores que automatizaba considerablemente los cálculos que era necesario realizar para las operaciones de cifrado y descifrado de mensajes. Para vencer al ingenio alemán, fue necesario el concurso de los mejores matemáticos de la época y un gran esfuerzo computacional. No en vano, los mayores avances tanto en el campo de la criptografía como en el del criptoanálisis no empezaron hasta entonces.

Tras la conclusión de la Segunda Guerra Mundial, la criptografía tiene un desarrollo teórico importante, siendo Claude Shannon y sus investigaciones sobre teoría de la información esenciales hitos en dicho desarrollo. Además, los avances en computación automática suponen tanto una amenaza para los sistemas existentes como una oportunidad para el desarrollo de nuevos sistemas. A mediados de los años 70, el Departamento de Normas y Estándares norteamericano publica el primer diseño lógico de un cifrador que estaría llamado a ser el principal sistema criptográfico de finales de siglo: el Estándar de Cifrado de Datos o DES. En esas mismas fechas ya se empezaba a gestar lo que sería la, hasta ahora, última revolución de la criptografía teórica y práctica: los sistemas asimétricos. Estos sistemas supusieron un salto cualitativo importante, ya que permitieron introducir la criptografía en otros campos que hoy día son esenciales, como el de la firma digital.

Medidas de seguridad:

19.-Políticas de Seguridad Informática

Generalidades

La seguridad informática ha tomado gran auge, debido a las cambiantes condiciones y nuevas plataformas tecnológicas disponibles. La posibilidad de interconectarse a través de redes, ha abierto nuevos horizontes a las empresas para mejorar su productividad y poder explorar más allá de las fronteras nacionales, lo cual lógicamente ha traído consigo, la aparición de nuevas amenazas para los sistemas de información.

Estos riesgos que se enfrentan ha llevado a que muchas desarrollen documentos y directrices que orientan en el uso adecuado de estas destrezas tecnológicas y recomendaciones para obtener el mayor provecho de estas ventajas, y evitar el uso indebido de las mismas, lo cual puede ocasionar serios problemas a los bienes, servicios y operaciones de la empresa.

En este sentido, las políticas de seguridad informática surgen como una herramienta organizacional para concientizar a los colaboradores de la organización sobre la importancia y sensibilidad de la información y servicios críticos que permiten a la empresa crecer y mantenerse competitiva. Ante esta situación, el proponer o identificar una política de seguridad requiere un alto compromiso con la organización, agudeza técnica para establecer fallas y debilidades, y constancia para renovar y actualizar dicha política en función del dinámico ambiente que rodea las organizaciones modernas.

Definición de Políticas de Seguridad Informática

Una política de seguridad informática es una forma de comunicarse con los usuarios, ya que las mismas establecen un canal formal de actuación del personal, en relación con los recursos y servicios informáticos de la organización.

No se puede considerar que una política de seguridad informática es una descripción técnica de mecanismos, ni una expresión legal que involucre sanciones a conductas de los empleados, es más bien una descripción de los que deseamos proteger y él por qué de ello, pues cada política de seguridad es una invitación a cada uno de sus miembros a reconocer la información como uno de sus principales activos así como, un motor de intercambio y desarrollo en el ámbito de sus negocios. Por tal razón, las políticas de seguridad deben concluir en una posición consciente y vigilante del personal por el uso y limitaciones de los recursos y servicios informáticos.

Elementos de una Política de Seguridad Informática
Como una política de seguridad debe orientar las decisiones que se toman en relación con la seguridad, se requiere la disposición de todos los miembros de la empresa para lograr una visión conjunta de lo que se considera importante.

Las Políticas de Seguridad Informática deben considerar principalmente los siguientes elementos:

o **Alcance de las políticas,** incluyendo facilidades, sistemas y personal sobre la cual aplica.
o **Objetivos de la política y descripción clara de** los elementos involucrados en su definición.
o Responsabilidades por cada uno de los servicios y recursos informáticos aplicado a todos los niveles de la organización.
o Requerimientos mínimos para configuración de la seguridad de los sistemas que abarca el alcance de la política.
o Definición de violaciones y sanciones por no cumplir con las políticas.
o **Responsabilidades de los usuarios** con respecto a la información a la que tiene acceso.

Las políticas de seguridad informática, también deben ofrecer explicaciones comprensibles sobre por qué deben tomarse ciertas decisiones y explicar la importancia de los recursos. Igualmente, deberán establecer las expectativas de la organización en relación con la seguridad y especificar la autoridad responsable de aplicar los correctivos o sanciones.
Otro punto importante, es que las políticas de seguridad deben redactarse en un lenguaje sencillo y entendible, libre de tecnicismos y términos ambiguos que impidan una comprensión clara de las mismas, claro está sin sacrificar su precisión.
Por último, y no menos importante, el que las políticas de seguridad, deben seguir un proceso de actualización periódica sujeto a los cambios organizacionales relevantes, como son: el aumento de personal, cambios en la infraestructura computacional, alta rotación de personal, desarrollo de nuevos servicios, regionalización de la empresa, cambio o diversificación del área de negocios, etc.

Parámetros para Establecer Políticas de Seguridad

Es importante que al momento de formular las políticas de seguridad informática, se consideren por lo menos los siguientes aspectos:
* **Efectuar un análisis de riesgos informáticos**, para valorar los activos y así adecuar las políticas a la realidad de la empresa.
* **Reunirse con los departamentos dueños de los recursos**, ya que ellos

poseen la experiencia y son la principal fuente para establecer el alcance y definir las violaciones a las políticas.

* **Comunicar a todo el personal involucrado sobre el desarrollo de las políticas**, incluyendo los beneficios y riesgos relacionados con los recursos y bienes, y sus elementos de seguridad.

*** Identificar quién tiene la autoridad para tomar decisiones en cada departamento**, pues son ellos los interesados en salvaguardar los activos críticos su área.

* **Monitorear periódicamente los procedimientos y operaciones de la empresa,** de forma tal, que ante cambios las políticas puedan actualizarse oportunamente.

*** Detallar explícita y concretamente el alcance de las políticas con el propósito de evitar situaciones de tensión** al momento de establecer los mecanismos de seguridad que respondan a las políticas trazadas.

Razones que Impiden la Aplicación de las Políticas de Seguridad Informática

A pesar de que un gran número de organizaciones canalizan sus esfuerzos para definir directrices de seguridad y concretarlas en documentos que orienten las acciones de las mismas, muy pocas alcanzan el éxito, ya que la primera barrera que se enfrenta es convencer a los altos ejecutivos de la necesidad y beneficios de buenas políticas de seguridad informática.

Otros inconvenientes lo representan los tecnicismos informáticos y la falta de una estrategia de mercadeo por parte de los Gerentes de Informática o los especialistas en seguridad, que llevan a los altos directivos a pensamientos como: “más dinero para juguetes del Departamento de Sistemas”.

Esta situación ha llevado a que muchas empresas con activos muy importantes, se encuentren expuestas a graves problemas de seguridad y riesgos innecesarios, que en muchos casos comprometen información sensitiva y por ende su imagen corporativa. Ante esta situación, los encargados de la seguridad deben confirmar que las personas entienden los asuntos importantes de la seguridad, conocen sus alcances y están de acuerdo con las decisiones tomadas en relación con esos asuntos.

Si se quiere que las políticas de seguridad sean aceptadas, deben integrarse a las estrategias del negocio, a su misión y visión, con el propósito de que los que toman las decisiones reconozcan su importancia e incidencias en las proyecciones y utilidades de la compañía.

Finalmente, es importante señalar que las políticas por sí solas no constituyen una garantía para la seguridad de la organización, ellas deben responder a

intereses y necesidades organizacionales basadas en la visión de negocio, que lleven a un esfuerzo conjunto de sus actores por administrar sus recursos, y a reconocer en los mecanismos de seguridad informática factores que facilitan la formalización y materialización de los compromisos adquiridos con la organización.

20-SEGURIDAD ACTIVA Y PASIVA

Podemos encontrar dos tipos de técnicas de seguridad para el proteger nuestro ordenador:

Seguridad activa: Tiene como objetivo proteger y evitar posibles daños en los sistemas informáticos. Podemos encontrar diferentes recursos para evitarlos como:

-Una de esas técnicas que podemos utilizar es el uso adecuado de contraseñas, que podemos añadirles números, mayúsculas, etc.
-También el uso de software de seguridad informática: como por ejemplo ModSecurity, que es una herramienta para la detección y prevención de intrusiones para aplicaciones web, lo que podríamos denominar como "firewall web".
-Y la encriptación de los datos.

Seguridad pasiva: Su fin es minimizar los efectos causados por un accidente, un usuario o malware. Las practicas de seguridad pasiva más frecuentes y mas utilizadas hoy en día son:

-El uso de hardware adecuado contra accidentes y averías.
-También podemos utilizar copias de seguridad de los datos y del sistema operativo.

Una practica también para tener seguro nuestro ordenador es hacer particiones del disco duro, es decir dividirlo en distintas partes. Existen dos tipos de particiones, particiones primarias y particiones extendidas. Las particiones primarias sirven para albergar sistemas operativos y datos de programa, todo disco duro tiene al menos una partición primaria y las particiones extendidas, las cuales se utilizan para alargar el número máximo de particiones (aunque no se recomienden mas de 12), puesto que una partición extendida puede contener tantas particiones primarias como se quiera.

•Análisis forense en sistemas informáticos:

21.-Análisis Forense

Es la investigación y análisis de cualquier dispositivo electrónico para la obtención de pruebas admisibles judicialmente o de información relevante para negociaciones internas.

Con el servicio de Análisis Forense de medios digitales se realiza un análisis detallado y minucioso de cualquier tipo de dispositivo electrónico (ordenadores, teléfonos, agendas PDA, servidores corporativos, etc.…).

El objetivo del análisis, llevado a cabo en nuestro Laboratorio Forense, es la identificación de indicios y certificación de hechos realizados a través de los mismos.

En situaciones de conflicto, este servicio da respuesta al *qué, quién, cuándo, dónde y cómo* se ha cometido un determinado fraude, ilícito o delito.

Debido a la arquitectura de los sistemas operativos actuales, donde el rendimiento prevalece sobre la seguridad de la información, un experto informático forense puede recuperar archivos o fragmentos que previamente el usuario había borrado o modificado. El aumento exponencial del tamaño de las unidades de almacenamiento permite a los expertos forenses recuperar ficheros borrados o manipulados con meses e incluso años de antigüedad. La mayoría de sistemas operativos actuales generan una gran cantidad de información relacionada con el trabajo que el usuario está realizando en el ordenador de una forma totalmente inapreciable para el usuario y que el experto forense, con las herramientas y metodología adecuadas, puede extraer, analizar e interpretar para obtener prueba electrónica.

En el caso de emitir un informe pericial, nuestros expertos podrán ratificar dicho informe en juicio a través del servicio de Declaración en Juicio

- Funcionalidad y fases de un análisis forense.

Análisis Forense– Fase de Evaluación

Lo que se debe realizar en esta fase es la evaluación de los recursos a los que tenemos acceso y cuales son los objetivos para realizar la investigaron interna, pasando por las siguientes etapas:

- **Notificar y obtener la autorización:** En esta etapa del proceso forense, debemos obtener una autorización por escrito para iniciar el análisis forense, al igual que la firma de los acuerdos de confidencialidad, sin esta autorización por escrito nuestro análisis no tendría una validez legal y de hecho estaríamos cometiendo un delito.
- **Revisar las políticas y la legislación:** Debemos documentarnos sobre todas las políticas y legislación vigente para el análisis forense y manejo de evidencias en el país donde se presente el incidente, ademas de todas las acciones y antecedentes que preceden la investigación.

- **Identificar a los miembros del equipo:** Debemos identificar el grupo de trabajo que realizará la investigación, definir las responsabilidades de cada miembro, así como sus limites y funciones.
- **Realizar una evaluación:** Debemos realizar una investigación preliminar que nos permita exponer la situación actual, hechos sucedidos, las personas u organizaciones afectadas, posibles sospechosos, gravedad y criticidad de la

situación, daños causados*(clientes, impacto financiero, I+D, etc..)*, identificar topología *(red, equipos, SO, etc..)*, realizar entrevista con funcionarios, usuarios, administradores y responsables de los sistemas, con esto lograremos tener un panorama mas claro que nos facilite una mejor comprensión de la situación.

- **Prepararse para la adquisición de pruebas:** Identifique los equipos afectados*(capacidad de disco, sistemas operativos, etc..)*, dispositivos de almacenamiento*(memorias USB, discos duros, CDs, DVDs,cintas, etc…)* vinculados al caso, así como realizar la sanitizacion de los medios donde realizaremos las respectivas copias bit a bit de los medios identificados en la etapa de identificación.
  Al terminar esta etapa del análisis debemos entregar un documento con toda la información detallada de los procedimientos realizados, para establecer el inicio de la adquisición de datos, la cadena de custodia, y la elaboración de los informes finales.

Análisis Forense– Fase de Adquisición

En esta fase se debe iniciar la investigación, determinar las herramientas que vamos a utilizar, recopilar los datos, revisar la legislación para el manejo de evidencias y almacenar la evidencia, para ello pasamos por las siguientes etapas:

- **Construcción de la investigación:** Debemos iniciar una bitácora, ya sea digital o manuscrita donde documentemos detalladamente toda la información referente a la investigación, quien realiza una determinada labor y por qué, que intentaba conseguir con esa labor, como la realizó, que herramientas y procedimientos utilizó, todo esto detallado con fechas y horas.
- **Recopilar los datos:** Antes de iniciar con la recolección de datos, es recomendable asegurarse que ya se han realizado los respectivos procedimientos para salvaguardar la evidencia física *(huellas, rastros de ADN, toma de fotografías, etc…)* para poder realizar ciertos procedimientos con el dispositivo iOS *(que no afecta la evidencia si se documenta adecuadamente)* y pueden evitarnos algunos dolores de cabeza mas adelante, como por ejemplo desactivar el bloqueo automático,

extraer información básica del dispositivo y activar el modo avión, después de esto pasamos a realizar una copia *(bit a bit)* del dispositivo y firmarla con un hash SHA1 0 MD5, generando de esta forma *“el segundo original”*, a partir del

cual se generaran las copias que se utilizaran en la fase de análisis *(con cada una de ellas se debe comprobar que el hash corresponda al del segundo original)*.

- **Almacenar y archivar:** En esta etapa debemos documentar adecuadamente la evidencia con su correspondiente documento de embalaje y cadena de custodia, la cual debe contener una linea de tiempo donde relacione quien ha accedido a la evidencia, que realizo con ella, por que motivo y a que hora; Después de eso pasamos a archivar dicha evidencia asegurandonos que el lugar donde lo hagamos cumpla con las buenas practicas para conservar la información y la legislación existente sobre el manejo de evidencias digitales. El lugar donde se almacene la evidencia debe contar con una buena seguridad física que evite la manipulación de la evidencia, una jaula de Faraday para almacenar en ella los dispositivos que accedan a redes telefónicas o inalámbricas y una bitácora donde se almacenen los nombres de las personas que después de almacenada, accedan a la evidencia, la cual debe tener la fecha/hora, el tiempo que demoró revisando la evidencia y la fecha/hora en que esta la devuelve si acaso la sacó; La información de esta bitácora debe ser completa, correcta, autentica y convincente, para que en caso de un proceso legal pueda ser admitida en un juzgado.

Análisis Forense – Fase de Análisis

En esta fase se debe iniciar el análisis de los dispositivos, para llevar a cabo esta labor, definiremos los objetivos y criterios de búsqueda a utilizar para dar con la información que necesitamos, utilizaremos una copia del segundo original generado previamente y una vez comprobada *(determinar si los hash corresponden al segundo original)* analizaremos sus archivos para extraer y relacionar la información que nos permita cumplir con los objetivos planteados, las etapas de este paso son:

- **Análisis de datos de la red:** Normalmente cuando realizamos una investigación donde están relacionados equipos de computo, lo primero que hacemos en la fase de análisis es identificar los dispositivos de defensa *(IDS, IPS, Firewall, Proxy, etc…)* y de comunicación que se encuentran en la red, ya que normalmente al recuperar sus logs y relancionarlos con el equipo que estamos analizando, podemos obtener una buena cantidad de información sobre el comportamiento de ese equipo en la red donde se encuentra. Pero cuando tratamos con dispositivos móviles el escenario es muy diferente, ya que por lo general ellos cuentan con su propia red de datos o se conectan a distintas redes según donde se encuentren y en la mayoría de casos, las redes

a las que se conectan, no cuentan con alguna implementación de defensa a la cual sacarle logs.

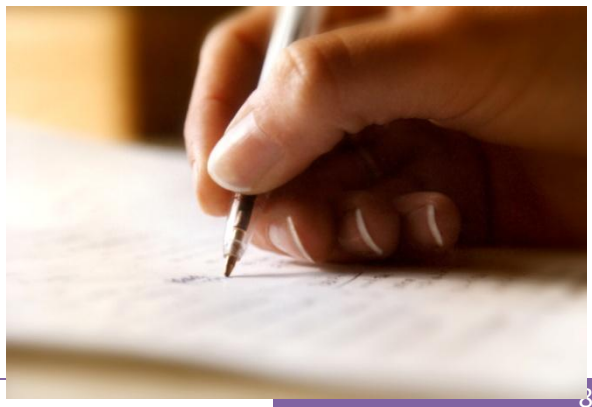
- **Análisis los datos host:** Utilizando una copia de su segundo original, procesamos la información obtenida de cada sistema adquirido, de la lectura de las Aplicaciones, logs y las configuraciones propias del iOS, *(esto se puede hacer manualmente o con herramientas automatizadas)*. En cada caso esta etapa debe estar limitada a los parámetros y criterios de búsquedas definidos inicialmente para nuestro caso, ya que la información encontrada en estos dispositivo, suele ser extensa y puede complicar el análisis de datos si no definimos previamente lo que estamos buscando.

- **Análisis los medios de almacenamiento:** Al analizar los medios de almacenamiento*(en modo de solo lectura para evitar alterar la evidencia)*, debemos determinar si los archivos no tienen algún tipo de cifrado, es recomendable crear una estructura de Directorios y Archivos recuperados para ubicar fácilmente los datos, estudiar los Metadatos en especial las fechas de creación, actualización, acceso, modificación, que nos pueden ayudar a determinar una linea de tiempo a evidencia debe ser cargada de solo lectura.

Análisis Forense – Fase de Informes

En esta fase se debe iniciar la organización de la información, para poder escribir los informes que sustentarán las pruebas en un proceso legal, para esto básicamente debemos tener en cuenta los siguientes pasos:

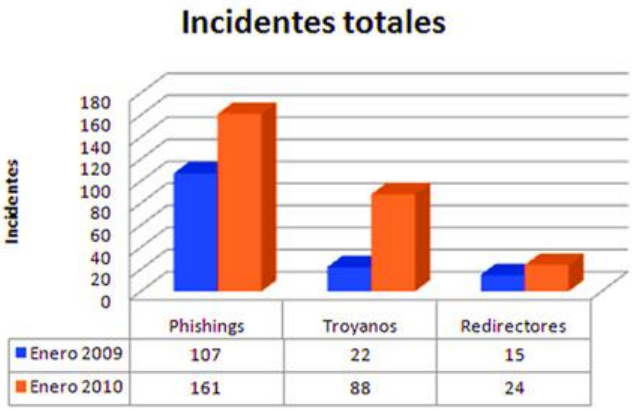
- **Recopilar y Organizar:** En esta etapa retomamos toda la documentación generada en las fases anteriores, las notas, las bitácoras, los anexos y cualquier otra información generada, después identifiquemos lo mas importante y relevante para nuestra investigación, realizamos una lista de pruebas para presentar en el informe y unas conclusiones para ingresar en el.



- **Escribir el informe:** Pasamos a escribir los informes, debemos tener en cuenta que tanto el informe debe tener los siguientes parámetros:
  - **Propósito:** Todo informe tiene que tener definido de forma clara cual

es su propósito, a que publico va dirigido y cual es su objetivo.

- **Autor/Autores:** En el informe debe estar detallado quien es el autor o autores de la investigación, cual fue su labor durante la investigación ademas de su responsabilidad en la misma y por ultimo debe tener la información de contactopara que puedan ubicarlos en caso de que sea necesario.
- **Resumen de Incidentes:** Se debe explicar el incidente y su impacto, de forma concisa, escrita de tal manera que una persona sin conocimientos técnicos, como un juez o jurado pueda entender lo sucedido y cómo ocurrió.



- **Pruebas:** Debes proporción una descripción de las pruebas adquiridas durante la investigación, las evidencias, cómo fueron adquiridas y quien las adquirió.
- **Detalles:** Debemos proporcionar una descripción detallada de lo que se analizó, los métodos que se utilizaron, explicar los resultados del análisis, listar los procedimientos que se llevaron a cabo durante la investigación y las técnicas de análisis que se utilizaron, también se deben incluir pruebas de sus resultados, los informes de servicios y las entradas de registro/logs del sistema.
- **Justificar:** Cada conclusión que se extrae del análisis debe estar justificada, debemos adjuntar documentos justificativos que incluya cualquier información de antecedentes a que se refiere en todo el informe, tales como documentos que describen los procedimientos de investigación de equipos usados, panorama general de las tecnologías que intervienen en la investigación. Es importante que los documentos justificativos proporcionen información suficiente para que el lector del informe pueda comprender el incidente tanto como sea posible.
- **Conclusión:** Las conclusiones deben ser lo más claras posibles y sin ambigüedades, en ellas debemos resumir los resultados de la investigación, debemos ser específicos y citar pruebas concretas para demostrar las conclusiones, pero sin dar muchos detalles sobre ellos para no ser redundantes *(ya que esta información esta en la sección "Detalles")*.

- **Glosario:** Se debe considerar la creación de un glosario de términos utilizados en el informe, este glosario es especialmente valioso si el organismo de aplicación de la ley no está bien informado sobre cuestiones técnicas o cuando un juez, jurado debe revisar los documentos.

- **El informe ejecutivo:** Debe ser claro, conciso y no debe contener lenguaje técnico, por el contrario debe ser escrito para la gente del común ya que por lo general va dirigido a gerentes, jueces que poco están relacionados con la informática en general y los términos ingenieriles que solemos utilizar.
- **El informe técnico:** Este informe contrario al informe ejecutivo, va dirigido por lo general al departamento de sistemas u otros investigadores forense, por tanto debemos detallar todos los procedimientos realizados, debemos utilizar información técnica que permita a cualquier persona que siga esos pasos conseguir los mismos resultados que conseguimos nosotros.

- Análisis de evidencias digitales.

Evidencia digital y análisis forense

El uso de las evidencias digitales, entendiendo como tales cualquier información almacenada o transmitida en formato electrónico, ha aumentado en los últimos años debido a que los Tribunales aceptan en sus procedimientos laborales, civiles y penales pruebas en formato digital. Correos electrónicos, documentos de office, fotografías digitales, ficheros de video o audio, logs de eventos o históricos son algunos ejemplos de evidencias digitales que pueden encontrase en diferentes dispositivos como discos duros de ordenadores o servidores, pdas, móviles, cintas de backup, tarjetas de memoria, etc.

22- Herramientas de análisis forense.

Herramientas

Tipos de herramientas forenses.

Recolección de evidencias

Existen un gran número de herramientas que se pueden utilizar para la recuperación de evidencia, la utilización de herramientas sofisticadas es necesaria. Esto se debe a la gran cantidad de datos que pueden estar guardados en la computadora, la gran cantidad de extensiones y formatos con los que nos podemos encontrar dentro de un mismo sistema operativo.

Es necesario recopilar información que sea correcta y que sea comprobable, es decir verificar que no ha sufrido alteraciones o corrupción. Cabe aclarar que las herramientas sofisticadas nos ayudan a disminuir los tiempos para poder analizar toda la información recopilada.

Por otro lado nos encontramos también la simplicidad con la que se pueden borrar los archivos de la computadora como así también las distintas herramientas de encriptación y contraseñas.

Monitoreo y/o control de computadoras

Hay ocasiones en las que necesitamos saber cual ah sido la utilización que se le ah dado a la computadora antes de que se le realice la pericia por lo tanto tenemos herramientas que controlan que se le da ah la computadora para poder recopilar la información.

Dentro de las herramientas nos encontramos con algunas de mucha simpleza como lo es un key logger, el cual almacena en un archivo de texto todo lo que ingresamos por el teclado. De esta misma forma tenemos los intermedios que guardan screenshots de la pantalla que ve el usuario observado y los de mayor complejidad que nos permiten tomar el control de la computadora en su totalidad además de observar lo que hace el usuario.

Marcado de documentos

Una herramienta interesante es aquella que permite hacerle una marca a un documento importante, esto es de gran utilidad si nos encontramos con un caso en el que se está sustrayendo información, ya que al marcar el

documento se lo puede seguir y detectarlo con facilidad.

La intención principal de la seguridad está centrada en prevenir los ataques. Nos encontramos con algunos sitios los cuales tienen información confidencial o de mucho valor los cuales intentan protegerse a través de mecanismos de validación. Pero lo cierto es que nada es seguro en su totalidad siempre hay algo que se nos escapa por lo tanto debemos estar preparados para saber actuar ante algún posible ataque.

Hardware

Debido a que el proceso de recolección de evidencia debe ser preciso y no debe modificar la información se han diseñado varias herramientas como DIBS las cuales son las que nos permiten poder recuperar la información sin alterar los datos. Pero seguimos teniendo el inconveniente de que cuando encendemos la computadora se modifican los registros de la misma.

Herramientas para realizar análisis forense

Herramientas utilizadas en el ámbito de la informática forense para la recuperación de datos borrados o recolección de evidencia digital.

- Outport
- AIRT (Advanced incident response tool
- Foremost
- WebJob
- HashDig
- Md5deep

Programas para informática forense

Herramientas que permiten la recuperación de datos como así también el análisis de los navegadores. Los programas son lo siguientes.

Srprint

Pasco

Web Historian

Rifuiti, etc.