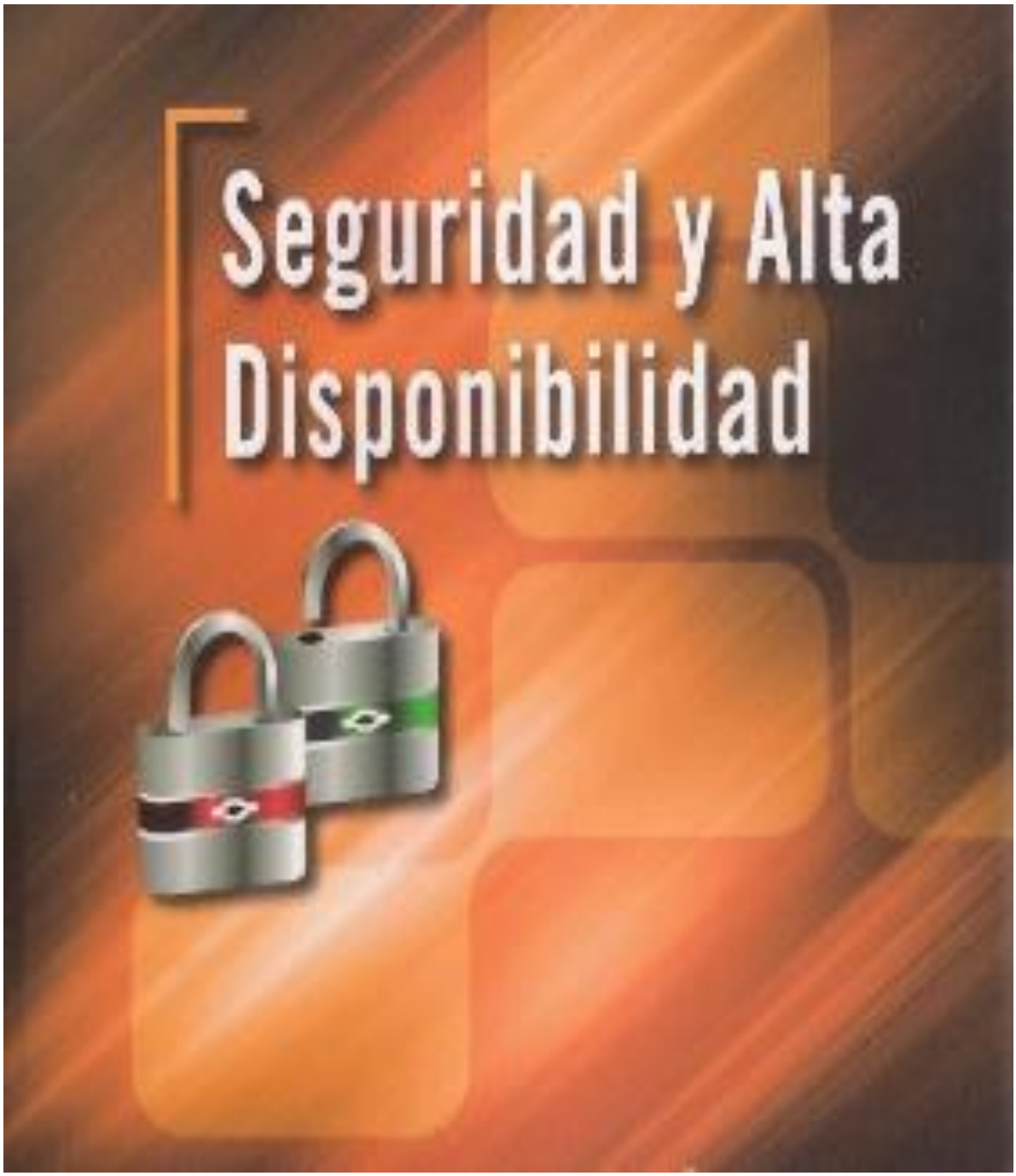

Seguridad y Alta
Disponibilidad

INDICE

-1.1-Fiabilidad, confidencialidad, integridad y disponibilidad

¿Qué es la seguridad informática?

La **seguridad informática** es el área de la informática que se enfoca en la protección de la infraestructura computacional y todo lo relacionado con esta (incluyendo la información contenida). Para ello existen una serie de estándares, protocolos, métodos, reglas, herramientas y leyes concebidas para minimizar los posibles riesgos a la infraestructura o a la información. La seguridad informática comprende software, bases de datos, metadatos, archivos y todo lo que la organización valore (activo) y signifique un riesgo si ésta llega a manos de otras personas.

Ventajas:

1. Asegurar el acceso a la información en el momento oportuno, incluyendo respaldos de la misma en caso de que esta sufra daños o pérdida producto de accidentes, atentados o desastres.
2. Procesar datos de manera rápida y fiable: realizar cálculos, escribir y copiar textos, crear bases de datos, modificar imágenes siempre conversando los estándares planteados.

Desventajas:

1. Por vulnerabilidad entendemos la exposición latente a un riesgo. En el área de informática, existen varios riesgos tales como: ataque de virus, códigos maliciosos, gusanos, caballos de troya y hackers; no obstante, con la adopción de Internet como instrumento de comunicación y colaboración, los riesgos han evolucionado y, ahora, las empresas deben enfrentar ataques de negación de servicio y amenazas combinadas; es decir, la integración de herramientas automáticas de "hackeo", accesos no autorizados a los sistemas y capacidad de identificar y explotar las vulnerabilidades de los sistemas operativos o aplicaciones para dañar los recursos informáticos.

2. Como toda herramienta creada por el hombre en ocasiones sufre daños que de una u otra forma pueden retrasar el trabajo de una empresa o institución.

FIABILIDAD

Característica de los sistemas informáticos por la que se mide el tiempo de funcionamiento sin fallos. En el caso del hardware, se han conseguido altísimos grados de fiabilidad, mientras que en el software siguen existiendo bugs que dificultan el buen funcionamiento de los programas.

CONFIABILIDAD:

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

INTEGRIDAD

Para la Seguridad de la Información, la integridad es la propiedad que busca mantener los datos libres de modificaciones no autorizadas. La integridad de un mensaje se obtiene adjuntándole otro conjunto de datos de comprobación de la integridad: la firma digital Es uno de los pilares fundamentales de la seguridad de la información.

DISPONIBILIDAD

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

En el caso de los sistemas informáticos utilizados para almacenar y procesar la información, los controles de seguridad utilizados para protegerlo, y los canales de comunicación protegidos que se utilizan para acceder a ella deben estar funcionando correctamente.

2 Elementos vulnerables en hardware, software y datos.

En seguridad informática, la palabra vulnerabilidad hace referencia a una debilidad en un sistema permitiendo a un atacante violar la confidencialidad, integridad, disponibilidad, control de acceso y consistencia del sistema o de sus datos y aplicaciones.
Las amenazas siempre están presentes, pero sin la identificación de una vulnerabilidad, no podrán causar ningún impacto.

1.2.1 Hardware.

Las vulnerabilidades de hardware representan la probabilidad de que las piezas físicas del sistema fallen (ya sea por mal uso, descuido, mal diseño etc.) dejando al sistema desprotegido o inoperable. También trata sobre las formas en que el hardware puede ser usado por personas para atacar la seguridad del sistema, por ejemplo el sabotaje de un sistema al sobrecargarlo deliberadamente con componentes de hardware que no han sido diseñados correctamente para funcionar en el sistema.

1.2.2 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.

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 inofensiva, 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.

1.2.3 Ataques de datos

Los ataques a datos pueden ser atacados por:

Bomba lógica: el programa incluye instrucciones que, al cumplirse una condición, provocan una distorsión del funcionamiento normal del programa, que normalmente, deriva en daños al ordenador que lo ejecuta. Esta técnica es usada por algunos programadores. Introducen en la aplicación un código que se activa en una fecha determinada para que, si no ha cobrado por su trabajo ese día, destruya la información del ordenador en el que ha sido instalado.
Virus. Todos sabemos lo que son, cómo se comportan e incluso habremos sufrido sus consecuencias. Hoy en día, la conectividad entre ordenadores hace que existan muchísimos más de los 30 o 40 mil conocidos a finales de los 80, y que su impacto, cuando logran trascender, sea mucho mayor.

3-Analisis de las principales vulnerabilidades de un sistema informático

A continuación se expondrán diferentes tipos de ataques perpetrados, principalmente, por Hackers. Estos ataques pueden ser realizados sobre cualquier tipo de red, sistema operativo, usando diferentes protocolos, etc.

En los primeros tiempos, los ataques involucraban poca sofisticación técnica. Los Insiders (operadores, programadores, data entrys) utilizaban sus permisos para alterar archivos o registros. Los Outsiders ingresaban a la red simplemente averiguando una password válida. A través de los años se han desarrollado formas cada vez más sofisticadas de ataque para explotar "agujeros" en el diseño, configuración y operación de los sistemas.

1.3.1-Errores de Diseño, Implementación y Operación

Muchos sistemas están expuestos a "agujeros" de seguridad que son explotados para acceder a archivos, obtener privilegios o realizar sabotaje. Estas vulnerabilidades ocurren por variadas razones, y miles de "puertas invisibles" son descubiertas (cada día) en sistemas operativos, aplicaciones de software, protocolos de red, browsers de Internet, correo electrónico y todas clase de servicios informático disponible.

Los Sistemas operativos abiertos (como Unix y Linux) tienen agujeros mas conocidos y controlados que aquellos que existen en sistemas operativos cerrados (como Windows©). La importancia (y ventaja) del código abierto radica en miles de usuarios analizan dicho código en busca de posibles bugs y ayudan a obtener soluciones en forma inmediata.

1.3.2 Causas de las vulnerabilidades de los sistemas informáticos

- Debilidad en el diseño de los protocolos utilizados en las redes

Ej. Telnet, FTP, SNMP (simple network management protocol) pero también conocido como "security not my problem".

- Configuración inadecuada de sistemos informáticos

- Políticas de seguridad deficientes o inexistentes

- Desconocimiento y falta de sensibilización de los usuarios y de los responsables de informática.

- Errores de programación

- Limitación gubernamental al tamaño de las claves criptográficas y a la utilización de este tipo de tecnologías
- Disponibilidad de herramientas que facilitan los ataques
- Descuido de los fabricantes.
- Existencia de "puertas traseras" en los sistemas

Tipos de vulnerabilidades

- Vulnerabilidades que afectan equipos
  - Cámaras web y servidores de video
  - Teléfonos móviles (snarfing o bluesnarfing)
  - Agendas electrónicas
  - Routers, modems

- Vulnerabilidades que afectan programas y aplicaciones
  - Navegadores
  - Aplicaciones de oficina (word, excel)
  - Sistemas operativos, servidores y bases de datos

Inyección de código

Aquí encontramos distintos sub-tipos dentro de esta clase de vulnerabilidad:

Inyección directa de código estático: el software permite que las entradas sean introducidas directamente en un archivo de salida que se procese más adelante como código, un archivo de la biblioteca o una plantilla. En una inyección de código de tipo estático o también llamada permanente, una vez inyectado el código en una determinada parte de la aplicación web, este código queda almacenado en una base de datos.

Evaluación directa de código dinámico: el software permite que las entradas sean introducidas directamente en una función que evalúa y ejecuta dinámicamente la entrada como código, generalmente en la misma lengua que usa el producto.

Inclusión remota de archivo PHP: vulnerabilidad existente únicamente en paginas dinámicas escritas en PHP está debida a la inclusión de la función include() la cual permite el enlace de archivos situados en otros servidores, mediante los cuales se puede ejecutar código PHP en el servidor.

Error de búfer

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

El desbordamiento del búfer: un búfer se desborda cuando, de forma incontrolada, al intentar meter en él más datos de los que caben, ese exceso se vierte en zonas del sistema causando daños.

Condición de carrera

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

Error en la gestión de recursos

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

Permisos, privilegios y/o control de acceso

Se produce cuando el mecanismo de control de acceso o asignación de permisos es defectuoso. Hay que tener en cuenta que se trata del sistema en sí y no se debe confundir con una mala gestión por parte del administrador.

Fallo de autenticación

Esta vulnerabilidad se produce cuando la aplicación o el sistema no es capaz de autenticar al usuario, proceso, etc. correctamente.

Carácter criptográfico

La generación de números aleatorios para generar secuencias criptográficas, la debilidad o distintos fallos en los algoritmos de encriptación así como defectos en su implementación estarían ubicados dentro de este tipo de vulnerabilidad.

5. Amenazas. Tipos: físicas y lógicas.

5.1. Amenazas Lógicas

Bajo la etiqueta de “amenazas lógicas” encontramos todo tipo de programas que de una forma u otra pueden dañar a nuestro sistema, creados de forma intencionada para ello (software malicioso, también conocido como malware) o simplemente por error (bugs o agujeros). Algunas de estas amenazas son:

a) Software incorrecto.

Las amenazas más habituales a un sistema provienen de errores cometidos de forma involuntaria
por los programadores de sistemas o de aplicaciones. A estos errores de programación se les denomina bugs, y a los programas utilizados para aprovechar uno de estos fallos y atacar al sistema, exploits. Algunos ejemplos de software incorrecto son:
-Defectos de instalación o programación.
-Eliminación o sustitución de bibliotecas comunes a más de un programa o del sistema (DLL Hell).
-Reiniciar arbitrariamente la sesión de un usuario para que la instalación tenga efecto.
-Presuponer que el usuario tiene una conexión permanente a internet.

b) Herramientas de seguridad

Cualquier herramienta de seguridad representa un arma de doble filo: de la misma forma que un administrador las utiliza para detectar y solucionar fallos en sus sistemas o en la subred completa, un potencial intruso las puede utilizar para detectar esos mismos fallos y aprovecharlos para atacar los equipos.

El mal uso de estas herramientas puede concluir en situaciones de bloqueo, enlentecimiento e incluso denegación de servicio de las máquinas analizadas. Estas herramientas sólo deben ser lanzadas contra máquinas ajenas única y exclusivamente cuando sus responsables nos hayan autorizado a ello.

c) Puertas traseras.

Software que permite el acceso al sistema y facilita la entrada a la información de un usuario sin su permiso o conocimiento.

Durante el desarrollo de aplicaciones grandes o de sistemas operativos es habitual entre los programadores insertar `atajos' en los sistemas habituales de autenticación del programa o del núcleo que se está diseñando.

Algunos programadores pueden dejar estos atajos en las versiones definitivas de su software para facilitar un mantenimiento posterior, para garantizar su propio acceso, o simplemente por descuido; la cuestión es que si un atacante descubre una de estas puertas traseras (no nos importa el método que utilice para hacerlo) va a tener un acceso global a datos que no debería poder leer, lo que obviamente supone un grave peligro para la integridad de nuestro sistema.

d) Bombas lógicas

Software que permanece oculto hasta que se cumplen unas condiciones preprogramadas (por ejemplo una fecha) momento en el que se ejecuta, en ese punto, la función que realizan no es la original del programa, sino que generalmente se trata de una acción perjudicial.

Ejemplos de acciones que puede realizar una bomba lógica:
- Borrar información del disco duro
- Mostrar un mensaje
- Reproducir una canción
- Enviar un correo electrónico
- Apagar el Monitor

e) Canales cubiertos

Son canales de comunicación que permiten a un proceso transferir información de forma que viole la política de seguridad del sistema; dicho de otra forma, un proceso transmite información a otros (locales o remotos) que no están autorizados a leer dicha información. Los canales cubiertos no son una amenaza demasiado habitual en redes de I+D.

f) Virus

Un virus es una secuencia de código que se inserta en un fichero ejecutable (denominado huésped), de forma que cuando el archivo se ejecuta, el virus también lo hace, insertándose a sí mismo en otros programas.

Algunas acciones que puede realizar un virus son:
- Mostrar en la pantalla mensajes o imágenes humorísticas, generalmente molestas.
- Ralentizar o bloquear el ordenador.

g) gusanos

Un gusano es un tipo de malware que tiene la capacidad de copiarse a sí mismo para infectar otros sistemas utilizando servicios del propio sistema operativo que normalmente son invisibles al usuario. En ocasiones porta virus o aprovecha los bugs de los sistemas a los que se conecta para dañarlos.
Al ser difíciles de programar su número no es muy elevado, pero el daño que pueden causar es muy grande.

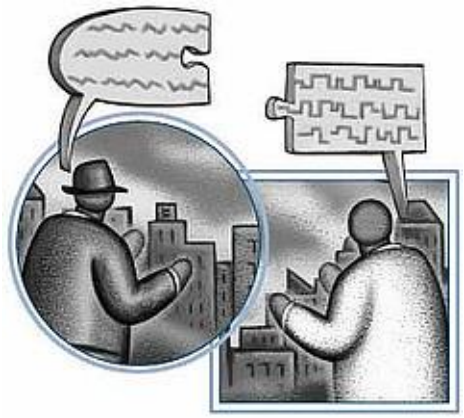
h) Caballos de Troya

Los troyanos o caballos de Troya son instrucciones escondidas en un programa de forma que éste parezca realizar las tareas que un usuario espera de él, pero que realmente ejecute funciones ocultas (generalmente en detrimento de la seguridad) sin el conocimiento del usuario.

Evitar la infección de un troyano es difícil, algunas de las formas más comunes de infectarse son:
- Descarga de programas de redes p2p y sitios web que no son de confianza.
- Páginas web que contienen contenido ejecutable (por ejemplo controles ActiveX o aplicaciones Java).
- Exploits para aplicaciones no actualizadas (navegadores, reproductores multimedia, clientes de mensajería instantánea).

Técnicas salami

Por técnica salami se conoce al robo automatizado de pequeñas cantidades de bienes (generalmente dinero) de una gran cantidad origen. El hecho de que la cantidad inicial sea grande y la robada pequeña hace extremadamente difícil su detección: si de una cuenta con varios millones de pesetas se roban unos céntimos, nadie va a darse cuenta de ello; si esto se automatiza para, por ejemplo, descontar una peseta de cada nómina pagada en la universidad o de cada beca concedida, tras un mes de actividad seguramente se habrá robado una enorme cantidad de dinero sin que nadie se haya percatado de este hecho, ya que de cada origen se ha tomado una cantidad ínfima.



Amenzas Fisicas:

Entre las amenazas físicas a los equipos informáticos se encuentran los problemas de alimentación y enfriamiento, los errores humanos o actividades maliciosas, los incendios, las pérdidas y la calidad del aire. Algunas de estas amenazas, incluyendo aquellas relacionadas con la alimentación y algunas relacionadas con el enfriamiento y los incendios, se monitorean regularmente por medio de capacidades integradas en los dispositivos de alimentación, enfriamiento y extinción de incendios. Por ejemplo, los sistemas UPS monitorean la calidad de la energía, la carga y la integridad de las baterías; las unidades PDU monitorean las cargas de los circuitos; las unidades de enfriamiento monitorean las temperaturas de entrada y salida y el estado de los filtros; los sistemas de extinción de incendios (los que exigen los códigos de edificación) monitorean la presencia de humo o exceso de calor. Estas amenazas físicas monitoreadas en forma automática son una parte clave de los sistemas de administración integral, pero en este informe no se tratará este tema. Sin embargo, para cierta clase de amenazas físicas en el centro de datos –y hablamos de amenazas graves–, El usuario no cuenta con soluciones de monitoreo prediseñadas e integradas.

Amenaza	Definición	Impacto en el centro de datos	Tipos de sensores
Temperatura del aire	Temperatura del aire en la sala, rack y los equipos	Fallos en los equipos y disminución de la vida útil de los equipos debido a temperaturas mayores de las especificadas y/o Cambios drásticos de temperatura	Sensores de temperatura
Humedad	Humedad relativa de la sala y del rack a una temperatura determinada	Fallos en los equipos debido a la acumulación de electricidad estática en los puntos de baja humedad. Formación de condensación en los puntos de humedad alta.	Sensores de humedad
Filtraciones de liquidos	Filtraciones de agua o refrigerante	Daños en los pisos,el cableado y los equipos causados por liquido indicios de problemas en la unidad CRAC	Sensores de cable de filtraciones Sensores puntuales de filtraciones
Error humano y acceso del personal	Daños involuntarios causados por el personal. Ingreso no autoriazado y/o por la fuerza al centro de datos con intenciones maliciosas	Daño a los equipos y pérdida de datos Tiempo de inactividad de los equipos Robo o sabotaje de equipos	-Cámaras digitales de video -Sensores de movimiento -Conmutadores de rack

¿Qué es la seguridad física?

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

¿En qué consiste la seguridad Física?

Consiste en la "aplicación de barreras físicas y procedimientos de control, como medidas de prevención y contramedidas ante amenazas a los recursos e información confidencial. Se refiere a los controles y mecanismos de seguridad dentro y alrededor del Centro de Cómputo así como los medios de acceso remoto al y desde el mismo; implementados para proteger el hardware y medios de almacenamiento de datos.

Tipos de Desastres

Este tipo de seguridad está enfocado a cubrir las amenazas ocasionadas tanto por el hombre como por la naturaleza del medio físico en que se encuentra ubicado el centro.

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

1. Desastres naturales, incendios accidentales tormentas e Inundaciones.

2. Amenazas ocasionadas por el hombre.

3. Disturbios, sabotajes internos y externos deliberados.

A continuación se analizan los peligros más importantes que se corren en un centro de procesamiento; con el objetivo de mantener una serie de acciones a seguir en forma eficaz y oportuna para la prevención, reducción, recuperación y corrección de los diferentes tipos de riesgos.

Incendios:

Los incendios son causados por el uso inadecuado de combustibles, fallas de instalaciones eléctricas defectuosas y el inadecuado almacenamiento y traslado de sustancias peligrosas.

El fuego es una de las principales amenazas contra la seguridad. Es considerado el enemigo número uno de las computadoras ya que puede destruir fácilmente los archivos de información y programas.

Inundaciones

Se define como la invasión de agua por exceso de escurrimientos superficiales o por acumulación en terrenos planos, ocasionada por falta de drenaje ya sea natural o artificial. Esta es una de las causas de mayores desastres en centros de computadoras. Además de las causas naturales de inundaciones, puede existir la posibilidad de una inundación provocada por la necesidad de apagar un incendio en un piso superior.

Condiciones Climatológicas

La comprobación de los informes climatológicos o la existencia de un servicio que notifique la proximidad de una tormenta severa, permite que se tomen precauciones adicionales, tales como la retirada de objetos móviles, la provisión de calor, iluminación o combustible para la emergencia.

Señales de Radar

La influencia de las señales o rayos de radar sobre el funcionamiento de una computadora ha sido exhaustivamente estudiada desde hace varios años. Los resultados de las investigaciones más recientes son que las señales muy fuertes de radar pueden inferir en el procesamiento electrónico de la información, pero únicamente si la señal que alcanza el equipo es de 5 Volts/Metro, o mayor.

Instalaciones Eléctricas

Las subidas (picos) y caídas de tensión no son el único problema eléctrico al que se han de enfrentar los usuarios. También está el tema del ruido que interfiere en el funcionamiento de los componentes electrónicos. El ruido interfiere en los datos, además de favorecer la escucha electrónica.

Ergometría

El enfoque ergonómico plantea la adaptación de los métodos, los objetos, las maquinarias, herramientas e instrumentos o medios y las condiciones de trabajo a la anatomía, la fisiología y la psicología del operador.

Control de Accesos

El control de acceso no sólo requiere la capacidad de identificación, sino también asociarla a la apertura o cerramiento de puertas, permitir o negar acceso basado en restricciones de tiempo, área o sector dentro de una empresa o institución.

Utilización de Guardias

El Servicio de Vigilancia es el encargado del control de acceso de todas las personas al edificio. Este servicio es el encargado de colocar los guardias en lugares estratégicos para cumplir con sus objetivos y controlar el acceso del personal.

Utilización de Detectores de Metales

El detector de metales es un elemento sumamente práctico para la revisión de personas, ofreciendo grandes ventajas sobre el sistema de palpación manual. La sensibilidad del detector es regulable, permitiendo de esta manera establecer un volumen metálico mínimo, a partir del cual se activará la alarma.

Seguridad con animales:

Sirven para grandes extensiones de terreno, y además tienen órganos sensitivos mucho más sensibles que los de cualquier dispositivo y, generalmente, el costo de cuidado y mantenimiento se disminuye considerablemente utilizando este tipo de sistema. Así mismo, este sistema posee la desventaja de que los animales pueden ser engañados para lograr el acceso deseado.

Ubicación y protección física de los equipos y servidores.

Para minimizar el impacto de un posible problema físico tendremos que imponer condiciones de seguridad para los equipos y sistemas de la organización. Por otra lado para que los equipos informáticos funcionen correctamente deben de encontrarse en bajo ciertas condiciones.

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

- Se debe evitar el polvo y la electricidad estática.

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

- Se debe evitar el uso de techos falsos.

- Deben estar libres de cualquier amenaza contra inundación.

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

Sistemas de control de acceso:
- Llaves tradicionales
- Contraseñas: con su correspondiente polítca de contraseñas.
- Tarjetas magnéticas.
- Sistemas de identificación por radiofrecuencia:
- Sistemas de token: se compone de un elemento móvil que genera claves aleatorias.
- Sistemas biométricos.
- Sistemas de control de temperatura.

Dependiendo del entorno y los sistemas a proteger la seguridad física será más o menos importante y restrictiva, aunque siempre deberemos tenerla en cuenta.

A continuación mencionaremos algunos de los problemas de seguridad física con los que nos podemos enfrentar y las medidas que podemos tomar para evitarlos o al menos minimizar su impacto:

Protección del hardware

El hardware es frecuentemente el elemento más caro de todo sistema informático y por tanto las medidas encaminadas a asegurar su integridad son una parte importante de la seguridad física de cualquier organización.

Problemas a los que nos enfrentamos:

Acceso físico
Si alguien que desee atacar un sistema tiene acceso físico al mismo todo el resto de medidas de seguridad implantadas se convierten en inútiles.

Desastres naturales

Además de los posibles problemas causados por ataques realizados por personas, es importante tener en cuenta que también los desastres naturales pueden tener muy graves consecuencias, sobre todo si no los contemplamos en nuestra política de seguridad y su implantación.
Algunos desastres naturales a tener en cuenta:
-Terremotos y vibraciones
-Tormentas eléctricas
-Inundaciones y humedad
-Incendios y humos

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

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

Otro desastre natural importante son las tormentas con aparato eléctrico, especialmente frecuentes en verano, que generan subidas súbitas de tensión muy superiores a las que puedagenerar un problema en la red eléctrica.

Alteraciones del entorno

Deberemos contemplar problemas que pueden afectar el régimen de funcionamiento habitual de las máquinas como la alimentación eléctrica, el ruido eléctrico producido por los equipos o los cambios bruscos de temperatura.

Electricidad

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

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

Temperaturas extremas

Las temperaturas extremas, ya sea un calor excesivo o un frio intenso, perjudican gravemente a todos los equipos. En general es recomendable que los equipos operen entre 10 y 32 grados Celsius. Para controlar la temperatura emplearemos aparatos de aire acondicionado.

6. Sistema de alimentación ininterrumpida

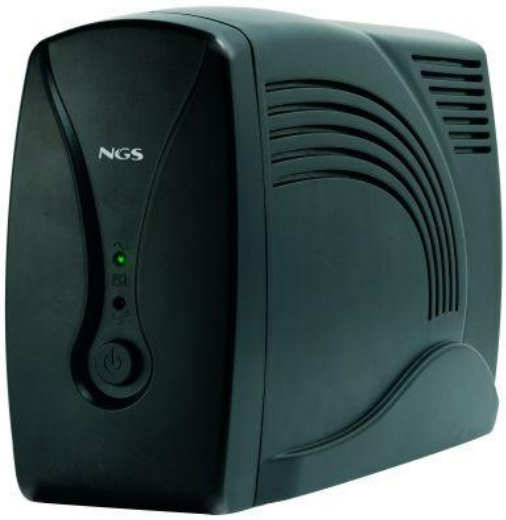
Un **sistema de alimentación ininterrumpida**, **SAI** es un dispositivo que gracias a sus baterías, puede proporcionar energía eléctrica tras un apagón a todos los dispositivos que tenga conectados. Otra de las funciones de los UPS es la de mejorar la calidad de la energía eléctrica que llega a las cargas, filtrando subidas y bajadas de tensión y eliminando armónicos de la red en el caso de usar corriente alterna.

Potencia

La unidad de potencia para configurar un SAI es el voltiamperio (VA) , que es la potencia aparente, o el vatio (W) que es la potencia activa, también denominada potencia efectiva o eficaz, consumida por el sistema. Para calcular cuánta energía requiere un equipo de UPS, se debe conocer el consumo del dispositivo. Si la que se conoce es la potencia efectiva o eficaz, en vatios, se multiplica la cantidad de vatios por 1,4 para tener en cuenta el pico máximo de potencia que puede alcanzar el equipo. Por ejemplo: 200 vatios x 1,4 = 280 VA. Si lo que encuentra es la tensión y la corriente nominales, para calcular la potencia aparente (VA) hay que multiplicar la corriente (amperios) por la tensión (voltios), por ejemplo: 3 amperios. x 220 voltios = 660 VA..

TIPOS DE SAI

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**.

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.

Sistemas biométricos:

Entenderemos por *sistema biométrico* a un sistema automatizado que realiza labores de biometría. Es decir, un sistema que fundamenta sus decisiones de reconocimiento mediante una característica personal que puede ser reconocida o verificada de manera automatizada. En esta sección son descritas algunas de las características más importantes de estos sistemas.

2.1. Modelo del proceso de identificación personal

Cualquier proceso de identificación personal puede ser comprendido mediante un modelo simplificado. Este postula la existencia de tres indicadores de identidad que definen el proceso de identificación:

1. **Conocimiento:** la persona tiene conocimiento (por ejemplo: un código),
2. **Posesión:** la persona posee un objeto (por ejemplo: una tarjeta), y
3. **Característica:** la persona tiene una característica que puede ser verificada (por ejemplo: una de sus huellas dactilares).

2.2. Características de un indicador biométrico

Un indicador biométrico es alguna característica con la cual se puede realizar biometría. Cualquiera sea el indicador, debe cumplir los siguientes requerimientos [4]:

1. **Universalidad***:* cualquier persona posee esa característica;
2. **Unicidad:** la existencia de dos personas con una característica idéntica tiene una probabilidad muy pequeña;
3. **Permanencia:** la característica no cambia en el tiempo; y
4. **Cuantificación:** la característica puede ser medida en forma cuantitativa.

2.3. Características de un sistema biométrico para identificación personal

Las características básicas que un sistema biométrico para identificación personal debe cumplir pueden expresarse mediante las restricciones que deben ser satisfechas. Ellas apuntan, básicamente, a la obtención de un sistema biométrico con utilidad práctica.

El desempeño, que se refiere a la exactitud, la rapidez y la robustez alcanzada en la identificación, además de los recursos invertidos y el efecto de factores ambientales y/u operacionales. El objetivo de esta restricción es comprobar si el sistema posee una exactitud y rapidez aceptable con un requerimiento de recursos razonable.

La aceptabilidad, que indica el grado en que la gente está dispuesta a aceptar un sistema biométrico en su vida diaria. Es claro que el sistema no debe representar peligro alguno para los usuarios y debe inspirar "confianza" a los mismos. Factores psicológicos pueden afectar esta última característica.

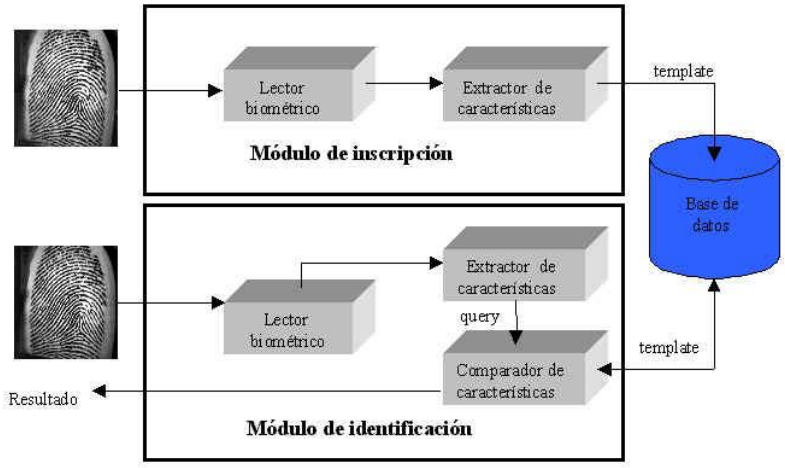
La fiabilidad, que refleja cuán difícil es burlar al sistema. El sistema biométrico debe reconocer características de una persona viva, pues es posible crear dedos de látex, grabaciones digitales de voz prótesis de ojos, etc.

2.4. Arquitectura de un sistema biométrico para identificación personal

Los dispositivos biométricos poseen tres componentes básicos. El primero se encarga de la adquisición análoga o digital de algún indicador biométrico de una persona, como por ejemplo, la adquisición de la imagen de una huella dactilar mediante un escáner.

El módulo de inscripción se encarga de adquirir y almacenar la información proveniente del indicador biométrico con el objeto de poder contrastar a ésta con la proporcionada en ingresos posteriores al sistema. Las labores ejecutadas por el módulo de inscripción son posibles gracias a la acción del lector biométrico y del extractor de características.

El primero se encarga de adquirir datos relativos al indicador biométrico elegido y entregar una representación en formato digital de éste. El segundo extrae, a partir de la salida del lector, características representativas del indicador.



Fase operacional de un sistema de identificación personal.

Un sistema biométrico en su fase operacional puede operar en dos modos:

1. *Modo de verificación, o*
2. *Modo de identificación*

Un sistema biométrico operando en el modo de verificación comprueba la identidad de algún individuo comparando la característica sólo con los templates del individuo. Por ejemplo, si una persona ingresa su nombre de usuario entonces no será necesario revisar toda la base de datos buscando el template que más se asemeje al de él, sino que bastará con comparar la información de entrada sólo con el template que está asociado al usuario.

2.6. Exactitud en la identificación: medidas de desempeño

La información provista por los templates permite particionar su base de datos de acuerdo a la presencia o no de ciertos patrones particulares para cada indicador biométrico. Las "clases" así generadas permiten reducir el rango de búsqueda de algún template en la base de datos. Sin embargo, los templates pertenecientes a una misma clase también presentarán diferencias conocidas como *variaciones intraclase*.

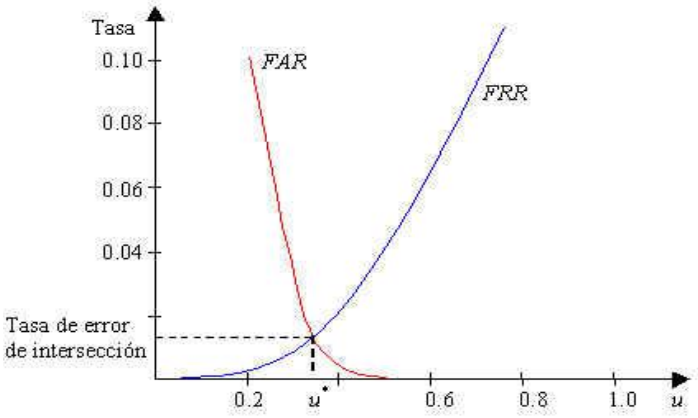
La información provista por los templates permite particionar su base de datos de acuerdo a la presencia o no de ciertos patrones particulares para cada indicador biométrico. Las "clases" así generadas permiten reducir el rango de búsqueda de algún template en la base de datos.

Por lo tanto existe un total de cuatro posibles respuestas del sistema:

1. Una persona autorizada es aceptada,
2. Una persona autorizada es rechazada,
3. Un impostor es rechazado,
4. Un impostor es aceptado.

Las salidas números 1 y 3 son correctas, mientras que las números 2 y 4 no lo son.

La *FAR* y la *FRR* son funciones del grado de seguridad deseado. En efecto, usualmente el resultado del proceso de identificación o verificación será un número real normalizado en el intervalo [0, 1], que indicará el "grado de parentesco" o correlación entre la característica biométrica proporcionada por el usuario y la(s) almacenada(s) en la base de datos.



3. Huellas dactilares

Una huella dactilar es la representación de la morfología superficial de la epidermis de un dedo. Posee un conjunto de líneas que, en forma global, aparecen dispuestas en forma paralela (colinas o *ridge lines* y *furrows*). Sin embargo estas líneas se intersectan y a veces terminan en forma abrupta. Los puntos donde las colinas terminan o se bifurcan se conocen técnicamente como minucias. Otros puntos singulares de una huella dactilar son aquellos donde la curvatura de los ridges es máxima. En primer lugar se

clasifica a la huella, es decir, se asigna a una clase previamente determinada de acuerdo a la estructura global de los ridges. El objetivo de esta etapa es establecer una partición en la base de datos con huellas.

COPIAS DE SEGUIRDAD:

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.

Tipos de copia de seguridad

La utilidad Copia de seguridad admite cinco métodos para hacer copia de seguridad de los datos del equipo o de la red.

Copia de seguridad de copia

Copia todos los archivos seleccionados pero no los marca individualmente como copiados (es decir, no desactiva el atributo de modificado). Este método es útil cuando desea realizar copias de seguridad de archivos entre copias de seguridad normales e incrementales, ya que no afecta a estas otras operaciones.

Copia de seguridad diaria

Copia todos los archivos seleccionados que se hayan modificado el día en que se realiza la copia diaria. Los archivos incluidos en la copia de seguridad no se marcan como copiados (es decir, no se desactiva el atributo de modificado).

Copia de seguridad diferencial

Copia los archivos creados o modificados desde la última copia de seguridad normal o incremental. Los archivos no se marcan como copiados (es decir, no se desactiva el atributo de modificado). Si realiza una combinación de copias de seguridad normal y diferencial, para restaurar los archivos y las carpetas debe disponer de la última copia de seguridad normal y de la última copia de seguridad diferencial.

Copia de seguridad incremental

Sólo copia los archivos creados o modificados desde la última copia de seguridad normal o incremental. Marca los archivos como copiados (es decir, se desactiva el atributo de modificado). Si usa una combinación de copias de seguridad normal e incremental, la restauración de los datos debe realizarse con el último conjunto copia de seguridad normal y todos los conjuntos de copia de seguridad incremental.

Copia de seguridad normal

Copia todos los archivos seleccionados y los marca como copiados (es decir, se desactiva el atributo de modificado). En las copias de seguridad normales sólo necesita la copia más reciente del archivo o la cinta que contiene la copia de seguridad para restaurar todos los archivos. Las copias de seguridad normales se suelen realizar al crear por primera vez un conjunto de copia de seguridad.

La combinación de copias de seguridad normales e incrementales utiliza el mínimo espacio de almacenamiento posible y es el método de copia de seguridad más rápido. Sin embargo, la recuperación de archivos puede ser difícil y laboriosa ya que el conjunto de copia de seguridad puede estar repartido entre varios discos o cintas.

Si realiza una copia de seguridad de sus datos empleando una combinación de copias de seguridad normales y diferenciales consumirá más tiempo, especialmente si los datos sufren cambios frecuentes, aunque será más fácil restaurar los datos ya que el conjunto de copia de seguridad sólo estará repartido en unos pocos discos o cintas.

MEDIOS DE ALMACENAMIENTO

Los materiales físicos en donde se almacenan los datos se conocen como medios de almacenamiento o soportes de almacenamiento.

Ejemplos :

-Discos magnéticos(disquetes, discos duros),

- Discos ópticos (CD, DVD),

- Cintas magnéticas,

- Discos magneto-ópticos (discos Zip, discos Jaz, SuperDisk),

- Tarjetas de memoria

- Y muchas más.

Los componentes de hardware que escriben o leen datos en los medios de

almacenamiento se conocen como dispositivos o unidades de almacenamiento.

CINTA MAGNETICA

La cinta magnética es un tipo de medio o soporte de almacenamiento de datos que se graba en pistas sobre una banda plástica con un material magnetizado, generalmente óxido de hierro o algún cromato. Hay diferentes tipos de cintas, tanto en sus medidas físicas, como en su constitución química, así como diferentes formatos de grabación, especializados en el tipo de información que se quiere grabar.

Su uso también se ha extendido para el almacenamiento analógico de música , casete y para vídeo, como las cintas de VHS.

La cinta magnética de audio dependiendo del equipo que la reproduce/graba

recibe distintos nombres:

-Se llama cinta de bobina abierta si es de magnetófono.

-Casete cuando es de formato compacto utilizada

en pletina o walkman.

DISCO MAGNETICO

Un disco magnético (flexible o duro) sirve como soporte de almacenamiento para archivos de información. Almacena los bytes de estos archivos en uno o varios sectores de pistas circulares.

COMPOSICION DE DISCO MAGNETICO.

Pistas circulares

Las pistas circulares son anillos concéntricos separados lo menos posible entre sí, existentes en sus dos caras recubiertas de una fina capa superficial de material magnetizable.

Estructura física del disco

La estructura física de un disco, con sus pistas y sectores se hallan invisibles en el disco. Estas pistas, invisibles, se crean durante el formateo. El formateo consiste en grabar (escribir) magnéticamente los sucesivos sectores que componen cada una de las pistas de un disco o disquete, quedando así ellas magnetizadas.

DISQUETE

Cartucho plástico para almacenar información. Se tratan de una clase de discos magnéticos. Las dos versiones más conocidas para PC son: la más antigua de 5 1/4 pulgadas y la de 3 1/2, prácticamente sin uso en la actualidad.

Son llamados discos flexibles, contrastando con los discos rígidos. La información en ellos contenida puede perderse o afectarse fácilmente con el tiempo, el polvo, la humedad, el magnetismo, el calor, etc. La versión de 5 1/4 podía llegar a almacenar hasta 1,2 MB. La versión 3 1/2 pulgadas almacenaban 1,44 MB como máximo.

Partes o componentes de un disquete

Como se puede ver en la imagen de la derecha (* imagen de dominio público), las diferentes partes de un disquete son:

1. Muesca para protección de escritura
2. Base central
3. Cubierta móvil
4. Chasís plástico
5. Anillo de papel
6. Disco magnético
7. Sector de disco

DISCO DURO

Un disco duro o disco rígido es un dispositivo de almacenamiento de datos no volátil que emplea un sistema de grabación magnética para almacenar datos digitales. Se compone de uno o más platos o discos rígidos, unidos por un mismo eje que gira a gran velocidad dentro de una caja metálica sellada. Sobre cada plato, y en cada una de sus caras, se sitúa un cabezal.

Para poder utilizar un disco duro, un sistema operativo debe aplicar un formato de bajo nivel que defina una o más particiones. La operación de formateo requiere el uso de una fracción del espacio disponible en el disco, que dependerá del formato empleado.

CARACTERISTICA DE DISCO DURO

Las características que se deben tener en cuenta en un disco duro son:
-**Tiempo medio de acceso:** Tiempo medio que tarda la aguja en situarse en la pista y el sector deseado; es la suma del Tiempo medio de búsqueda (situarse en la pista), Tiempo de lectura/escritura y la Latencia media (situarse en el sector).
-**Tiempo medio de búsqueda:** Tiempo medio que tarda la aguja en situarse en la pista deseada; es la mitad del tiempo empleado por la aguja en ir desde la pista más periférica hasta la más central del disco.
-**Tiempo de lectura/escritura:** Tiempo medio que tarda el disco en leer o escribir nueva información: Depende de la cantidad de información que se quiere leer o escribir, el tamaño de bloque, el número de cabezales, el tiempo por vuelta y la cantidad de sectores por pista.
-**Latencia media:** Tiempo medio que tarda la aguja en situarse en el sector deseado; es la mitad del tiempo empleado en una rotación completa del disco.
-**Velocidad de rotación:** Revoluciones por minuto de los platos. A mayor velocidad de rotación, menor latencia media.

TIPOS DE CONEXIÓN

Si hablamos de disco duro podemos citar los distintos tipos de conexión que poseen los mismos con la placa base, es decir pueden ser SATA, IDE,SCSI o SAS:

-**IDE:** ("Dispositivo electrónico integrado") o ATA controla los dispositivos de almacenamiento masivo de datos, como los discos duros. Son planos, anchos y alargados.

SCSI: Son interfaces preparadas para discos duros de gran capacidad de almacenamiento y velocidad de rotación.

SATA (Serial ATA): El más novedoso de los estándares de conexión, utiliza un bus serie para la transmisión de datos. Notablemente más rápido y eficiente que IDE.

DIRECCIONAMIENTO DE DISCO DURO

Hay varios conceptos para referirse a zonas del disco:
-Plato: cada uno de los discos que hay dentro del disco duro.
-Cara: cada uno de los dos lados de un plato.
-Cabeza: número de cabezales.
-Pistas: una circunferencia dentro de una cara; la pista 0 está en el borde exterior.
-Cilindro: conjunto de varias pistas; son todas las circunferencias que están alineadas verticalmente (una de cada cara).
-Sector : cada una de las divisiones de una pista. El tamaño del sector no es fijo, siendo el estándar actual 512 bytes, aunque próximamente serán 4 KiB.

DISCO DURO EXTERNO

Un disco duro portátil (o disco duro externo) es un disco duro que es fácilmente transportable de un lado a otro sin necesidad de consumir energía eléctrica o batería.

DISCO ÓPTICO

Un disco óptico es un formato de almacenamiento de datos digital, que consiste en un disco circular en el cual la información se codifica , se guarda y almacena, haciendo unos surcos microscópicos con un láser sobre una de las caras planas que lo componen.

CD-ROM

Un CD-ROM Es un prensado disco compacto que contiene los datos de acceso, pero sin permisos de escritura, un equipo de almacenamiento y reproducción de música.

La Unidad de CD-ROM debe considerarse obligatoria en cualquier computador que se ensamble o se construya actualmente, porque la mayoría del software se distribuye en CD-ROM. Algunas de estas unidades leen CD-ROM y graban sobre los discos compactos de una sola grabada (CD-RW).

DVD

El DVD es un disco óptico de almacenamiento de datos cuyo estándar surgió en . Sus siglas corresponden con Digital Versatile Disc en inglés (disco versátil digital traducido al español). En sus inicios, la v intermedia hacía referencia a video (digital videodisk), debido a su desarrollo como reemplazo del formato VHS para la distribución de vídeo a los hogares.
Unidad de DVD: el nombre de este dispositivo hace referencia a la multitud de maneras en las que se almacenan los datos: DVD-ROM (dispositivo de lectura únicamente), DVDR y DVD+R (solo pueden escribirse una vez), DVD-RW y DVD+RW (permiten grabar y borrar las veces que se quiera). También difieren en la capacidad de almacenamiento de cada uno de los tipos.

DVD-R

Un DVD-R o DVD-Recordable (DVD-Grabable) es un disco óptico en el que se puede grabar o escribir datos con mucha mayor capacidad de almacenamiento que un CD-R, normalmente 4.7 GB (en lugar de los 700 MB de almacenamiento estándar de los CD), también ha desarrollado una versión de doble capa con 8,5 GB. Un DVD-R sólo puede grabarse una vez, mientras que un DVD-RW es regrabable.

Dvd+R

El DVD+R (+ Grabable) es un disco óptico grabable sólo una vez. Este formato de disco Técnicamente el formato DVD+R es superior al DVD-R entre otros motivos por ofrecer mejor soporte a la unidad grabadora para detectar y corregir errores.
Al día de hoy un 85% de los lectores y grabadores son compatibles con ambos formatos.

DVD-RW

Un DVD-RW (Menos Regrabable) es un DVD regrabable en el que se puede grabar y borrar la información varias veces. La capacidad estándar es de 4,7 GB.
El DVD-RW es análogo al CD-RW, por lo que permite que su información sea grabada, borrada y regrabada varias veces, esto es una ventaja respecto al DVD-R, ya que se puede utilizar como un disquete de 4,7 GB y también ahorra tener que adquirir más discos para almacenar nueva información pues se puede eliminar la antigua almacenada en el dvd.

BLUE –RAY DISC

También conocido como Blu-ray o BD, es un formato de disco óptico de nueva generación de 12 cm de diámetro (igual que el CD y el DVD) para vídeo de gran definición y almacenamiento de datos de alta densidad. Su capacidad de almacenamiento llega a 25 GB por capa. Aunque otros apuntan que el sucesor del DVD no será un disco óptico, sino la tarjeta de memoria.

TARJETAS DE MEMORIA

Una tarjeta de memoria o tarjeta de memoria flash es un dispositivo de almacenamiento que conserva la información que le ha sido almacenada de forma correcta aun con la pérdida de energía, es decir, es una memoria no volátil.

SECURE DIGITAL

Secure Digital (SD) es un formato de tarjeta de memoria inventado por Panasonic. Se utiliza en dispositivos portátiles tales como cámaras fotográficas digitales, PDA, teléfonos móviles, computadoras portátiles e incluso videoconsolas (tanto de sobremesa como portátiles), entre muchos otros.

MICRODRIVE

El Microdrive es en realidad un disco duro de una pulgada que suele ser empaquetado y habilitado con interfaces CompactFlash o IDE/ATA según el uso al que se desee destinar la unidad. Normalmente, es usado en las tarjetas CompactFlash de tipo 2. La única diferencia entre éstas y las de tipo 1, es que son ligeramente más gruesas (5 mm) mientras las de tipo 1 con de tan solo 3,5 mm.

SMARTMEDIA

SmartMedia es una tarjeta de memoria estándar desarrollada por Toshiba en 1995 para competir con las CompactFlash, las PC Card y las MiniCard, uno de los más difundidos de almacenamiento de imágenes junto con las tarjetas CompactFlash. La SmartMedia era una de las primeras tarjetas de memoria más pequeñas y delgadas, se usaba como almacenaje de dispositivo portátil, para sacarla fácilmente y usarla en un PC. Fue popular en cámara digital.

XD-PICTURE CARD

La xD-Picture Card es un formato de tarjeta de memoria desarrollada por Olympus y Fujifilm y utilizadas para sus cámaras de fotos digitales. Actualmente se las puede encontrar en 8 diferentes modelos: 16MB, 32MB, 64MB, 128MB, 256MB, 512MB, 1GB y 2GB.

UNIDAD DE ESTADO SÓLIDO

Una unidad de estado sólido o SSD Es un dispositivo de almacenamiento de datos que usa una memoria no volátil, como la memoria flash, o una memoria volátil como la SDRAM, para almacenar datos, en lugar de los platos giratorios magnéticos encontrados en los discos duros convencionales. En comparación con los discos duros tradicionales, las unidades de estado sólido son menos susceptibles a golpes, son prácticamente inaudibles y tienen un menor tiempo de acceso y de latencia.

Almacenamiento redundante y distribuido: RAID y Centros de Respaldo.

Raid

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.

RAID 0

También llamado partición de los discos, los datos son distribuidos a través de discos paralelos. RAID 0 distribuye los datos rápidamente a los usuarios, pero no ofrece más protección a fallas de hardware que un simple disco.

El RAID 0 se usa normalmente para incrementar el rendimiento, aunque también puede utilizarsecomo forma de crear un pequeño número de grandes discos virtuales a partir de un gran número de pequeños discos físicos.

Debido a su alta velocidad, pero hay que tener en cuenta de que si un disco rompe, se pierde absolutamente TODA la información de TODOS los discos.

RAID 1

También llamado Disk espejo provee la más alta medida de protección de datos a través de una completa redundancia. Los datos son copiados a dos discos simultáneamente. La disponibilidad es alta pero el costo también dado que los usuarios deben comprar dos veces la capacidad de almacenamiento que requieren.

Esto resulta útil cuando el rendimiento en lectura es más importante que la capacidad. Adicionalmente, dado que todos los datos están en dos o más discos, con hardwarehabitualmente independiente, el rendimiento de lectura se incrementa aproximadamente como múltiplo lineal del número del copias; es decir, un RAID 1 puede estar leyendo simultáneamente dos datos diferentes en dos discos diferentes, por lo que su rendimiento se duplica.

RAID 0+1

Combina Disk espejo y partición de datos. El resultado es gran disponibilidad al más alto

desempeño de entrada y de salida para las aplicaciones de negocios más criticas. A este nivel como

en el RAID 1 los discos son duplicados. Dado que son relativamente no costosos, RAID 0/1 es una alternativa para los negocios que necesitan solamente uno o dos discos para sus datos, sin embargo, el costo puede convertirse en un problema cuando se requieren más de dos discos. Combina el RAID 0 y el RAID 1. RAID (0+1) permite la perdida de múltiples discos debido a la redundancia de discos duros.

RAID 2

Un RAID 2 divide los datos a nivel de bits en lugar de a nivel de bloques y usa un código de Hamming para la corrección de errores. Los discos son sincronizados por la controladora para funcionar al unísono. Éste es el único nivel RAID original que actualmente no se usa. Permite tasas de trasferencias extremadamente altas.

RAID 3

Logra redundancia sin espejo completo. El flujo de los datos es particionado a través de todos los HD de datos en el arreglo. La información extra que provee la redundancia está escrita en un HD dedicado a la paridad. Si cualquier HD del arreglo falla, los datos perdidos pueden ser reconstruidos matemáticamente desde los miembros restantes del arreglo. RAID 3 es especialmente apropiado para procesamiento de imagen, colección de datos científicos, y otras aplicaciones en las cuales grandes bloques de datos guardados secuencialmente deben ser transferidos rápidamente.

RAID 5

Todos los HD en el arreglo operan independientemente. Un registro entero de datos es almacenado en un solo disco, permitiendo al arreglo satisfacer múltiples requerimientos de entrada y salida al mismo tiempo. La información de paridad está distribuida en todos los discos, aliviando el cuello de botella de acceder un solo disco de paridad durante operaciones de entrada y salida concurrentes. RAID 5 está bien recomendado para procesos de transacciones on-line, automatización de oficinas, y otras aplicaciones caracterizadas por gran numero de requerimientos concurrentes de lectura.

RAID 10

La información se distribuye en bloques como en RAID-0 y adicionalmente, cada disco se duplica como RAID-1, creando un segundo nivel de arreglo. Se conoce como "striping de arreglos duplicados". Se requieren, dos canales, dos discos para cada canal y se utiliza el 50% de la capacidad para información de control. Este nivel ofrece un 100% de redundancia de la información y un soporte para grandes volúmenes de datos, donde el precio no es un factor importante. Ideal para sistemas de misión crítica donde se requiera mayor confiabilidad de la información, ya que pueden fallar dos discos inclusive (uno por cada canal) y los datos todavía se mantienen en línea. Es apropiado también en escrituras aleatorias pequeñas.

7.3.3. Almacenamiento remoto: SAN, NAS y almacenamietno clouding.

a) SAN.

Una red de área de almacenamiento, en inglés SAN (storage area network), es una red concebida para conectar servidores, matrices (arrays) de discos y librerías de soporte. Principalmente, está basada en tecnología fibre channel y más recientemente en iSCSI. Su función es la de conectar de manera rápida, segura y fiable los distintos elementos que la conforman.

Una red SAN se distingue de otros modos de almacenamiento en red por el modo de acceso a bajo nivel. El tipo de tráfico en una SAN es muy similar al de los discos duros como ATA,SATA y SCSI.

La mayoría de las SAN actuales usan el protocolo SCSI para acceder a los datos de la SAN, aunque no usen interfaces físicas SCSI. Este tipo de redes de datos se han utilizado y se utilizan tradicionalmente en grandes main frames como en IBM, SUN o HP.

Una SAN es una red de almacenamiento dedicada que proporciona acceso de nivel de bloque a LUNs. Un LUN, o número de unidad lógica, es un disco virtual proporcionado por la SAN. El administrador del sistema tiene el mismo acceso y los derechos a la LUN como si fuera un disco directamente conectado a la misma.

Las SAN se componen de tres capas:

-Capa Host. Esta capa consiste principalmente en Servidores, dispositivos ó componentes (HBA,GBIC, GLM) y software (sistemas operativos).

-Capa Fibra. Esta capa la conforman los cables (Fibra óptica) así como los SAN Hubs y los SAN switches como punto central de conexión para la SAN.

-Capa Almacenamiento. Esta capa la componen las formaciones de discos (Disk Arrays, Memoria Caché, RAIDs) y cintas empleados para almacenar datos.

a) NAS.

NAS (del inglés Network Attached Storage) es el nombre dado a una tecnología de

almacenamiento dedicada a compartir la capacidad de almacenamiento de un ordenador (Servidor)

con ordenadores personales o servidores clientes a través de una red (normalmente TCP/IP),

haciendo uso de un Sistema Operativo optimizado para dar acceso con los protocolos CIFS, NFS, FTP o TFTP.

Generalmente, los sistemas NAS son dispositivos de almacenamiento específicos a los que se accede desde los equipos a través de protocolos de red (normalmente TCP/IP). También se podría considerar un sistema NAS a un servidor (Linux, Windows,...) que comparte sus unidades por red, pero la definición suele aplicarse a sistemas específicos.

Los protocolos de comunicaciones NAS están basados en ficheros por lo que el cliente solicita el fichero completo al servidor y lo maneja localmente, están por ello orientados a información almacenada en ficheros de pequeño tamaño y gran cantidad. Los protocolos usados son protocolos de compartición de ficheros como NFS, Microsoft Common Internet File System (CIFS).

El precio de las aplicaciones NAS ha bajado en los últimos años, ofreciendo redes dealmacenamiento flexibles para el consumidor doméstico con costos menores de lo normal, con discos externos USB o FireWire.

a) Almacenamiento Clouding.

El almacenamiento en la nube también es conocido como discos duros virtuales (no confundir con unidades virtuales). Un disco duro virtual es un espacio en un servidor que vamos a utilizar para guardar nuestros archivos. Es como si tuviéramos varios ordenadores conectados en red y en uno de ellos creamos una partición para guardar nuestros archivos. Esta información está accesible en un ordenador mediante internet.

En la red hay varias empresas que alquilan espacio en sus servidores, también hay páginas o empresas que ofrecen este servicio de forma gratuita, normalmente financiados mediante publicidad.

El acceso a estos discos se pude hacer de varias formas, siendo las principales mediante IP (trabajarían igual que una unidad más, y es lo que realmente sería un Cloud Storage), páginas web o FTP.

Las principales ventajas del almacenamiento en la nube son:

-Las empresas sólo tendrán que pagar por el almacenamiento que realmente utilizan.

-Nos es necesario instalar en las empresas dispositivos de almacenamiento físico en su propio centro de datos u oficinas, lo que reduce los costos de TI y hosting.

-Las tareas mantenimiento del almacenamiento, tales como copia de seguridad, replicación de datos, y la compra de dispositivos de almacenamiento adicionales quedan bajo la responsabilidad de un proveedor de servicios, permitiendo a las organizaciones centrarse en su negocio principal.

Políticas de Almacenamiento.

a. Almacenamiento primario. Se realiza en los servidores con los sistemas operativos: UNIX, WINDOWS 2003 SERVER, LINUX SUSE, LINUX RED HAT.
- Almacenamiento en los discos duros de los servidores

- Arreglo de discos en modelos RAI para los servidores LINUX SUSE y WINDOWS 2003 SERVER
b. Almacenamiento secundario Utilizando Unidad de Cinta con dos unidades formato LTO3 de 800GB y cintas magnéticas 400/800 GB.

c. Backup de usuarios Se tiene una estructura en el servidor WINDOWS 2003

SERVER, en la cual se crearon carpetas con el nombre de cada usuario de la red LAN, a ese "home" solo tiene acceso el usuario que inicie su sesión de red y en el puede guardar y actualizar permanentemente la información que considere importante y la cual debe guardarse en copia de seguridad.

d. Capacitación y divulgación
Se tienen instructivos para el manejo de:

- Correo electrónico interno y externo utilizando zimbra
- Mensajería Instantánea. Spark

IDENTIFICACION, AUTENTICACION Y AUTORIZACIÓN

Se denomina Identificación al momento en que el usuario se da a conocer en el sistema; y Autenticación a la verificación que realiza el sistema sobre esta identificación. 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 Al igual que se consideró para la seguridad física, y basada en ella, existen cuatro tipos de técnicas que permiten realizar la autenticación de la identidad del usuario, las cuales pueden ser utilizadas individualmente o combinadas:

La Seguridad Informática se basa, en gran medida, en la efectiva administración de los permisos de acceso a los recursos informáticos, basados en la identificación, autenticación y autorización de accesos.

Esta administración abarca:
-Proceso de solicitud, establecimiento, manejo, seguimiento y cierre de las cuentas de usuarios. Es necesario considerar que la solicitud de habilitación de un permiso de acceso para un usuario determinado, debe provenir de su superior y, de acuerdo con sus

requerimientos específicos de acceso, debe generarse el perfil en el sistema de seguridad, en el sistema operativo o en la aplicación según corresponda.

Revisiones periódicas sobre la administración de las cuentas y los permisos de acceso establecidos. Las mismas deben encararse desde el punto de vista del sistema operativo, y aplicación por aplicación, pudiendo ser llevadas a cabo por personal de auditoría o por la gerencia propietaria del sistema; siempre sobre la base de que cada usuario disponga del mínimo permiso que requiera de acuerdo con sus funciones.

Nuevas consideraciones relacionadas con cambios en la asignación de funciones del empleado. Para implementar la rotación de funciones, o en caso de reasignar funciones por ausencias temporales de algunos empleados, es necesario considerar la importancia de mantener actualizados los permisos de acceso.

Procedimientos a tener en cuenta en caso de desvinculaciones de personal con la organización, llevadas a cabo en forma amistosa o no. Los despidos del personal de sistemas presentan altos riesgos ya que en general se trata de empleados con capacidad para modificar aplicaciones o la configuración del sistema, dejando "bombas lógicas" o destruyendo sistemas o recursos informáticos.

POLITICAS DE CONTRASEÑAS

Política y acciones para construir contraseñas seguras:

1. Se deben utilizar al menos 8 caracteres para crear la clave. Según 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. 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”.

   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”)

Auditorias de seguridad informática .

Concepto auditoria

Una auditoría de seguridad informática o auditoría de seguridad de sistemas de información (SI) es el estudio que comprende el análisis y gestión de sistemas llevado a cabo por profesionales generalmente por Ingenieros o Ingenieros Técnicos en Informática para identificar, enumerar y posteriormente describir las diversas vulnerabilidades que pudieran presentarse en una revisión exhaustiva de las estaciones de trabajo, redes de comunicaciones o servidores.

TIPOS DE AUDITORIA

Los servicios de auditoría pueden ser de distinta índole:
- **Auditoría de seguridad interna**. En este tipo de auditoría se contrasta el nivel de seguridad y privacidad de las redes locales y corporativas de carácter interno
- **Auditoría de seguridad perimetral.** En este tipo de análisis, el perímetro de la red local o corporativa es estudiado y se analiza el grado de seguridad que ofrece en las entradas exteriores
- **Test de intrusión.** El test de intrusión es un método de auditoría mediante el cual se intenta acceder a los sistemas, para comprobar el nivel de resistencia a la intrusión no deseada. Es un complemento fundamental para la auditoría perimetral.
- **Análisis forense.** El análisis forense es una metodología de estudio ideal para el análisis posterior de incidentes, mediante el cual se trata de reconstruir cómo se ha penetrado en el sistema, a la par que se valoran los daños ocasionados. Si los daños han provocado la inoperabilidad del sistema, el análisis se denomina análisis postmortem.

Criptografía.

Criptografía es el estudio de las técnicas matemáticas relativos a los aspectos de seguridad información, tales técnicas abarcan: confidencialidad, integridad de los datos, autenticación de la entidad, y autenticación del origen de los

datos. Sin embargo la criptografía no pretende proveer los medios para asegurar la información, sino ofrecer las técnicas para lograr este aseguramiento.

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.

Objetivos

Los objetivos básicos de la criptografía son los siguientes:

· **Confidencialidad:** es un servicio es usado para mantener el contenido de la información exclusivo únicamente para quien debe leerlo o quién está autorizado el error.

Integridad de los datos: con ese servicio se pretende mantener la información y modificable por parte de personal no autorizado se logra que información se mantenga a largo del tránsito de toda la comunicación para lograrlo se debe tener la habilidad de detectar cualquier cambio no autorizado en el tránsito de la información estos cambios abarcan desde la inserción información el borrado sustitución de información original.

Autenticación: este segmento abarcan tanto la información como las entidades participantes en la comunicación cada una de las partes de poder identificar plenamente adicionalmente la información de poderse garantiza que fue la enviada originalmente.

No repudiación: implica que ninguna de las partes puede negar la recepción información u el envío de información ejemplo: yo prometo que voy a comprar un artículo el día de mañana. A un precio de 100, y al llegar al momento, digo que prometí comprar por menor valor, si existen mecanismos de no repudiación yo no puedo cambiar las cantidades ni los tiempos de la promesa. Para lograr dichos objetivos la criptografía se vale conjunto básico de elementos denominadas primitivas criptográficas, las cuales se evalúan con respecto a varios criterios estos son:

-nivel de seguridad
-funcionalidad
- métodos de operación
- desempeño
- facilidades implementación

CIFRADO Y DESCIFRADO

Cifrado El cifrado es un método que permite aumentar la seguridad de un mensaje o de un archivo mediante la codificación del contenido, de manera que sólo pueda leerlo la persona que cuente con la clave de cifrado adecuada para descodificarlo.

Métodos y Técnicas de Cifrado

Cifrado de sustitución

El cifrado de sustitución consiste en reemplazar una o más entidades (generalmente letras) de un mensaje por una o más entidades diferentes.

Existen varios tipos de criptosistemas de sustitución:

-La sustitución monoalfabética consiste en reemplazar cada una de las letras del mensaje por otra letra del alfabeto.
-La sustitución polialfabética consiste en utilizar una serie de cifrados monoalfabéticos que son re-utilizados periódicamente.
- La sustitución homófona hace posible que cada una de las letras del mensaje del texto plano se corresponda con un posible grupo de caracteres distintos.

-La sustitución poligráfica consiste en reemplazar un grupo de caracteres en un mensaje por otro grupo de caracteres.

Cifrado ROT 13 El caso específico del cifrado César donde la clave de cifrado es N (la 13º letra del alfabeto) se denomina ROT 13 (se eligió el número 13, la mitad de 26, para que sea posible cifrar y descifrar fácilmente mensajes textuales).

Cifrado de Transposición El método de cifrado por transposición consiste en reordenar datos para cifrarlos a fin de hacerlos ininteligibles. Esto puede significar, por ejemplo, reordenar los datos geométricamente para hacerlos visualmente inutilizables.

El Cifrado Simétrico.

El cifrado simétrico (también conocido como cifrado de clave privada o cifrado de clave secreta) consiste en utilizar la misma clave para el cifrado y el descifrado. El cifrado consiste en aplicar una operación (un algoritmo) a los datos que se desea cifrar utilizando la clave privada para hacerlos ininteligibles. El algoritmo más

simple (como un OR exclusivo) puede lograr que un sistema prácticamente a prueba de falsificaciones (asumiendo que la seguridad absoluta no existe).

El Cifrado Asimétrico.

El cifrado asimétrico (también conocido como cifrado con clave pública). En un criptosistema asimétrico (o criptosistema de clave pública), las claves se dan en pares:
-Una clave pública para el cifrado;
- Una clave secreta para el descifrado.

En un sistema de cifrado con clave pública, los usuarios eligen una clave aleatoria que sólo ellos conocen (ésta es la clave privada). A partir de esta clave, automáticamente se deduce un algoritmo (la clave pública). Los usuarios intercambian esta clave pública mediante un canal no seguro.