TIC06 SEGURIDAD INFORMÁTICA

1. INTRODUCCION

Nuestro mundo está repleto de sistemas compuestos por máquinas y por programas. Muchos de esos sistemas (por ejemplo, los ordenadores) forman parte de redes privadas o públicas, grandes o pequeñas, interconectadas entre sí. Internet, probablemente, es un ejemplo del sistema más complejo que se haya desarrollado jamás.

Cada día, más y más personas mal intencionadas, intentan tener acceso a los datos de nuestros ordenadores (sistemas). El acceso no autorizado a una red informática o a los equipos que en ella se encuentran pueden ocasionar en la gran mayoría de los casos graves problemas. Entre las posibles consecuencias de una intrusión se pueden citar la pérdida de datos (es un hecho frecuente y ocasiona muchos trastornos, sobre todo si no estamos al día de las copias de seguridad. Y aunque estemos al día, no siempre es posible recuperar la totalidad de los datos) o el robo de información sensible y confidencial (la divulgación de la información que posee una empresa sobre sus clientes puede acarrear demandas millonarias contra esta, o un ejemplo mas cercano es el de nuestras contraseñas de las cuentas de correo por las que intercambiamos información con otros).

Ahora bien, la complejidad de esos sistemas, hace que sea muy difícil conseguir un sistema totalmente seguro y que se aproveche esa complejidad para atacar dichos sistemas. La seguridad informática tiene como objetivo conseguir la seguridad más completa para los sistemas y redes de comunicación.

Se entiende por **seguridad informática** al conjunto de normas, procedimientos y herramientas, que tienen como objetivo garantizar la disponibilidad, integridad, confidencialidad y buen uso de la información que reside en un sistema de información.

Con la constante evolución de las computadoras es fundamental saber que recursos necesitar para obtener seguridad en los sistemas de información. Existen muchos y variados mecanismos de seguridad informática. Su selección depende del tipo de sistema, de su

función y de los factores de riesgo que lo amenazan.

2. LA SEGURIDAD INFORMÁTICA

Se entiende por **seguridad informática** al conjunto de normas, procedimientos y herramientas, que tienen como objetivo garantizar la disponibilidad, integridad, confidencialidad y buen uso de la información que reside en un sistema de información.

El objetivo de la seguridad informática consiste en asegurar que los recursos del sistema de información (material informático o programas) de una organización sean utilizados de la manera que se decidió y que el acceso a la información allí contenida, así como su modificación, sólo sea posible a las personas que se encuentren acreditadas y dentro de los límites de su autorización.

2.1. Principios de Seguridad Informática

Para que un sistema informático pueda considerarse seguro debe garantizar las siguientes características:

- **Confidencialidad**: La confidencialidad hace referencia a la privacidad de los elementos de información almacenados y procesados en un sistema informático. Basándose en este principio, las herramientas de seguridad informática deben proteger el sistema de invasiones y accesos por parte de personas o programas no autorizados. Este principio es particularmente importante en sistemas distribuidos (aquellos en los que los usuarios, computadores y datos residen en lugares diferentes, pero están física y lógicamente interconectados). ~~Dicho de otra manera, un sistema es confidencial si impide la visualización de datos a los usuarios que no tengan privilegios en el sistema.~~
- **Integridad**: La integridad hace referencia a la validez y consistencia de los elementos de información almacenados y procesados en un sistema informático. Basándose en este principio, las herramientas de seguridad informática deben asegurar que los

procesos de actualización estén bien sincronizados y no se dupliquen, de forma que todos los elementos del sistema manipulen adecuadamente los mismos datos. Este principio es importante en sistemas descentralizados (aquellos en los que diferentes usuarios, computadores y procesos comparten la misma información). ~~Un sistema es integro cuando se impide la modificación de la información a cualquier usuario que no ha sido autorizado con anterioridad.~~

- **Disponibilidad**: La disponibilidad hace referencia a la continuidad de acceso a los elementos de información almacenados y procesados en un sistema informático. Basándose en este principio, las herramientas de seguridad informática deber reforzar la permanencia del sistema informático, en condiciones de actividad adecuadas para que los usuarios accedan a los datos con la frecuencia y dedicación que requieran, este principio es importante en sistemas informáticos cuyos compromiso con el usuario, es prestar servicio permanente. El concepto de disponibilidad hace referencia a la posibilidad de que un sistema sea accesible y esté disponible para ser utilizado.

La seguridad informática es el conjunto de acciones, herramientas y dispositivos cuyo objetivo es dotar a un sistema informático de integridad, confidencialidad y disponibilidad.

2.2. Principales amenazas

Las principales amenazas de un sistema informático son las siguientes:

- **Los usuarios**: que, a menudo, con sus acciones (descargar archivos, abrir correos sospechosos, borrar archivos del sistema, etc.), premeditadas o no, desencadenan episodios de vulnerabilidad del sistema.
- **Los intrusos**: que ingresan al sistema sin autorización con propósitos perjudiciales.
- **El Software malicioso (malware)**: se trata de software creado para instalarse en un ordenador ajeno sin el conocimiento del usuario. Su finalidad consiste en obtener información y en ralentizar el funcionamiento o destruir archivo.
- **Los accidentes, averías y siniestros (incendios, inundaciones, etc.)**: que tienen un

efecto devastador para cualquier sistema informático.

La seguridad informática utiliza un sinfín de recursos para paliar los efectos de las amenazas y los riesgos. Entre ellos se pueden citar la realización de copias de seguridad, la instalación de programas antivirus, la encriptación de datos, los cortafuegos, etc.

4. SEGURIDAD ACTIVA Y PASIVA

La seguridad se puede clasificar desde distintos puntos de vista:

- Desde el punto de vista del activo a proteger, entendiendo como activo cualquier elemento del sistema de información necesario para el correcto funcionamiento de la actividad de la empresa, se puede distinguir entre seguridad física y seguridad lógica.

    - La **seguridad física** es aquella que trata de proteger el hardware (los equipos informáticos, el cableado, etc.) de los posibles desastres naturales (terremotos, tifones, etc.), incendios, inundaciones, sobrecargas eléctricas, robos y un sinfín de amenazas más.
    - La **seguridad lógica** complementa a la seguridad física, protegiendo el software de los equipos informáticos (es decir, las aplicaciones y los datos de los usuarios) de robos, pérdida de datos, entrada de virus informáticos, modificaciones no autorizadas de los datos, ataques desde la red, etc.

- Desde el punto de vista del momento preciso de actuación, se puede distinguir entre seguridad activa y seguridad pasiva.

    - La **seguridad activa** interviene antes de producirse el percance, de tal manera que se eviten los daños en el sistema. La seguridad activa la podemos definir como el conjunto de medidas que previenen e intentan evitar los daños en los sistemas informáticos.

- La **seguridad pasiva** actúa después del percance, minimizando los efectos ocasionados por el mismo. La seguridad pasiva complementa a la seguridad activa y se encarga de minimizar los efectos que haya ocasionado algún percance.

Entre las técnicas de seguridad activa y pasiva más utilizadas se pueden citar las siguientes:

- **Técnicas de Seguridad Activa** (tienen como finalidad evitar daños a los sistemas informáticos)
  - Empleo de contraseñas seguras.
  - Encriptación de datos.
  - Uso de software de seguridad informática.
  - Firmas y certificados.
- **Técnicas de Seguridad Pasiva** (tienen como finalidad minimizar los efectos o desastres causados por un accidente, usuario o malware).
  - Uso de hardware y dispositivos físicos de protección adecuados.
  - Realización de copias de seguridad.
  - Particiones del disco duro.
  - Conjunto de discos redundantes.

4. SEGURIDAD ACTIVA

La seguridad se puede clasificar en seguridad activa y seguridad pasiva. La seguridad activa tiene como finalidad evitar daños a los sistemas informáticos. Entre las técnicas de seguridad activa, se pueden citar:

- Empleo de contraseñas seguras.
- Encriptación de datos.
- Uso de software de seguridad informática.

- Firmas y certificados.

4.1. Las contraseñas

Las contraseñas (passwords) son las herramientas más utilizadas para restringir el acceso a los sistemas informáticos. Su misión es prevenir el acceso a los recursos por parte de personas no autorizadas. Sin embargo, sólo son efectivas si se escogen con cuidado y se cambian periódicamente.

Es muy importante cambiar periódicamente la contraseñas. En los sistemas informáticos, mantener una buena política de seguridad de creación, mantenimiento y recambio de claves es un punto crítico para salvaguardar la seguridad y privacidad.

Nota: La mayor parte de los usuarios de computadoras eligen contraseñas que son fáciles de adivinar (el nombre de un familiar o el de una mascota, palabras relacionadas con trabajos o aficiones, caracteres consecutivos del teclado, etc.). Los hackers conocen y explotan este hecho, por lo que un usuario precavido no debe utilizarlos. Muchos sistemas de seguridad no permiten que los usuarios utilicen palabras reales o nombres como contraseñas, evitando así que los hackers puedan usar diccionarios o programas especiales para adivinarlas. Los diccionarios son archivos con millones de palabras, las cuales pueden ser posibles passwords de los usuarios. Este archivo es utilizado para descubrir dicha password en pruebas de fuerza bruta.

Criterios para elegir una buena contraseña

A la hora de elegir una contraseña, hay que tener en cuenta los siguientes consejos:

- No utilizar contraseñas que sean palabras (aunque sean extranjeras) o nombres (el del usuario, miembros de la familia, mascotas, personajes de ficción, marcas, ciudades, etc.).
- No usar contraseñas completamente numéricas con algún significado (número de

teléfono, D.N.I., fecha de nacimiento, etc.).

- No utilizar terminología técnica conocida.
- Elegir una contraseña que mezcle caracteres alfabéticos (mayúsculas y minúsculas) y numéricos. Combine letras, números y símbolos. Cuanto más diversos sean los tipos de caracteres de la contraseña, más difícil será adivinarla.
- Deben ser largas (de 8 caracteres o más).
- Tener contraseñas diferentes en máquinas diferentes y sistemas diferentes. Es posible usar una contraseña base y ciertas variaciones lógicas de la misma para distintas máquinas. Esto permite que si una password de un sistema cae no caigan todos los demás sistemas por utilizar la misma password.
- Deben ser fáciles de recordar para no verse obligado a escribirlas. Algunos ejemplos son:
  - Combinar palabras cortas con algún número o carácter de puntuación: soy2_yo3
  - Usar un acrónimo de alguna frase fácil de recordar: A río Revuelto Ganancia de Pescadores: ArRGdP.
  - Añadir un número al acrónimo para mayor seguridad: A9r7R5G3d1P.
  - Mejor incluso si la frase no es conocida: Hasta Ahora no he Olvidado mi Contraseña: aHoelIo.
  - Elegir una palabra sin sentido, aunque pronunciable: taChunda72, AtajulH, Wen2Mar.
  - Realizar reemplazos de letras por signos o números: En Seguridad Más Vale Prevenir que Curar.

Algunos consejos a seguir:

- No permitir ninguna cuenta sin contraseña. Si se es administrador del sistema, repasar este hecho periódicamente (auditoría).
- No mantener las contraseñas por defecto del sistema. Por ejemplo, cambiar las cuentas de Administrador, Root, System, Invitado, Guest, etc.

- Nunca compartir con nadie la contraseña. Si se hace, cambiarla inmediatamente.
- No escribir la contraseña en ningún sitio. Si se escribe, no debe identificarse como tal y no debe identificarse al propietario en el mismo lugar.
- No teclear la contraseña si hay alguien observando. Es una norma tácita de buen usuario no mirar el teclado mientras alguien teclea su contraseña
- No enviar la contraseña por correo electrónico ni mencionarla en una conversación. Si e necesario mencionarla, no hacerlo explícitamente diciendo: "mi contraseña es...".
- No mantener una contraseña indefinidamente. Cambiarla regularmente. Se puede disponer de una lista de contraseñas que pueden usarse cíclicamente (por lo menos 5).

4.2. Encriptación de datos.

Las encriptación (una posible traducción al castellano sería cifrado) es el proceso mediante el cual cierta información o texto sin formato es transformada en un código ilegible a menos que se conozcan los datos necesarios para su interpretación. Es una medida de seguridad utilizada para que, al almacenar o transmitir información sensible, ésta no pueda ser interpretada por personas no autorizadas.

Algunos de los usos mas comunes de la encriptación son el almacenamiento y transmisión de información sensible como contraseñas, números de identificación legal, números de tarjetas crédito, informes contables y conversaciones privadas, entre otros.

En criptografía, la encriptación es un procedimiento que utiliza un algoritmo de cifrado con cierta clave (clave de cifrado) para transformar un mensaje, de tal forma que sea incomprensible a toda persona que no tenga la clave secreta (clave de descifrado) del algoritmo. Las claves de cifrado y de descifrado pueden ser iguales (criptografía simétrica) o distintas (criptografía asimétrica).

Tipos de cifrado

Existen diferentes tipos de cifrado:

- **simétrico**: cuando utiliza la misma clave para cifrar y descifrar;
- **asimétrico**: cuando utiliza claves diferentes para cifrar y descifrar;

El proceso de encriptación se puede llevar a cabo utilizando diferentes tipos de algoritmos: algoritmos hash, algoritmos simétricos y algoritmos asimétricos.

4.3.1. Algoritmo HASH:

Este algoritmo efectúa un cálculo matemático sobre los datos que constituyen el documento y da como resultado un número llamado valor hash. Un mismo documento dará siempre un mismo valor hash.

4.3.2. Criptografía de Clave Secreta o Simétrica

La criptografía simétrica, también llamada criptografía de clave secreta, es un método criptográfico en el cual se usa una misma clave para cifrar y descifrar mensajes en el emisor y el receptor. Las dos partes que se comunican han de ponerse de acuerdo de antemano sobre la clave a usar. Una vez que ambas partes tienen acceso a esta clave, el remitente cifra un mensaje usando la clave, lo envía al destinatario, y éste lo descifra con la misma clave.

Es importante destacar que la clave ha de viajar con los datos, lo que hace arriesgada la operación e imposible de utilizar en ambientes donde interactúan varios interlocutores.

Los Criptosistemas de clave secreta se caracterizan porque la clave de cifrado y de la descifrado es la misma, por tanto la robustez del algoritmo recae en mantener el secreto de la misma.

4.3.3. Criptografía de clave pública o Asimétrica

La criptografía asimétrica, también llamada criptografía de clave pública, es el método criptográfico que usa un par de claves para el envío de mensajes. Las dos claves pertenecen a la misma persona que ha enviado el mensaje. Una clave es pública y se puede entregar a cualquier persona, la otra clave es privada y el propietario debe guardarla de modo que nadie tenga acceso a ella. Además, los métodos criptográficos garantizan que esa pareja de claves sólo se puede generar una vez, de modo que se puede asumir que no es posible que dos personas hayan obtenido casualmente la misma pareja de claves.

Si el remitente usa la clave pública del destinatario para cifrar el mensaje, una vez cifrado, sólo la clave privada del destinatario podrá descifrar este mensaje, ya que es el único que la conoce. Por tanto se logra la confidencialidad del envío del mensaje, nadie salvo el destinatario puede descifrarlo.

Si el propietario del par de claves usa su clave privada para cifrar el mensaje, cualquiera puede descifrarlo utilizando su clave pública. En este caso se consigue por tanto la identificación y autentificación del remitente, ya que se sabe que sólo pudo haber sido él quien empleó su clave privada (salvo que alguien se la hubiese podido robar). Esta idea es el fundamento de la firma electrónica.

Los sistemas de cifrado de clave pública o sistemas de cifrado asimétricos se inventaron con el fin de evitar por completo el problema del intercambio de claves de los sistemas de cifrado simétricos. Con las claves públicas no es necesario que el remitente y el destinatario se pongan de acuerdo en la clave a emplear. Todo lo que se requiere es que, antes de iniciar la comunicación secreta, el remitente consiga una copia de la clave pública del destinatario. Es más, esa misma clave pública puede ser usada por cualquiera que desee comunicarse con su propietario. Por tanto, se necesitarán sólo n pares de claves por cada n personas que deseen comunicarse entre sí.

Ejemplos

Los métodos criptográficos más conocidos son el DES, el Triple DES y el AES para la criptografía simétrica, y el RSA para la criptografía asimétrica.

La utilización de un sistema simétrico o asimétrico depende de la aplicación en que se vaya a utilizar. La criptografía asimétrica presenta dos ventajas principales: suprime el problema de transmisión segura de la clave y permite la firma electrónica. No reemplaza sin embargo los sistemas simétricos, ya que los tiempos de cálculo son evidentemente más cortos con los sistemas simétricos que con los asimétricos.

4.5 Firma Digital

La firma digital es una información cifrada que identifica al autor de un documento electrónico.

La firma digital permite garantizar algunos conceptos de seguridad (identidad o autenticidad, integridad y no repudio) que son importantes al utilizar documentos en formato digital. El modo de funcionamiento es similar al explicado para los algoritmos de encriptación, se utilizan también algoritmos de clave pública, aplicados en dos etapas. Las firmas digitales y certificados permiten comprobar la procedencia, autenticidad e integridad de los mensajes.

Ventajas ofrecidas por la firma Digital

Entre ls ventajas ofrecidas por la firma digital, se pueden citar las siguientes:

- **Integridad de la información**: la integridad del documento es una protección contra la modificación de los datos en forma intencional o accidental. El emisor protege el documento, incorporándole un valor control de integridad. El receptor deberá efectuar el mismo cálculo sobre el documento recibido y comparar el valor calculado con el enviado por el emisor.

- **Autenticidad del origen del mensaje**: este aspecto de seguridad protege al receptor del documento, garantizándole que dicho mensaje ha sido generado por la parte identificada en el documento como emisor del mismo, no pudiendo alguna otra entidad suplantar a un usuario del sistema.
- **No repudio del origen**: el no repudio del origen protege al receptor del documento de la negación del emisor de haberlo enviado. Este aspecto de seguridad es más fuerte que los anteriores ya que el emisor no puede negar bajo ninguna circunstancia que ha generado dicho mensaje, transformándose en un medio de prueba inequívoco respecto de la responsabilidad del usuario del sistema.

4.3. Uso de software de seguridad informática

El objetivo del software de seguridad informática es prevenir contra virus informáticos y entradas indeseadas al sistema.

Antivirus y antiespías

Se denomina **malware** (software malicioso) al software específicamente diseñado para llevar a cabo acciones no deseadas (como infiltrase o dañar un ordenador o sistema informático) sin el consentimiento explicito del usuario.

Existen muchos tipos de malware: virus, gusanos, troyanos, adware, keyloggers, dialers, rootkits, spyware, ransomware, rogueware, etc. que se diseñan con diferentes fines. Algunos tipos de malware se diseñan con ánimo de lucro, otros son destructivos y su misión es alterar programas y archivos, otros hacen que un equipo sea controlado y explotado con fines ilícitos (envío de correo electrónico, almacenar pornografía, ataques a otros equipos o almacenar datos de actividades ilegales), etc.

Dentro del software de seguridad informática, se pueden citar: los antivirus, los antiespías, etc.

Los **antivirus** son programas que ayudan a proteger el equipo contra virus y otras amenazas a la seguridad.

Los **programas antiespía** impiden que se instalen en nuestro ordenador determinados programas cuyo objetivo es alterar su correcto funcionamiento (impiden acceder a determinadas páginas Web, muestran continuamente ventanas emergentes en nuestro navegador, etc.) o recopilar información del usuario.

Los cortafuegos (firewalls)

Otro elemento a tener en cuenta son los cortafuegos (firewalls). Los cortafuegos (Firewalls) están diseñados para proteger una red interna contra los accesos no autorizados. Un cortafuegos es un gateway (puerta de enlace) con un bloqueo que sólo deja pasar los paquetes de información que pasan una o varias inspecciones de seguridad. Aunque los cortafuegos (firewalls) son las herramientas o elementos más utilizadas a la hora de establecer seguridad, estos aparatos sólo son utilizados por las grandes organizaciones.

Nota: Un gateway (puerta de enlace) es un dispositivo, con frecuencia un ordenador, que permite interconectar redes con protocolos y arquitecturas diferentes a todos los niveles de comunicación. Su propósito es traducir la información del protocolo utilizado en una red al protocolo usado en la red de destino. Es normalmente un equipo informático configurado para dotar a las máquinas de una red local (LAN) conectadas a él de un acceso hacia una red exterior.

Como ya hemos dicho, un cortafuegos es el mecanismo encargado de proteger una red confiable de una que no lo es (por ejemplo Internet). Un cortafuegos puede consistir en distintos dispositivos, tendientes a los siguientes objetivos:

- Todo el tráfico desde dentro hacia fuera, y viceversa, debe pasar a través de él.

- Sólo el tráfico autorizado, definido por la política local de seguridad, es permitido.

Algunos cortafuegos aprovechan esta capacidad de que toda la información entrante y saliente debe pasar a través de ellos para proveer servicios de seguridad adicionales como la encriptación del tráfico de la red.

Como puede observarse, los cortafuegos, sólo sirven de defensa perimetral de las redes, no defienden de ataques o errores provenientes del interior, así como tampoco pueden ofrecer protección una vez que el intruso lo traspasa. Por eso, es conveniente, complementar el trabajo del cortafuegos con una defensa interna. El cortafuegos tampoco provee de herramientas contra la filtración de software o archivos infectados con virus, aunque es posible dotar, a la máquina donde se aloja el cortafuegos, de antivirus apropiados.

Nota: Aunque se ha hablado de los cortafuegos dentro del apartado del software de seguridad informática, hay que decir que, los cortafuegos pueden ser soluciones hardware o software.

5. SEGURIDAD PASIVA

La seguridad se puede clasificar en seguridad activa y seguridad pasiva. La seguridad pasiva tiene como finalidad minimizar los efectos o desastres causados por un accidente, usuario o malware. Entre las técnicas de seguridad pasiva, se pueden citar

- Uso de hardware y dispositivos físicos de protección adecuados.
- Realización de copias de seguridad.
- Particiones del disco duro.
- Conjunto de discos redundantes.

5.1. Uso de hardware y dispositivos físicos de protección adecuados.

Ningún sistema de seguridad, ni siquiera el más sofisticado, puede garantizar al cien por

ciento una protección completa de los datos. Un pico o una caída de tensión pueden limpiar en un instante hasta el dato más cuidadosamente guardado. Entre los dispositivos físicos que se pueden utilizar para aumentar la seguridad se pueden citar:

- **Sistemas de alimentación ininterrumpida (SAI)**: Un SAI se utiliza para proteger a los ordenadores contra la perdida de datos durante una caída de tensión.
- **Protectores de sobrecarga**: Los protectores de sobrecarga protegen los equipos contra los dañinos picos de tensión, evitando así costosas reparaciones posteriores.

Sistemas de alimentación ininterrumpida (SAI)

Un sistema de alimentación ininterrumpida (SAI), en inglés uninterruptible power supply (UPS), es un dispositivo que gracias a sus baterías u otros elementos almacenadores de energía, puede proporcionar energía eléctrica por un tiempo limitado y durante un apagón eléctrico a todos los dispositivos que tenga conectados. Una vez que la corriente se pierde, las baterías del SAI se ponen en funcionamiento proporcionando la corriente necesaria para el correcto funcionamiento del sistema. Otras de las funciones que se pueden adicionar a estos equipos es la de mejorar la calidad de la energía eléctrica que llega a las cargas, filtrando subidas y bajadas de tensión y eliminando armónicos de la red en el caso de usar corriente alterna.

Los SAI dan energía eléctrica a los equipos llamados cargas críticas, como pueden ser aparatos médicos, industriales o informáticos que, como se ha mencionado anteriormente, requieren tener siempre alimentación y que ésta sea de calidad, debido a la necesidad de estar en todo momento operativos y sin fallos (picos o caídas de tensión).

Protectores de sobrecarga

Los protectores de sobrecarga, aunque no sirven durante un apagón, protegen los equipos contra los dañinos picos de tensión, evitando así costosas reparaciones posteriores.

5.2. Realización de copias de seguridad (backup)

Como ya se ha comentado anteriormente, ningún sistema de seguridad puede garantizar al cien por ciento una protección completa de los datos. Los desastres pueden aparecer de forma muy diversa (sabotajes, errores humanos, fallos de la máquina, fuego, inundaciones, rayos, terremotos, etc.) y pueden dañar o destruir tanto el hardware como los datos de un sistema informático. Cualquier sistema de seguridad completo debe incluir un plan de recuperación en el caso de producirse un desastre. La técnica más utilizada es llevar a cabo copias de seguridad regulares.

Las copias de seguridad son una manera de proteger la inversión realizada en los datos. Las pérdidas de información no es tan importante si existen varias copias resguardadas

La copia de seguridad es útil por varias razones:

- Para restaurar un ordenador a un estado operacional después de un desastre (copias de seguridad del sistema)
- Para restaurar un pequeño número de ficheros después de que hayan sido borrados o dañados accidentalmente (copias de seguridad de datos).
- En el mundo de la empresa, además es útil y obligatorio, para evitar ser sancionado por los órganos de control en materia de protección de datos.

Normalmente las copias de seguridad se suelen hacer en cintas magnéticas, aunque dependiendo de la cantidad y tipo de información también pueden utilizarse disquetes, CD, DVD, Discos Zip, Jaz o magnéticos-ópticos, pendrivers o pueden realizarse sobre un centro de respaldo remoto propio o vía Internet.

Las copias de seguridad en un sistema informático tienen por objetivo el mantener cierta capacidad de recuperación de la información ante posibles pérdidas. Las copias de seguridad pueden realizarse sobre los datos (se pueden incluir también archivos que formen parte del

sistema operativo). Así las copias de seguridad suelen ser utilizadas como la última línea de defensa contra pérdida de datos, y se convierten por lo tanto en el último recurso a utilizar.

Software de copias de seguridad

Existen una gran gama de software en el mercado para realizar copias de seguridad. Es importante definir previamente los requerimientos específicos para determinar el software adecuado.

Entre los más populares se encuentran ZendalBackup Cobian, SeCoFi, CopiaData y NortonGhost.

Para la realización de copias de seguridad de los datos y del sistema operativo existe software libre como:

- Cobian Backup o Clonecilla , para Windows.
- Keep KDE para Linux.

5.3. Particiones del disco duro.

Una partición de disco, en mantenimiento, es el nombre genérico que recibe cada división presente en una sola unidad física de almacenamiento de datos. Toda partición tiene su propio sistema de archivos (formato) y generalmente, casi cualquier sistema operativo interpreta, utiliza y manipula cada partición como un disco físico independiente, a pesar de que dichas particiones estén en un solo disco físico. Las razones principales para tener más de una partición de disco suelen ser, por un lado, tener más de un sistema operativo en el ordenador, y por otro, conseguir una mejor distribución del contenido (normalmente con una partición para el sistema operativo y las aplicaciones y otra para los documentos y archivos del usuario).

Ventajas del uso de particiones

Generalmente, en una de las particiones se mantiene el sistema operativo y en la otra los archivos del usuario (documentos, correos electrónicos, etc). La principal ventaja del uso de particiones es que si se necesita formatear e instalar de cero el sistema por cualquier inconveniente, simplemente se procede a formatear la partición que contiene el sistema operativo, dejando intacta la otra.

Dado que si se rompe el disco duro pueden verse afectadas las dos particiones, no suele ser buena idea utilizar una partición como respaldo. Siempre es conveniente utilizar como respaldo otra unidad de almacenamiento.

Aplicaciones para la edición de particiones

- Gparted y KDE Partition Manager: GParted es el editor de particiones de GNOME. Esta aplicación es usada para crear, destruir, redimensionar, inspeccionar y copiar particiones, como también sistemas de archivos. Esto es útil para crear espacio para nuevos sistemas operativos, para reorganizar el uso del disco y para crear imágenes de un disco en una partición. KDE Partition Manager es la contraparte de GParted pero para entornos de escritorios KDE.
- DiskPart y Administrador de Discos: En los sistemas operativos basados en Windows NT (XP, 2003, Vista, 2008, 7, 8) la herramienta gráfica predeterminada es la utilidad Administración de Discos y para la línea de comandos existe el programa diskpart.

5.4. Conjunto de discos redundantes.

La utilización de un conjunto de discos redundantes permite restaurar la información que no es válida ni consistente.

6. ACTIVIDADES

xxxxxxxx