1 Seguridad informática

Objetivos del capítulo

- ✓ Analizar la problemática general de la seguridad informática.
- ✓ Ver desde qué puntos de vista se puede analizar.
- ✓ Identificar las principales vulnerabilidades y ataques a los sistemas.

Supongamos que un día su unidad de DVD empieza a abrirse y cerrarse por sí sola, sin que haya ninguna explicación de ningún otro tipo; supongamos que en la carpeta donde usted archivó unas fotos de sus amigos aparecen, inexplicablemente, fotos de delfines; o supongamos que usted recibe la visita de un vecino, quien lo acusa de haberlo atacado informáticamente, es decir, el vecino recibió un ataque en su ordenador, y al tratar de averiguar quién lo hizo, encontró los datos del ordenador de usted.

Prevenir, corregir y entender estas situaciones son las que dan sentido al estudio de la seguridad informática.

Con la proliferación de la informática en todos los ámbitos de la vida, el número de usuarios y profesionales de informática ha crecido exponencialmente en los últimos años, del mismo modo que las necesidades de comunicación y compartir recursos en red. El desarrollo de las telecomunicaciones en la década de los noventa posibilitó la interconexión de las distintas redes existentes mediante la red global Internet.

Del mismo modo que surgen nuevas posibilidades y ventajas derivadas de la comunicación entre distintos usuarios remotos, en los últimos años han crecido el número de ataques y vulnerabilidades de los sistemas informáticos.

1.1 PRINCIPIOS DE LA SEGURIDAD INFORMÁTICA

La seguridad informática, en general, está teniendo una importancia cada vez mayor. Los usuarios, particulares y trabajadores de las empresas, deben ser conscientes de que el funcionamiento correcto de sus sistemas depende en gran medida, de protegerlos como el mayor de sus tesoros.

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.

ACTIVIDADES

La seguridad informática lleva asociada un **conjunto de términos**, en muchos casos nuevos términos en inglés, que hacen difícil la tarea de estar al día en materia de seguridad.

Te proponemos que leas un **artículo de actualidad** en el cual deberás identificar palabras relacionadas con conceptos de seguridad informática que no conozcas y realizar un glosario de términos con sus definiciones.

A lo largo del curso te proponemos realizar tus actividades en un **blog** personal, donde puedas compartir tu trabajo con otros usuarios de la red.

Es impresionante la cantidad de sitios web que visitamos, y de empresas/organizaciones que ofrecen vía web los servicios que demandamos, ya sea como forma de vida, por trabajo, ocio, hobbies, interés particular, etc.

Cada día nos suscribimos a nuevos foros, compramos billetes de avión, tren, reservamos hoteles, accedemos a nuestra banca online, facturas de telefonía, luz, gas,... participamos en redes sociales (como Facebook, Twitter, Tuenti, Linkedin,...), gestionamos diferentes cuentas de correo (hotmail, gmail, yahoo,...), compramos y vendemos (Ebay, Paypal), foros

varios dependiendo de si nos gustan los coches, los libros, el cine, la música,... entre otros.

Para cada sitio web, es necesario introducir unas credenciales: en algunos casos podremos elegir el nombre de usuario (siempre y cuando no exista, o tendremos que derivar uno diferente al que generalmente usamos) y una contraseña (que en algunos casos deberá seguir un formato dado por la organización para satisfacer ciertos requisitos de complejidad). A no ser que seamos felices viviendo en el campo, ajenos a una conexión a Internet, estamos obligados a tener un montón de identidades digitales o una única con un nombre de usuario lo suficientemente raro y una misma contraseña.

¿Problemas? Pues ambas posibilidades tienen sus ventajas e inconvenientes. Tener diferentes identidades (pares usuario/contraseña) permite ser uno diferente en cada sitio, de manera que no se pueda concluir mediante herramientas online o mediante análisis las costumbres (a veces contradictorias) de un mismo individuo. Así, si un sitio de los que somos usuarios se ve comprometido (o picamos ante un ataque de *phishing*) y nuestras credenciales son expuestas, las que usamos para el resto de los servicios seguirán seguras. Mucha gente, incluso importante en el mundo de la seguridad, utiliza mecanismos de generación de credenciales basados en el nombre del sitio web o servicio que visitan. Una vez comprometido el algoritmo pensado, todas las credenciales de ese individuo, quedan expuestas.

Por lo mismo y dada la cantidad de servicios online que consumimos, lo más normal es que olvidemos aquellos que no utilizamos tan a menudo y haya que usar las opciones *Lost Password*.

En el caso de usar el mismo usuario/contraseña (siempre que se pueda) para todos los servicios, si alguien averigua nuestras credenciales (por *sniffing*, *shoulder surfing*, compromiso de uno de los *websites*, *ingeniería social*, *phishing*, etc...) podrá probar en otros sitios que exista el mismo usuario o de otros en los que conozca nuestros hábitos.

Para evitar este tipo de disyuntivas, las empresas se gastan un dineral anualmente en lo que se llaman proyectos de gestión de identidades, *single sign-on* y *provisioning*. Para el usuario de a pie, hay en el mercado variedad de productos, comerciales y libres (como por ejemplo KeepassX), que permiten mantener en un contenedor cifrado las diferentes identidades. Para aplicaciones web, incluso los navegadores proveen de servicios propios de auto-rellenado de usuario y contraseña.

En general, estos programas de protección de contraseñas, así como los de gestión de identidades, requieren una autenticación basada en una contraseña maestra. Lo cual nos lleva a otro problema más, si esa contraseña maestra cae, todas las demás quedan expuestas.

Este problema se solucionaría utilizando algún tipo de autenticación fuerte como contraseña maestra, basada en al menos dos factores de estos tres: algo que se tiene, algo que se sabe, algo que se es.

Si no es posible la autenticación fuerte, al menos:

Aseguraos de que cuando insertéis la contraseña maestra de vuestro gestor de credenciales no haya nadie mirando. Si tapáis el PIN cuando metéis la tarjeta en el cajero automático, ¿por qué no tener ciertas precauciones en el teclado del PC?

Como extensión al punto anterior, que no nos miren ni desde fuera ni desde dentro del PC: mantenedlo libre de *troyanos* y *keyloggers*. Política de parches y antivirus actualizados, *firewalls* personales, instalar sólo aquello que estéis seguros que no contiene *spyware/malware* y cuidado con los *rogue antivirus*.

Cerrad la sesión cuando terminéis la actividad para la que os hayáis tenido que autenticar (sobre todo para entornos de banca online).

Cuidado con los enlaces sobre los que pincháis (los que veáis en foros, los que os lleguen por correo), puede llevaros a no dar vuestra contraseña, pero sí a ceder vuestra sesión por robo de *cookies*.

Cuidado con las preguntas secretas para recuperar contraseñas. Extremad precauciones con respuestas demasiado triviales que puedan comprometer vuestra información de una forma trivial por quien os conoce.

Y sobre todo y más importante, cuidado con los ataques basados en ingeniería social. Cuando hay que dar una contraseña a alguien, no fiarse siempre es la opción correcta.

1.2 FIABILIDAD, CONFIDENCIALIDAD, INTEGRIDAD Y DISPONIBILIDAD

Si bien es cierto que todos los componentes de un sistema informático están expuestos a un ataque (hardware, software y datos) son los datos y la información los sujetos principales de protección de las técnicas de seguridad. La seguridad informática se dedica principalmente a proteger la confidencialidad, la integridad y disponibilidad de la información. Por tanto, actualmente se considera generalmente aceptado que la seguridad de los datos y la información comprende tres aspectos fundamentales:

- ✓ Confidencialidad, es decir, no desvelar datos a usuarios no autorizados; que comprende también la privacidad (la protección de datos personales).
- ✓ Integridad, permite asegurar que los datos no se han falseado.
- ✓ Disponibilidad, esto es, que la información se encuentre accesible en todo momento a los distintos usuarios autorizados.

Hay que tener en cuenta que tanto las amenazas como los mecanismos para contrarrestarlas, suelen afectar a estas tres características de forma conjunta. Así por ejemplo, fallos del sistema que hacen que la información no sea accesible pueden llevar consigo una pérdida de integridad.

Generalmente **tienen que existir los tres aspectos descritos para que haya seguridad.**

Dependiendo del entorno en que un sistema trabaje, a sus responsables les interesará dar prioridad a un cierto aspecto de la seguridad. Por ejemplo, en un sistema militar se antepondrá la confidencialidad de los datos almacenados o transmitidos sobre su disponibilidad: seguramente, es preferible que alguien borre información confidencial (que se podría recuperar después desde una cinta de backup) a que ese mismo atacante pueda leerla, o a que esa información esté disponible en un instante dado para los usuarios autorizados.

En cambio, en un servidor NFS de archivos en red, de un departamento se premiará la disponibilidad frente a la confidencialidad: importa poco que un atacante lea una unidad, pero que esa misma unidad no sea leída por usuarios autorizados va a suponer una pérdida de tiempo y dinero.

En un entorno bancario, la faceta que más ha de preocupar a los responsables del sistema es la integridad de los datos, frente a su disponibilidad o su confidencialidad: es menos grave que un usuario consiga leer el saldo de otro que el hecho de que ese usuario pueda modificarlo.

Los conceptos confidencialidad, integridad o disponibilidad son muy comunes en el ámbito de la seguridad y aparecen como fundamentales en toda arquitectura de seguridad de la información, ya sea en el ámbito de la protección de datos, normativa vigente relacionada con la protección de datos de carácter personal, como de códigos de buenas prácticas o recomendaciones sobre gestión de la seguridad de la información y de prestigiosas certificaciones internacionales, éstas últimas, relacionadas con la auditoría de los sistemas de información.

Junto a estos tres conceptos fundamentales se suelen estudiar conjuntamente la autenticación y el no repudio en los sistemas de información. Por lo que suele referirse al grupo de estas características como CIDAN, nombre sacado de la inicial de cada característica.

- ✓ Confidencialidad.
- ✓ Integridad.
- ✓ Disponibilidad.
- ✓ Autenticación.
- ✓ No repudio.

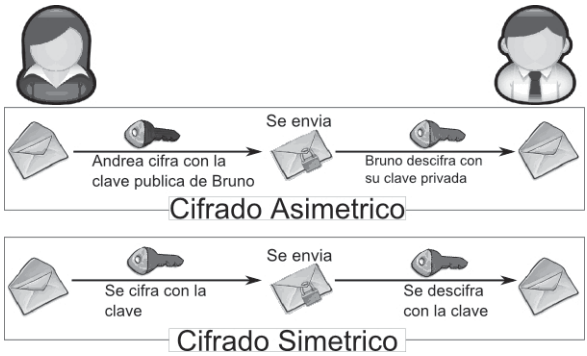
Por estos motivos es importante tener una idea clara de estos conceptos. Veamos con algo más de profundidad los mismos.

1.2.1 CONFIDENCIALIDAD

Se trata de la cualidad que debe poseer un documento o archivo para que este sólo se entienda de manera comprensible o sea leído por la persona o sistema que esté autorizado.

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

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



ACTIVIDADES

Analiza el significado de clave simétrica y asimétrica leyendo el siguiente texto. ¿Podrías poner algunos ejemplos donde se dispongan típicamente claves simétricas y asimétricas? ¿Cómo es que siendo una clave pública en el cifrado asimétrico es más seguro que el cifrado simétrico?

- Cifrado simétrico: es la técnica más antigua, la más extendida y mejor conocida. Una clave secreta, que puede ser un número, una palabra o simplemente una cadena de letras, aleatorias, se aplica al texto de un mensaje para cambiar el contenido en un modo determinado. Esto podría ser tan sencillo como desplazando cada letra a un número de posiciones en el alfabeto. Siempre que el remitente y destinatario conozcan la clave secreta, puede cifrar y descifrar todos los mensajes que utilizan esta clave.
- Cifrado asimétrico: el problema con las claves secretas intercambiadas a través de Internet o de una gran red es que caigan en manos equivocadas. Cualquiera que conozca la clave secreta puede descifrar el mensaje. Una respuesta a este problema es el cifrado asimétrico, en la que hay dos claves relacionadas, un par de claves. Una clave pública queda disponible libremente para cualquier usuario que desee enviar un mensaje. Una segunda clave privada se mantiene en secreto, de forma que sólo pueda conocerla el destinatario.

Cualquier mensaje (texto, archivos binarios o documentos) que están cifrados mediante clave pública sólo puede descifrarse aplicando el mismo algoritmo, pero mediante la clave privada correspondiente, por lo que aunque algún usuario de la red intercepte y disponga de la clave pública y del mensaje, también deberá disponer de la clave privada que sólo dispone el destinatario. Del mismo modo, cualquier mensaje que se cifra mediante la clave privada sólo puede descifrarse mediante la clave pública correspondiente.

En este caso, cada usuario ha de poseer una pareja de claves:

- Clave privada: será custodiada por su propietario y no se dará a conocer a ningún otro.
- Clave pública: puede ser conocida por todos los usuarios.

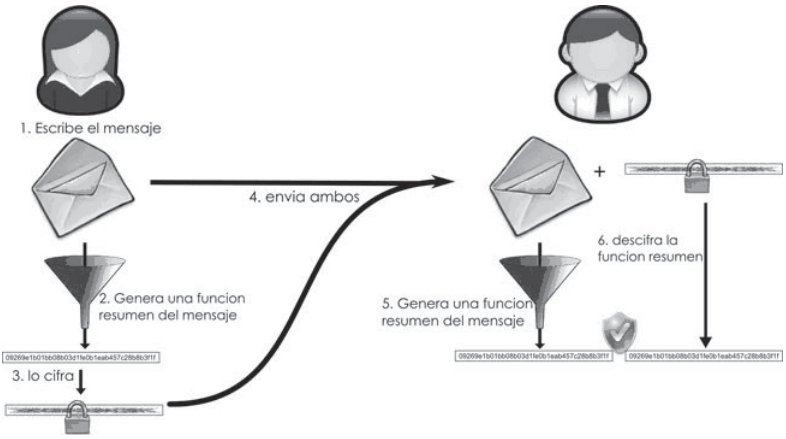
Esta pareja de claves es complementaria: lo que cifra una SÓLO lo puede descifrar la otra y viceversa.

Estas parejas de claves se obtienen mediante métodos matemáticos complejos.

Un problema con el cifrado asimétrico, sin embargo, es que es más lento que el cifrado simétrico. Requiere mucha más capacidad de procesamiento para cifrar y descifrar el contenido del mensaje, pero este coste de tiempo hace del mismo un mecanismo más seguro.

1.2.2 INTEGRIDAD

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



En el caso del envío de información y su no modificación durante su viaje a través de una red, teniendo como muestra el ejemplo anterior, Andrea envía tanto el propio mensaje como un resumen cifrado del mismo. Finalmente, Bruno en el lado del receptor, compara el mensaje como resumen (aplicando la misma función que Andrea) y el resumen cifrado enviado. Si en el transcurso de la comunicación el mensaje ha sido alterado por fallos en el canal de comunicaciones o por algún usuario intruso, la comparación será errónea, y si ésta da como resultado "iguales", quiere decir que no ha existido manipulación del mensaje.

1.2.3 DISPONIBILIDAD

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

También se refiere a la seguridad que la información pueda ser recuperada en el momento que se necesite, esto es, evitar su pérdida o bloqueo, bien sea por ataque doloso, mala operación accidental o situaciones fortuitas o de fuerza mayor.

ACTIVIDADES

Lee el siguiente artículo sobre alta disponibilidad y explica si el equipo que dispones la posee. Indica algunas medidas para aumentar la disponibilidad ante por ejemplo cortes de suministro de luz, o el error de lectura/escritura en una unidad de disco duro. ¿Qué es un sistema o centro de respaldo? ¿Los sistemas de alta disponibilidad cuántas horas y días a la semana deben funcionar?

Nos referimos a alta disponibilidad (en inglés High Availability) a los sistemas que nos permiten mantener nuestros sistemas funcionando las 24 horas del día, manteniéndolos a salvo de interrupciones.

Debemos diferenciar dos tipos de interrupciones en nuestros sistemas.

- Las interrupciones previstas: las que se realizan cuando paralizamos el sistema para realizar cambios o mejoras en nuestro hardware o software.
- Las interrupciones imprevistas: las que suceden por acontecimientos imprevistos (como un apagón, un error del hardware o del software, problemas de seguridad, un desastre natural, virus, accidentes, caídas involuntarias del sistema).

Y distintos niveles de disponibilidad del sistema:

- Los sistemas de la disponibilidad base: el sistema está listo para el uso inmediato, pero experimentará tanto interrupciones planificadas como no planificadas.
- Los sistemas de disponibilidad alta: incluyen tecnologías para reducir drásticamente el número y la duración de interrupciones imprevistas. Todavía existen interrupciones planificadas, pero los servidores incluyen herramientas que reducen su impacto.
- Entornos de operaciones continuas: utilizan tecnologías especiales para asegurarse de que no hay interrupciones planificadas para backups, actualizaciones, u otras tareas de mantenimiento que obliguen a no tener el sistema disponible.
- Los sistemas de la disponibilidad continua: van un paso más lejos para asegurarse de que no habrán interrupciones previstas o imprevistas que interrumpan los sistemas. Para alcanzar este nivel de la disponibilidad, las compañías deben utilizar servidores duales o los clusters de servidores redundantes donde un servidor asume el control automáticamente si el otro servidor cae.
- Los sistemas de tolerancia al desastre: requieren de sistemas alejados entre sí para asumir el control en cuanto pueda producirse una interrupción provocada por un desastre.

Normalmente, un sistema de alta disponibilidad funciona sobre un sistema de producción y otro sistema de respaldo (o varios, en caso de que queramos un sistema de alta disponibilidad con tolerancia al desastre), donde en caso de alguna incidencia podremos recuperar la información del sistema de producción.

Para que este sistema de respaldo sea realmente efectivo, no tan sólo debe recuperar la información (base de datos) del sistema de producción, sino que debe reflejar cualquier cambio realizado en el mismo (usuarios, autorizaciones, programas, configuraciones, colas de trabajo, etc.) y sobre todo que estos cambios se reflejen en el sistema de respaldo de la forma más automatizada posible.

Las herramientas de alta disponibilidad deben permitirnos por lo tanto disponer de nuestros equipos funcionando **24 horas al día, 7 días a la semana**, ofreciéndonos la seguridad de que bajo cualquier supuesto, nuestro sistema de producción estará disponible casi inmediatamente.

Dada la creciente dependencia en los sistemas, la globalización de los mercados, el comercio electrónico y la alta competencia entre las compañías, los costes asociados a los tiempos de parada (sea cual sea el tipo) son cada vez mayores y las empresas empiezan a tenerlos en consideración.

En el actual entorno de negocios, la alta disponibilidad de nuestros sistemas se ha convertido en una necesidad y no en un lujo.

1.2.4 AUTENTICACIÓN

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

Aplicado a la verificación de la identidad de un usuario, la autenticación se produce cuando el usuario puede aportar algún modo de que se pueda verificar que dicha persona es quien dice ser, a partir de ese momento se considera un usuario autorizado. La autenticación en los sistemas informáticos habitualmente se realiza mediante un usuario o login y una contraseña o password.

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

1.2.5 NO REPUDIO

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

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

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

Relación de los servicios de seguridad:

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

1.3 ELEMENTOS VULNERABLES EN EL SISTEMA INFORMÁTICO: HARDWARE, SOFTWARE Y DATOS

Seguridad es un concepto asociado a la certeza, falta de riesgo o contingencia. Conviene aclarar que no siendo posible la certeza absoluta, el elemento de riesgo está siempre presente, independientemente de las medidas que tomemos, por lo que debemos hablar de **niveles de seguridad**. La seguridad absoluta no es posible y en adelante entenderemos que la seguridad informática es un conjunto de técnicas encaminadas a obtener **altos niveles de seguridad** en los sistemas informáticos. Además, la seguridad informática precisa de un nivel organizativo, por lo que diremos que:

Sistema de Seguridad = TECNOLOGÍA + ORGANIZACIÓN

La seguridad es un problema integral: los problemas de seguridad informática no pueden ser tratados aisladamente ya que la seguridad de todo el sistema es igual a la de su punto más débil. Al asegurar nuestra casa no sacamos nada con ponerle una puerta blindada con sofisticada cerradura si dejamos las ventanas sin protección. De manera similar el uso de sofisticados algoritmos y métodos criptográficos es inútil si no garantizamos la confidencialidad de las estaciones de trabajo.

Por otra parte, existe algo que los hackers llaman Ingenieria Social que consiste simplemente en conseguir mediante engaño que los usuarios autorizados revelen sus passwords. Por lo tanto, la educación de los usuarios es fundamental para que la tecnología de seguridad pueda funcionar. Es evidente que por mucha tecnología de seguridad que se implante en una organización, si no existe una clara disposición por parte de los directores de la empresa y una cultura a nivel de usuarios, no se conseguirán los objetivos perseguidos con la implantación de un sistema de seguridad.

Los tres elementos principales a proteger en cualquier sistema informático son el *software,* el *hardware* y los datos. Por **hardware** entendemos el conjunto formado por todos los elementos físicos de un sistema informático, como CPU, terminales, cableado, medios de almacenamiento secundario (cintas, CD-ROM, disquetes...) o tarjetas de red. Por **software** entendemos el conjunto de programas lógicos que hacen funcionar al *hardware,* tanto sistemas operativos como aplicaciones, y por **datos** el conjunto de información lógica que manejan el *software* y el *hardware*, como por ejemplo paquetes que circulan por un cable de

red o entradas de una base de datos. Aunque generalmente en las auditorías de seguridad se habla de un cuarto elemento a proteger, los **fungibles** (elementos que se gastan o desgastan con el uso continuo, como papel de impresora, *tóners,* cintas magnéticas,...), aquí no consideraremos la seguridad de estos elementos por ser externos a la red.

Habitualmente **los datos constituyen el principal elemento** de los tres **a proteger**, ya que es el más amenazado y seguramente el más difícil de recuperar: con toda seguridad un servidor estará ubicado en un lugar de acceso físico restringido, o al menos controlado, y además en caso de pérdida de una aplicación (o un programa de sistema, o el propio núcleo del sistema operativo) este *software* se puede restaurar sin problemas desde su medio original (por ejemplo, el CD-ROM con el sistema operativo que se utilizó para su instalación). Sin embargo, en caso de pérdida de una base de datos o de un proyecto de un usuario, no tenemos un medio "original" desde el que restaurar: hemos de pasar obligatoriamente por un sistema de copias de seguridad, y a menos que la política de copias sea muy estricta, es difícil devolver los datos al estado en que se encontraban antes de la pérdida.

También debemos ser conscientes de que las medidas de seguridad que deberán establecerse comprenden el hardware y el sistema operativo, las comunicaciones (por ejemplo, medios de transmisión), medidas de seguridad físicas (ubicación de los equipos, suministro eléctrico, etc.), los controles organizativos (políticas de seguridad, niveles de acceso, contraseñas, normas, procedimientos, etc.) y legales (por ejemplo, la Ley Orgánica de Protección de Datos, LOPD).

1.4 AMENAZAS

Las amenazas a un sistema informático pueden provenir desde un hacker remoto que entra en nuestro sistema con un troyano, pasando por un programa descargado gratuito que nos ayuda a gestionar nuestras fotos, pero que supone una puerta trasera a nuestro sistema permitiendo la entrada a espias, hasta la entrada no deseada al sistema mediante una contraseña de bajo nivel de seguridad. Se pueden clasificar por tanto en amenzas provocadas por:

- ✓ Personas.
- ✓ Amenazas lógicas.
- ✓ Amenazas físicas.

A continuación se presenta una relación de los **elementos que potencialmente pueden amenazar a nuestro sistema.**

- **Personas.** No podernos engañarnos: la mayoría de ataques a nuestro sistema van a provenir en última instancia de personas que, intencionada o inintencionadamente, pueden causarnos enormes pérdidas. Generalmente se tratará de piratas que intentan conseguir el máximo nivel de privilegio posible aprovechando alguno (o algunos) de los riesgos lógicos de los que hablaremos a continuación, especialmente agujeros del *software*. Pero con demasiada frecuencia se suele olvidar que los piratas "clásicos" no son los únicos que amenazan nuestros equipos: es especialmente preocupante que mientras que hoy en día cualquier administrador mínimamente preocupado por la seguridad va a conseguir un sistema relativamente fiable de una forma lógica (permaneciendo atento a vulnerabilidades de su *software*, restringiendo servicios, utilizando cifrado de datos...), pocos administradores tienen en cuenta factores como la ingeniería social o el basurero, a la hora de diseñar una política de seguridad.

  Aquí se describen brevemente los diferentes tipos de personas que de una u otra forma pueden constituir un riesgo para nuestros sistemas; generalmente se dividen en dos grandes grupos: los atacantes **pasivos** aquellos que fisgonean por el sistema pero no lo modifican o destruyen, y los **activos** aquellos que dañan el objetivo atacado, o lo modifican en su favor.

- ***Personal.*** Se pasa por alto el hecho de que casi cualquier persona de la organización, incluso el personal ajeno a la infraestructura informática (secretariado, personal de seguridad, personal de limpieza y mantenimiento...) puede comprometer la seguridad de los equipos. Aunque los ataques pueden ser intencionados (en cuyo caso sus efectos son extremadamente dañinos, recordemos que nadie mejor que el propio personal de la organización conoce mejor los sistemas... y sus debilidades), lo normal es que más que de ataques se trate de **accidentes** causados por un error o por desconocimiento de las normas básicas de seguridad.

- ***Ex-empleados.*** Generalmente, se trata de personas descontentas con la organización que pueden aprovechar debilidades de un sistema que conocen perfectamente, pueden insertar troyanos, bombas lógicas, virus... o simplemente conectarse al sistema como si aún trabajaran para la organización (muchas veces se mantienen las cuentas abiertas incluso meses después de abandonar la universidad o empresa), conseguir el privilegio necesario, y dañarlo de la forma que deseen, incluso chantajeando a sus ex-compañeros o ex-jefes.

- ***Curiosos.*** Junto con los *crackers,* los curiosos son los atacantes más habituales de sistemas. En la mayoría de ocasiones esto se hace simplemente para leer el correo de un amigo, enterarse de cuánto cobra un compañero, copiar un trabajo o comprobar que es posible romper la seguridad de un sistema concreto. Aunque en la mayoría de situaciones se trata de ataques no destructivos (a excepción del borrado de huellas para evitar la detección), parece claro que no benefician en absoluto al entorno de fiabilidad que podamos generar en un determinado sistema.

- ***Hacker***. Es un término general que se ha utilizado históricamente para describir a un experto en programación. Recientemente, este término se ha utilizado con frecuencia con un sentido negativo, para describir a una persona que intenta obtener acceso no autorizado a los recursos de la red con intención maliciosa, aunque no siempre tiene que ser esa su finalidad.

- ***Cracker***. Es un término más preciso para describir a una persona que intenta obtener acceso no autorizado a los recursos de la red con intención maliciosa.

- ***Intrusos remunerados.*** Se trata de piratas con gran experiencia en problemas de seguridad y un amplio conocimiento del sistema, que

son pagados por una tercera parte generalmente para robar secretos (el nuevo diseño de un procesador, una base de datos de clientes, información confidencial sobre las posiciones de satélites espía...) o simplemente para dañar la imagen de la entidad afectada.

- **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).

  - ***Software incorrecto.*** A los errores de programación se les denomina *bugs*, y a los programas utilizados para aprovechar uno de estos fallos y atacar al sistema, *exploits*.

  - ***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. Herramientas como NESSUS, SAINT o SATAN pasan de ser útiles a ser peligrosas cuando las utilizan *crackers* que buscan información sobre las vulnerabilidades de un *host* o de una red completa.

  - ***Puertas traseras.*** 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.

  - ***Bombas lógicas.*** Las bombas lógicas son partes de código de ciertos programas que permanecen sin realizar ninguna función hasta que son activadas; en ese punto, la función que realizan no es la original del programa, sino que generalmente se trata de una acción perjudicial.

  - ***Canales cubiertos.*** Los canales cubiertos (o canales ocultos, según otras traducciones) 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.

- ***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. Todo el mundo conoce los efectos de los virus en algunos sistemas operativos de sobremesa como Windows; sin embargo, en GNU/Linux los virus no suelen ser un problema de seguridad grave.

- ***Gusanos.*** Un gusano es un programa capaz de ejecutarse y propagarse por sí mismo a través de redes, en ocasiones portando virus o aprovechando *bugs* de los sistemas a los que conecta para dañarlos. Al ser difíciles de programar su número no es muy elevado, pero el daño que pueden causar es muy grande: el mayor incidente de seguridad en Internet fue precisamente el *Internet Worm,* un gusano que en 1988 causó perdidas millonarias al infectar y detener más de 6.000 máquinas conectadas a la red.

- ***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; como el Caballo de Troya de la mitología griega, al que deben su nombre, ocultan su función real bajo la apariencia de un programa inofensivo que a primera vista funciona correctamente.

- ***Programas conejo o bacterias.*** Bajo este nombre se conoce a los programas que no hacen nada útil, sino que simplemente se dedican a reproducirse hasta que el número de copias acaba con los recursos del sistema (memoria, procesador, disco...), produciendo una negación de servicio.

■ **Amenazas físicas.** Algunas de las amenazas físicas que pueden afectar a la seguridad y por tanto al funcionamiento de los sistemas son:

- Robos, sabotajes, destrucción de sistemas.

- Cortes, subidas y bajadas bruscas de suministro eléctrico.

- Condiciones atmosféricas adversas. Humedad relativa excesiva o temperaturas extremas que afecten al comportamiento normal de los componentes informáticos.

- Las catástrofes (naturales o artificiales) son la amenaza menos probable contra los entornos habituales: simplemente por su ubicación geográfica. Un subgrupo de las catástrofes es el denominado de riesgos poco probables. Como ejemplos de catástrofes hablaremos de terremotos, inundaciones, incendios, humo o atentados de baja magnitud (más comunes de lo que podamos pensar); obviamente los riesgos poco probables los trataremos como algo anecdótico.

Hasta ahora hemos hablado de los aspectos que engloba la seguridad informática, de los elementos a proteger, de los tipos de amenazas que contra ellos se presentan y del origen de tales amenazas; parece claro que, para completar nuestra visión de la seguridad, hemos de hablar de las **formas de protección de nuestros sistemas**.

Para proteger nuestro sistema hemos de realizar un **análisis de las amenazas potenciales** que puede sufrir, las **pérdidas** que podrían generar, y la **probabilidad de su ocurrencia**; a partir de este análisis hemos de **diseñar una política de seguridad** que defina responsabilidades y **reglas a seguir** para evitar tales amenazas o minimizar sus efectos en caso de que se produzcan. A los mecanismos utilizados para implementar esta política de seguridad se les denomina **mecanismos de seguridad** son la parte más visible de nuestro sistema de seguridad, y se convierten en la herramienta básica para garantizar la protección de los sistemas o de la propia red.

Se distinguirán y estudiarán en los próximos temas las medidas de seguridad:

- **Activas:** que evitan daños en los sistemas informáticos, mediante:
  - Empleo de contraseñas adecuadas en el acceso a sistemas y aplicaciones.
  - Encriptación de los datos en las comunicaciones.
  - Filtrado de conexiones en redes.
  - El uso de software específico de seguridad informática. Antimalware.
- **Pasivas:** que minimizan el impacto y los efectos causados por accidentes, mediante:
  - Uso de hardware adecuado, protección física, eléctrica y ambiental.
  - Realización de copias de seguridad, que permitan recuperar los datos.

A lo largo de los siguientes temas analizaremos desde distintas perspectivas la seguridad informática:

- ✓ Capítulo 2: Seguridad física y ambiental.
- ✓ Capítulo 3: Seguridad lógica. Gestión de usuarios, privilegios, contraseñas, y actualizaciones.
- ✓ Capítulo 4: Software de seguridad, principalmente antimalware.
- ✓ Capítulo 5: Gestión de almacenamiento de la información, copias de seguridad y restauraciones.
- ✓ Capítulo 6: Seguridad en redes y comunicaciones.
- ✓ Capítulo 7: Encriptación de la información.
- ✓ Capítulo 8: Normativa legal en materia de seguridad. LOPD y LSSICE.
- ✓ Capítulo 9: Auditorías de seguridad informática.

ACTIVIDADES

Realiza un glosario de términos nuevos que encuentres en el siguiente artículo y busca sus definiciones formales en Internet. ¿Has recibido alguna vez un spam? ¿Podrías indicar algún ejemplo?

Realiza un debate en el que se analicen las posibles amenazas existentes en los sistemas del aula y qué tipo de medidas de prevención preliminares se podrían tomar.

El término phishing aparece por primera vez en el año 1996 en las newsgroups de hackers y en la edición del Magazine 2600. Este término tiene dos orígenes: 1) Fishing o pesca, refiriéndose a la pesca de credenciales o a la pesca de ingenuos para intentos de fraude, 2) Phishing - Password Harvesting que viene a significar cosecha de contraseñas.

En 1996 un phisher se hizo pasar por técnico de AOL y envió mensajes haciendo uso de la ingeniería social en los que solicitaba que el usuario verificase su cuenta o confirmase una factura y así poder solicitar las credenciales personales de la víctima. Con estos datos ya podía realizar acciones como el envío de spam. Para intentar solucionarlo, AOL incluyó como texto por defecto en el intercambio de mensajes: AOL nunca le solicitará contraseñas o información de facturación.

En 2001 aparecen los primeros scam en Hotmail con el texto "Usted es uno de los 100 ganadores de Hotmail" junto con un formulario que solicitaba el usuario y la contraseña de la cuenta de la víctima. Aunque este mensaje aparecía firmado por el Staff de Hotmail, en realidad provenía de una dirección IP de Ucrania. También AOL informó de un caso similar en donde el usuario recibía un mensaje que le avisaba de un error en su registro y no podían facturarle, para evitar que se le diera de baja debería rellenar un formulario lo antes posible. Además, incluía un enlace a una página para realizar la facturación de AOL. Ese mismo año se recibieron mensajes informando que un grupo de hackers había accedido a la base de datos de MSN en donde solicitaban el envío de un correo con los datos personales y la cuenta (usuario y contraseña) porque de lo contrario serían borrados de la base de datos.

En 2002 fueron los usuarios de ICQ quienes recibieron mensajes simulando la imagen de ICQ, en los que les solicitaban sus datos personales en un formulario, y mediante un script redireccionaban sus datos a una dirección de Hotmail. A finales de año Yahoo informaba que varios de sus clientes habían recibido correos donde les solicitaban los datos de sus tarjetas de crédito.

En 2003 le tocó el turno a los usuarios de EBAY quienes recibieron correos que simulaban alertas de Paypal solicitando sus datos bancarios y los números de sus tarjetas de crédito. Después aparecieron los primeros phishing a entidades de banca online como Barclays Bank, BBVA, en donde los phishers usaron técnicas para la ofuscación de URL. También comenzaron a registrarse nombres de dominio similares a los de las entidades bancarias. A finales de año se detectaron los primeros correos dirigidos a banca online que incluían troyanos con técnicas de ocultación. Un caso fue un ataque que introducía un troyano embedido en código HTML e incluía un script en la máquina de la víctima. Ese troyano era una variante del Spy-Tofger.

Las técnicas que se usaron a partir de entonces se enfocan hacia intentos de fraude como:

- Correos electrónicos: masivos de spam, selectivos, acompañados por ingeniería social para captar la atención de la víctima, también podían hacer uso de webspoofing o falsas páginas web, algunas venían acompañadas de malware que redirige el nombre de dominio a otra máquina (pharming). Aparece por primer vez un troyano con capacidad para capturar las pulsaciones de teclado (Keylogger).
- Sitio web: malware que explotaba las vulnerabilidades sin parchear de los navegadores, en el sistema operativo, y una vez infectado redireccionaba a los usuarios a servidores web en donde estaban las páginas que suplantaban a las originales. También se

insertaba código malicioso en HTML, frames, scripts PHP, en donde se ocultaban keyloggers, capturadores de pantalla, backdoors. Banners publicitarios para redireccionar al usuario a sitios con confiables.

- IRC y mensajería instantánea: donde se enviaban imágenes, URL, a los usuarios con contenidos maliciosos. Se enviaba SPAM y se conectaban bots para propagar los contenidos.
- VoIP: simulación telefónica, uso de Bots-IVR que solicitaban las credenciales personales. Redirección a webspoofing, otros canales.
- Buscadores: que proporcionaban sitios maliciosos en respuesta a las búsquedas de comercio electrónico o banca online.
- Mensajes en foros, en redes sociales, tablones de anuncios, con mensajes con ingeniería social para captar a la víctima.
- Redes P2P, descarga de software desde páginas de descarga masiva.
- Plataformas de juegos online, recordamos los casos de phishing que han sufrido los jugadores del World of Warcraft.
- Falsos antivirus y antispyware, utilizando llamativos anuncios o pop-ups con avisos alarmantes que advierten al usuario que su sistema está infectado y debe comprar la solución que se le propone. Al usar su tarjeta para obtener este producto sus datos son capturados para su posterior uso fraudulento.
- Vía teléfono móvil (SMiShing), enviando un SMS al usuario en donde se le invita a enviar su información privada o visitar un sitio web con contenidos maliciosos.
- Botnets: que tratan de controlar un número masivo de máquinas para la captura de datos bancarios, cuentas de correo.

El objetivo de estas mafias es la búsqueda de usuarios y los datos de sus cuentas bancarias. Haciendo uso de la ingeniería social, el spam y el malware. Entrando en las redes sociales como Facebook o Twitter. Aprovechándose de mensajes con carga emocional, como por ejemplo la catástrofe en Haití (terremoto 2010), en donde ya se han detectado casos de phishing para lucrar a estas organizaciones.

Los usuarios y las entidades deben tener una actitud responsable y utilizar medidas de protección. Se debe concienciar y educar al ciudadano para estar alerta y evitar que sus datos personales y bancarios sean robados.

ACTIVIDADES

En esta actividad vamos a analizar el centro de seguridad de sistemas Windows. Verifica que tienes correctamente configuradas sus opciones.

Sistema operativo Windows XP. Ir a Panel de control / Seguridad / Centro de seguridad.

En esta ubicación podemos encontrar algunos aspectos centralizados sobre seguridad del sistema:

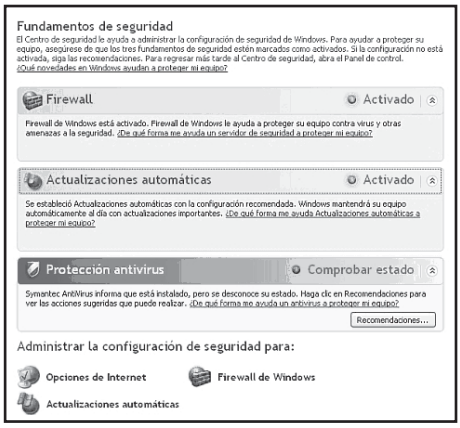
Para acceder al Centro de seguridad en Windows XP, debemos pulsar en el Inicio de Windows e ingresar al Panel de control.

Hacemos clic sobre "Centro de seguridad". A continuación, se abrirá la ventana del Centro de seguridad. Aquí encontraremos

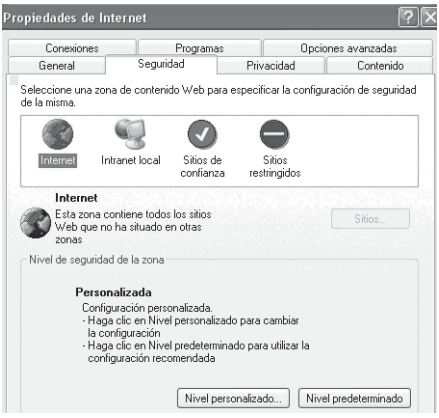
- Firewall.
- Actualizaciones automáticas.
- Protección antivirus.

Una luz verde nos indicará si están activados y una luz roja nos informará si están desactivados, o si hay que verificar su estado.

En la parte inferior de la ventana, tenemos tres opciones: Opciones de Internet, Firewall de Windows y Actualizaciones de Windows.



Ingresando a Opciones de Internet, en la solapa "Seguridad", podremos definir el nivel de seguridad de la navegación. Esta ventana, tiene botones que nos permiten agregar "Sitios de confianza" o definir una lista de "Sitios restringidos".



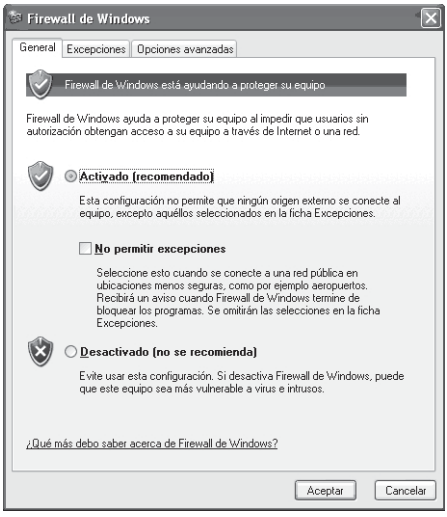
Si realizamos algún cambio en la configuración, debemos confirmarlo con el botón "Aplicar" y luego con "Aceptar".

Nuevamente, desde el Centro de seguridad de Windows, podremos configurar el Cortafuegos ingresando a "Firewall de Windows".

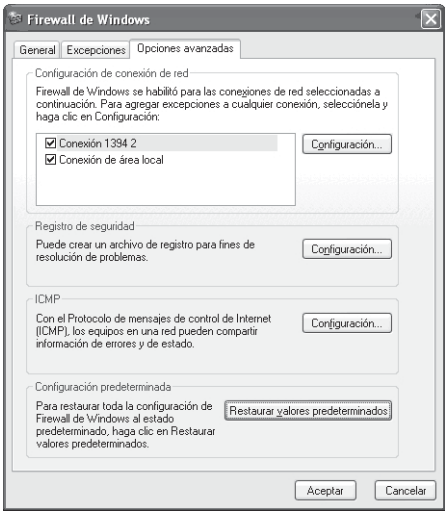
En esta ventana, podremos elegir entre tres opciones:

- Activado (es la opción por defecto).
- No permitir excepciones (es una alternativa útil cuando se necesita mayor seguridad), no permitiendo que ninguna aplicación tenga conexión de red.

- Desactivado (esta opción se puede utilizar si vamos a instalar un firewall distinto al que provee Windows).



Si ingresamos a la solapa "Excepciones" encontraremos una lista de programas que podremos marcar o desmarcar, para permitirles o prohibirles el acceso a la red.



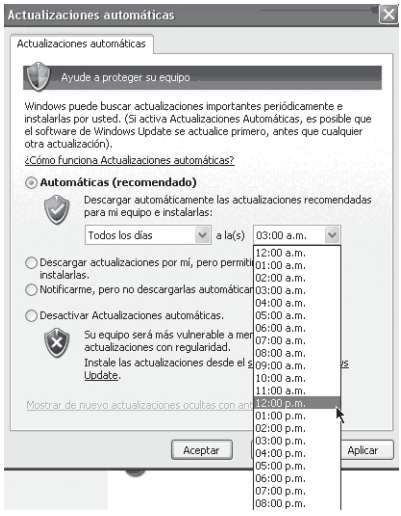
Podremos agregar nuevos programas a la lista y también puertos. Contamos con la posibilidad de configurar el firewall, para que nos advierta cuando está bloqueando un programa.

Dentro de la solapa "Opciones avanzadas" podremos habilitar o deshabilitar conexiones de red y configurar el registro de seguridad, entre otras opciones.

Si realizamos algún cambio, podremos confirmarlo con el botón "Aceptar".

Desde el Centro de seguridad de Windows, podremos ingresar a la opción "Actualizaciones automáticas". En esta ventana elegimos si deseamos que Windows descargue las actualizaciones de seguridad de manera automática.

Si escogemos esta alternativa, podremos indicar qué día y a qué hora, el equipo debe conectarse para verificar si hay alguna actualización.



También podremos optar para que se realice la descarga, pero elegir cuándo se instalan; notificación sin descarga automática; o desactivar la descarga automática, para manejar este tema por nuestra cuenta.

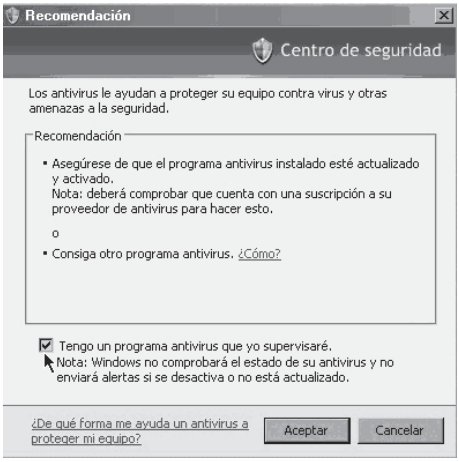
Si realizamos alguna modificación en la configuración, debemos confirmarlo con el botón "Aplicar" y luego con "Aceptar".

Nota: Si deseamos acceder a Microsoft Update para ver las últimas actualizaciones de nuestro sistema operativo, podremos hacerlo entrando con Internet Explorer 5 o superior a: http://www.update.microsoft.com/

En el ítem "Protección de virus" el sistema puede detectar si tenemos instalado un antivirus. Sin embargo, en algunos casos, nos puede alertar si no logra verificar al fabricante o las definiciones de virus.

Si preferimos manejar el antivirus por nuestra cuenta, sin que Windows nos

muestre las alertas del centro de seguridad para este ítem, hacemos clic en el botón "Recomendaciones" y accedemos a una ventana donde podemos tildar la opción "Tengo un programa antivirus que yo supervisaré".



De esta manera, el ítem "Protección antivirus" en el Centro de seguridad se pondrá de color amarillo y nos mostrará un cartel "Sin supervisión".

1.5 REFERENCIAS WEB

- ✓ Sitio web sobre seguridad informática de Microsoft: http://www.microsoft.com/spain/protect/default.mspx
- ✓ Sitio web sobre seguridad informática de GNU/Linux, de Criptonomicón, un servicio ofrecido libremente desde el Instituto de Física Aplicada del CSIC: http://www.iec.csic.es/CRIPTonOMICon/linux/
- ✓ *INTECO* - Instituto Nacional de Tecnologías de la Comunicación: www.inteco.es/
- ✓ Hispasec Sistemas: Seguridad y Tecnologías de información. Resúmenes anuales de noticias de actualidad sobre seguridad informática: http://www.hispasec.com/

RESUMEN DEL CAPÍTULO

En este capítulo se han analizado los fundamentos y conceptos de la seguridad informática.

Los principios que todo sistema informático debe contemplar son:

- **Confidencialidad**, es decir, no desvelar datos a usuarios no autorizados; que comprende también la privacidad (la protección de datos personales).
- **Disponibilidad**, esto es, que la información se encuentre accesible en todo momento a los distintos usuarios autorizados.
- **Integridad**, que permite asegurar que los datos no se han falseado.
- **Autenticación**, verificación de la identidad de un usuario, a partir de ese momento se considera un usuario autorizado.
- El **no repudio** o irrenunciabilidad, estrechamente relacionado con la autenticación, permite probar la participación de las partes en una comunicación.

Las amenazas a los sistemas que provienen de distintos ámbitos:

- **Personas:** como personal de la empresa, ex-empleados, curiosos, hacker, cracker, Intrusos remunerados
- **Amenazas lógicas**: software incorrecto, herramientas de seguridad, puertas traseras, bombas lógicas, canales cubiertos, virus, gusanos, caballos de Troya, programas conejo o bacterias
- **Amenazas físicas**: robos, sabotajes, destrucción de sistemas, cortes, subidas y bajadas bruscas de suministro eléctrico, condiciones atmosféricas adversas, catástrofes (naturales o artificiales como incendios).

Por otro lado en cuanto a las medidas para la prevención y recuperación se distinguen entre:

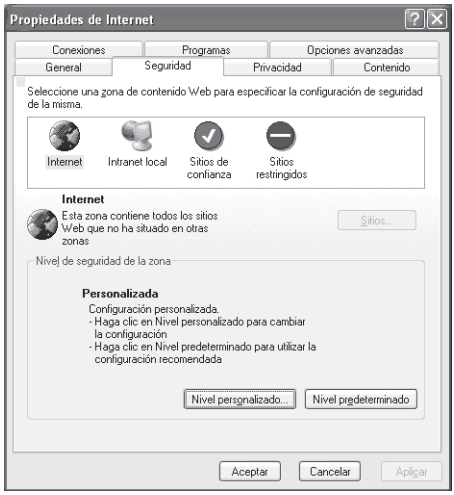
- **Activas:** contraseñas, encriptación y filtrado en las comunicaciones, uso de antimalware.
- **Pasivas:** protección física, eléctrica y ambiental, copias de seguridad, control de acceso físico.

Debemos ser conscientes de que las medidas de seguridad que deberán establecerse comprenden un conjunto de elementos que no pueden ser tratados dejando de lado o desprotegido ninguno de ellos: hardware, sistema operativo, comunicaciones (por ejemplo, medios de transmisión), medidas de seguridad físicas (ubicación de los equipos, suministro eléctrico, etc.), los controles organizativos (políticas de seguridad, niveles de acceso, contraseñas, normas, procedimientos, etc.) y legales (por ejemplo, la Ley Orgánica de Protección de Datos, LOPD).

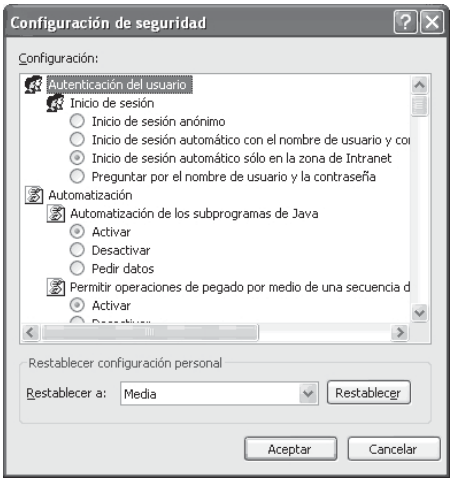
En los siguientes capítulos analizaremos dichas medidas para hacer de la seguridad la seña de identidad de nuestros sistemas.

EJERCICIOS PROPUESTOS

- **1.** Configura el firewall de tu sistema operativo para evitar contestar a peticiones de red de echo entrante.
- **2.** Configura el firewall para evitar que su navegador web tenga acceso a Internet.
- **3.** Contesta a las siguientes preguntas:
  ¿Qué nivel de seguridad posees en tu navegador web Internet Explorer? Puedes analizarlo en las propiedades de Internet / pestaña de privacidad.



En opciones avanzadas. Entre el nivel de configuración de seguridad a nivel medio y a nivel básico encuentra las diferencias de configuración de las opciones de seguridad. ¿Qué restricciones propone el nivel alto?



- **4.** ¿Dispones de restricciones de acceso a sitios web? Ver pestaña de seguridad en el apartado Sitios restringidos.

- **5.** ¿Tu sistema posee protección antivirus? ¿Te la proporciona el sistema operativo?

- **6.** Busca un software antivirus en línea y realiza un análisis de tu sistema.

TEST DE CONOCIMIENTOS

1 El servicio de no repudio:
- **a)** Se produce entre dos partes de una comunicación.
- **b)** Lo verifica el receptor.
- **c)** Se puede verificar por un tercero.
- **d)** Se realiza por emisor y un agente externo a la comunicación.

2 Indica qué sentencia es falsa:
- **a)** La integridad permite asegurar que los datos no se han falseado.
- **b)** Confidencialidad es desvelar datos a usuarios no autorizados; que comprende también la privacidad (la protección de datos personales).
- **c)** Disponibilidad es que la información se encuentre accesible en todo momento a los distintos usuarios autorizados.

3 ¿Cúal de estos principios no es aplicable a la seguridad informática?:
- **a)** Confidencialidad.
- **b)** Integridad.
- **c)** Disponibilidad.
- **d)** Verificación.
- **e)** No repudio.

4 ¿Qué elemento de un sistema informático se considera más crítico a la hora de protegerlo?:
- **a)** Comunicaciones.
- **b)** Software.
- **c)** Hardware.
- **d)** Datos.

5 Un hacker:
- **a)** Siempre tiene una finalidad maliciosa.
- **b)** La mayoría de las veces tiene una finalidad maliciosa.
- **c)** A veces posee una finalidad maliciosa, entonces se denomina cracker.
- **d)** Es un curioso con finalidad impredecible.

6 El phishing:
- **a)** Es un tipo de fraude bancario.
- **b)** Es un tipo de malware o virus.
- **c)** Se contrarresta con un spyware.
- **d)** Se propaga mediante correo electrónico siempre.

2 Seguridad física

Objetivos del capítulo

- ✓ Profundizar en aspectos de seguridad física y ambiental.
- ✓ Analizar los distintos dispositivos hardware que permiten mejorar la seguridad física.
- ✓ Valorar la importancia para la empresa de un centro de procesamiento de datos (CPD).
- ✓ Investigar sobre nuevos métodos de seguridad física y de control de acceso a los sistemas mediante biometría.

2.1 PRINCIPIOS DE LA SEGURIDAD FÍSICA

Es muy importante ser consciente que por más que nuestra empresa sea la más segura desde el punto de vista de ataques externos, hackers, virus, etc., la seguridad de la misma será nula si no se ha previsto cómo combatir un incendio.

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.

Esto puede derivar en que para un atacante sea más fácil lograr tomar y copiar una cinta de la sala, que intentar acceder vía lógica a los datos que contiene la misma.

Así, la seguridad física consiste en la ***aplicación de barreras físicas y procedimientos de control, como medidas de prevención y contramedidas ante amenazas a los recursos e información confidencial***. Se refiere a los controles y mecanismos de seguridad dentro y alrededor de la ubicación física de los sistemas informáticos, así como los medios de acceso remoto al y desde el mismo; implementados para proteger el hardware y medios de almacenamiento de datos.

En este tema se abarcarán medidas aplicables tanto a equipos de hogar y pequeñas oficinas como a servidores y centros de procesamiento de datos (CPD), que por su gran valor en la empresa requieren de medidas de seguridad específicas.

Analizaremos a continuación las principales amenazas a las que se ven sometidos los sistemas informáticos en general, y medidas adoptadas para su protección.

Cada sistema es único y por lo tanto la política de seguridad a implementar no será única. Es por ello que siempre se recomendarán pautas de aplicación general y no procedimientos específicos.

La **seguridad física** está enfocada 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:

- ✓ Amenazas ocasionadas por el hombre, como robos, destrucción de información, o equipos, etc.
- ✓ Desastres naturales, alteraciones y cortes de suministro eléctrico, incendios accidentales, tormentas e inundaciones.
- ✓ Disturbios, sabotajes internos y externos deliberados.

No hace falta recurrir a películas de espionaje para sacar ideas de cómo obtener la máxima seguridad en un sistema informático, además de que la solución sería extremadamente cara.

A veces basta recurrir al sentido común para darse cuenta que cerrar una puerta con llave o cortar la electricidad en ciertas áreas siguen siendo técnicas válidas en cualquier entorno.

2.1.1 CONTROL DE ACCESO

Los ordenadores, servidores, así como las copias de seguridad con datos importantes y el software, son elementos valiosos para las empresas y están expuestas a posibles robos y actos delictivos como sabotajes o destrozos, por parte de personal ajeno o propio de la empresa.

El software es una propiedad muy fácilmente sustraíble y las cintas y discos son fácilmente copiados sin dejar ningún rastro.

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

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.

A cualquier personal ajeno a la planta se le solicitará completar un **formulario** de datos personales, los motivos de la visita, hora de ingreso y de regreso, etc.

El uso de **credenciales de identificación** es uno de los puntos más importantes del sistema de seguridad, a fin de poder efectuar un control eficaz del ingreso y egreso del personal a los distintos sectores de la empresa.

En este caso la persona se identifica por **algo que posee**, por ejemplo una llave, o una tarjeta de identificación, o tarjeta inteligente (SmartCard). Cada una de éstas debe tener un PIN (Personal Identification Number) único, siendo este el que se almacena en una base de datos que controla el servicio de vigilancia para su posterior seguimiento, si fuera necesario. Su mayor desventaja es que estas tarjetas pueden ser copiadas, robadas, etc., permitiendo ingresar a cualquier persona que la posea.

Estas credenciales se pueden clasificar de la siguiente manera:

- ✓ Normal o definitiva: para el personal permanente de la empresa.
- ✓ Temporal: para personal recién ingresado.
- ✓ Contratistas: personas ajenas a la empresa, que por razones de servicio deben ingresar a la misma.
- ✓ Visitas. Para un uso de horas.

Las personas también pueden acceder mediante **algo que saben** (por ejemplo un número de identificación o una password) que se solicitará a su ingreso. Al igual que el caso de las tarjetas de identificación los datos introducidos se contrastarán contra una base donde se almacenan los datos de las personas autorizadas. Este sistema tiene la desventaja que generalmente se eligen identificaciones sencillas, bien se olvidan dichas identificaciones o incluso las bases de datos pueden verse alteradas o robadas por personas no autorizadas.

La principal desventaja de la aplicación de personal de guardia es que éste puede llegar a ser sobornado por un tercero para lograr el acceso a sectores donde no esté habilitado, como así también para poder ingresar o salir de la empresa con materiales no autorizados. Esta situación de soborno puede ocurrir frecuentemente, por lo que es recomendable la utilización de sistemas biométricos para el control de accesos.

ACTIVIDADES

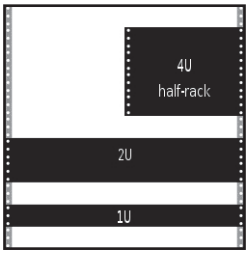
En esta actividad vamos a analizar distintas soluciones de seguridad física para evitar posibles robos, como son:

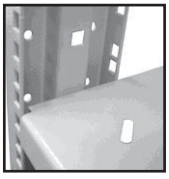
- Armarios de seguridad con llave, para sistemas informáticos.
- Cables de seguridad para portátiles.
- Llaves y candados para equipos y periféricos.

Una solución muy empleada para la seguridad de los sistemas informáticos, es disponer los mismos en un **armario o rack bajo llave**.

Un rack es un bastidor destinado a alojar equipamiento electrónico, informático y de comunicaciones. Sus medidas están **normalizadas** para que sea compatible con equipamiento de cualquier fabricante. También son llamados bastidores, cabinets o armarios.

Los racks son un simple armazón metálico con un ancho normalizado de **19 pulgadas**, mientras que el alto y el fondo son variables para adaptarse a las distintas necesidades. El armazón cuenta con guías horizontales donde puede apoyarse el equipamiento, así como puntos de anclaje para los tornillos que fijan dicho equipamiento al armazón. En este sentido, un rack es muy parecido a una simple estantería.

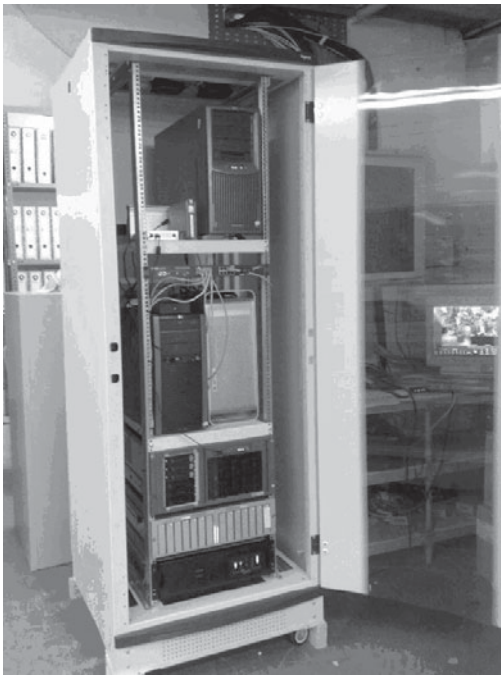




Los racks son muy útiles en un centro de proceso de datos, donde el espacio es escaso y se necesita alojar un gran número de dispositivos. Estos dispositivos suelen ser:

Servidores cuya carcasa ha sido diseñada para adaptarse al bastidor. Existen servidores de 1U, 2U y 4U, y recientemente, se han popularizado los servidores blade que permiten compactar más, compartiendo fuentes de alimentación y cableado.

- Conmutadores y enrutadores de comunicaciones.
- Paneles de parcheo, que centralizan todo el cableado de la planta.
- Cortafuegos.
- Sistemas de audio y vídeo.



El equipamiento simplemente se desliza sobre un raíl horizontal y se fija con tornillos. También existen **bandejas** que permiten apoyar equipamiento no normalizado o atornillado en la guías de 19". Por ejemplo, un monitor, PC de sobremesa y un teclado.

Las guías poseen agujeros a intervalos regulares llamados unidades de Rack (U) agrupados de tres en tres. Verticalmente, los racks se dividen en regiones de **1,75 pulgadas de altura**. En cada región hay tres pares de agujeros siguiendo un orden simétrico. Esta región es la que se denomina altura o U.

Lo normal es que existan desde 4U de altura hasta 46U de altura. La profundidad del bastidor no está normalizada, ya que así se otorga cierta flexibilidad al equipamiento. No obstante, suele ser de 600, 800 o incluso 1001 milímetros.

- Encuentra un armario y sus características en dimensiones para que dé cabida a un switch, panel de parcheo, PC (sobremesa con funciones de servidor) con monitor, teclado, ratón, y SAI. En primer lugar, deberás elaborar una lista con las dimensiones de cada componente, para poder hacer una estimación del espacio necesario en el armario.
- ¿Qué precio y en qué distribuidor has encontrado dicho armario? ¿Qué características tiene la puerta y la llave de dicho armario, crees que sería totalmente seguro? Explica tus razones.
- A través del distribuidor www.senfor.com podrás encontrar un conjunto de soluciones de seguridad para aulas de ordenadores. Diseña una solución con presupuesto, que permita dar seguridad a un aula como la que dispones, en la que se quiera tener también 15 ordenadores portátiles.

ACTIVIDADES

- Busca en la web de alguna empresa que facilite soluciones de control de accesos a CPD, como por ejemplo www.zksoftware.es, encuentra y explica las diferencias existentes, entre los terminales de presencia (con tarjeta identificadora), terminales de huella dactilar, y terminales con código y password. Analiza y explica cómo funciona el software de control de accesos, para una empresa con cientos de empleados.

2.1.2 SISTEMAS BIOMÉTRICOS

Definimos a la **Biometría** como *la parte de la biología que estudia en forma cuantitativa la variabilidad individual de los seres vivos utilizando métodos estadísticos*.

La Biometría es una tecnología que realiza mediciones en forma electrónica, guarda y compara características únicas para la identificación de personas.

La forma de identificación consiste en la comparación de características físicas de cada persona con un patrón conocido y almacenado en una base de datos. Los lectores biométricos identifican a la persona **por lo que es** (manos, ojos, huellas digitales y voz).

Beneficios de una tecnología biométrica:

- Pueden eliminar la necesidad de poseer una tarjeta para acceder, y de una contraseña difícil de recordar o que finalmente acaba siendo escrita en un papel visible por cualquier persona.
- Utilizando un dispositivo biométrico los costes de administración son más pequeños, se realiza el mantenimiento del lector, y una persona se encarga de mantener la base de datos actualizada. Sumado a esto, las características biométricas de una persona son intransferibles a otra.

Emisión de calor

Se mide la emisión de calor del cuerpo (termograma), realizando un mapa de valores sobre la forma de cada persona.

Huella digital

Basado en el principio de que no existen dos huellas dactilares iguales, este sistema viene siendo utilizado desde el siglo pasado con excelentes resultados.

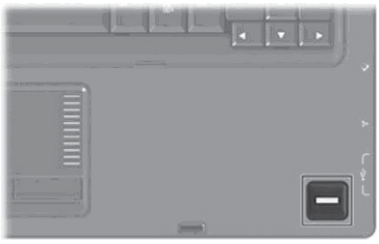
Cada huella digital posee pequeños arcos, ángulos, bucles, remolinos, etc. (llamados **minucias**) características y la posición relativa de cada una de ellas es lo analizado para establecer la identificación de una persona. Está aceptado que cada persona posee más de 30 minucias, y que dos personas no tienen más de ocho minucias iguales, lo que hace al método sumamente confiable.

ACTIVIDADES

Muchas aplicaciones de negocios y sitios web requieren que los usuarios introduzcan un nombre de usuario y contraseña para acceder a la información protegida. El lector de huellas digitales permite iniciar sesión en un sitio protegido colocando el dedo sobre un sensor, en lugar de usar el teclado para ingresar sus datos. El lector de huellas digitales puede adquirirse independiente del equipo mediante soluciones USB lectores de huella dactilar o puede venir integrado en la carcasa de muchos equipos portátiles como es el caso de los equipos HP, pero no en todos.

En este último caso HP, el administrador de acceso por huella digital (Fingerprint Logon Manager) es un software que permite acceder a diversas aplicaciones y sitios web con su huella digital. Fingerprint Logon Manager guarda un registro de los diferentes sitios visitados y de los nombres de usuario y contraseñas utilizados.

Cuando se abre un sitio web o un programa en la página de inicio para el cual se requiere inicio de sesión con huella digital, una vez se use la huella, Fingerprint Logon Manager ingresa automáticamente el nombre de usuario y contraseña correctos. Este procedimiento es mucho más fácil que intentar recordar e introducir nombre de usuario y contraseña.



En los notebooks y portátiles HP, el lector de huellas digitales es un pequeño sensor metálico ubicado cerca del teclado o pantalla. Al pasar el dedo sobre el sensor metálico puede **iniciar sesión en el PC, una red o abrir un programa**.

- Busca información referente al lector de huella dactilar de hp y contesta las siguientes preguntas como entrada en tu blog:

  a. ¿Cuáles son las ventajas de usar el lector de huellas digitales para iniciar sesión en mi equipo?

  b. ¿Cómo es el proceso de configuración software del lector de huellas digitales?

c. ¿Qué precauciones o recomendaciones de uso se recomiendan a la hora de emplear el lector de huella?

d. ¿Se puede iniciar la sesión en Windows con el lector de huellas digitales?

e. ¿Se puede usar un dedo diferente para iniciar sesión en el PC?

f. ¿Es posible que varios usuarios inicien sesión con el lector de huellas digitales en el mismo PC?

ACTIVIDADES

Ya existen ratones informáticos con lectores de huellas digitales. El ratón es capaz de reconocer nuestra huella digital e identificarnos. Vinculando ese ratón con nuestra huella digital y solamente identificándonos como dueños del ratón gracias a nuestras huellas podríamos usarlo. También existe este concepto para el teclado.

Un teclado y ratón con lector de huellas digitales.

La idea consiste en ampliar este concepto de forma que cuando el ratón reconozca nuestras huellas también se active automáticamente el teclado, sin necesidad de que el teclado incorpore el lector, al menos en los equipos no portátiles. El lector de huellas digitales serviría tanto para desbloquear el ratón como para desbloquear el teclado. De manera que el sistema quedaría totalmente protegido, inaccesibles todos los archivos de tu ordenador para los amigos de lo ajeno. Es cierto que se pueden poner contraseñas antes del inicio de sesión e incluso, con determinados programas, encriptar las carpetas deseadas. Pero, ¿y si nos hemos dejado el ordenador encendido para descargar algo de Internet y nos hemos ido? O, como ocurre frecuentemente, con el messenger conectado donde cualquiera puede chatear con nuestros contactos y ver nuestros mensajes. La novedad de este sistema consiste en que el bloqueo y el desbloqueo de tu ordenador se realiza en cuestión de segundos. Cada vez que se retiran los dedos del ratón, el ratón y el teclado exigirán el reconocimiento dactilar para ponerse de nuevo en funcionamiento.

- Si tu equipo no dispone de lector de huella existen diversos periféricos que permiten el control del PC únicamente mediante la utilización de la huella registrada de usuario. Investiga acerca de los precios y características de periféricos como teclado, ratón, o lector de huella USB, así como las opciones de software que existen, como eNDeSS. Realiza una tabla resumen. ¿Qué niveles de acceso controla dicho software?

Verificación de voz

La dicción de una (o más) frase es grabada y en el acceso se compara la voz (entonación, diptongos, agudeza, etc.).

Este sistema es muy sensible a factores externos como el ruido, el estado de ánimo y enfermedades de la persona, el envejecimiento, etc.

ACTIVIDADES

- Analiza el sistema BioCloser de reconocimiento de voz en la web: http://www.biometco.com/productos/control.acceso/biocloser.php.
- Explica, mediante una entrada en tu blog, su principio de funcionamiento y para qué se puede emplear.

Verificación de patrones oculares

Estos modelos pueden estar basados en los patrones del iris o de la retina y hasta el momento son los considerados más efectivos (en 200 millones de personas la probabilidad de coincidencia es casi 0).

Su principal desventaja reside en la resistencia por parte de las personas a que les analicen los ojos, por revelarse en los mismos, enfermedades que en ocasiones se prefiere mantener en secreto.

Verificación Automática de Firmas (VAF)

Mientras es posible para un falsificador producir una buena copia visual o facsímil, es extremadamente difícil reproducir las dinámicas de una persona: por ejemplo la firma genuina con exactitud.

La VAF, usando emisiones acústicas, toma datos del proceso dinámico de firmar o de escribir.

La secuencia sonora de emisión acústica generada por el proceso de escribir constituye un patrón que es único en cada individuo. El patrón contiene información extensa sobre la manera en que la escritura es ejecutada. El equipamiento de colección de firmas es inherentemente de bajo coste y robusto.

Esencialmente, consta de un bloque de metal (o algún otro material con propiedades acústicas similares) y una computadora con una base de datos con patrones de firmas, asociadas a cada usuario.

Tabla-Resumen comparativa de soluciones biométricas:

Existen algunas otras soluciones a la biometría más complejas y menos usadas en acceso a organizaciones o a un sistema informático concreto, como son la geometría de la mano y el reconocimiento facial.

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

Tabla 2.1

	Ojo (Iris)	Huellas dactilares	Escritura y firma	Voz
Fiabilidad	Muy alta	Muy alta	Media	Alta
Facilidad de uso	Media	Alta	Alta	Alta
Prevención de ataques	Muy alta	Alta	Media	Media
Aceptación	Media	Alta	Muy alta	Alta
Estabilidad	Alta	Alta	Baja	Media

2.1.3 PROTECCIÓN ELECTRÓNICA

Se llama así a la detección de robo, intrusión, asalto e incendios mediante la utilización de **sensores conectados a centrales de alarmas**. Estas centrales tienen conectados los elementos de señalización, que son los encargados de hacer saber al personal de una situación de emergencia. Cuando uno de los elementos sensores detectan una situación de riesgo, éstos transmiten inmediatamente el aviso a la central; ésta procesa la información recibida y ordena en respuesta la emisión de señales sonoras o luminosas alertando de la situación.

Barreras infrarrojas y de micro-ondas

Transmiten y reciben haces de luces infrarrojas y de micro-ondas respectivamente. Se codifican por medio de pulsos con el fin de evadir los intentos de sabotaje. Estas barreras están compuestas por un transmisor y un receptor de igual tamaño y apariencia externa.

Cuando el haz es interrumpido, se activa el sistema de alarma, y luego vuelve al estado de alerta. Estas barreras son inmunes a fenómenos aleatorios como calefacción, luz ambiental, vibraciones, movimientos de masas de aire, etc.

Detector ultrasónico

Este equipo utiliza ultrasonidos para crear un campo de ondas. De esta manera, cualquier movimiento que realice un cuerpo dentro del espacio protegido generará una perturbación en dicho campo que accionará la alarma. Este sistema posee un circuito refinado que elimina las falsas alarmas. La cobertura de este sistema puede llegar a un máximo de 40 metros cuadrados.

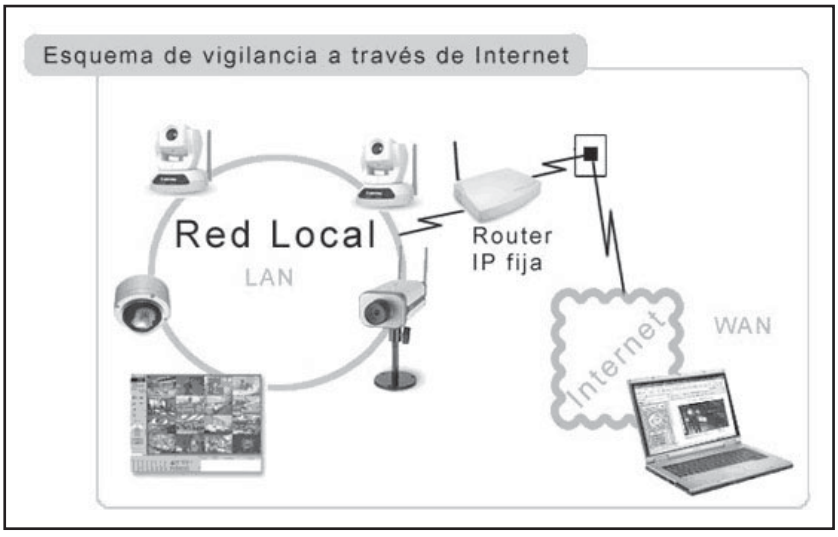
Circuitos cerrados de televisión (CCTV)

Permiten el control de todo lo que sucede en la planta según lo captado por las cámaras estratégicamente colocadas. Los monitores de estos circuitos deben estar ubicados en un sector de alta seguridad. Las cámaras pueden estar a la vista (para ser utilizadas como medida disuasiva) u ocultas (para evitar que el intruso sepa que está siendo captado por el personal de seguridad).

Todos los elementos anteriormente descriptos poseen un control contra sabotaje, de manera que si en algún momento se corta la alimentación o se produce la rotura de alguno de sus componentes, se enviará una señal a la central de alarma para que ésta accione los elementos de señalización correspondientes.

ACTIVIDADES

Las **cámaras IP** son dispositivos autónomos que cuentan con un servidor web de vídeo incorporado, lo que les permite transmitir su imagen a través de redes IP como redes **LAN**, **WAN** e **Internet**. Las cámaras IP permiten al usuario tener la cámara en una localización y ver el vídeo en tiempo real desde otro lugar a través de Internet.



Las cámaras IP tienen incorporado un microprocesador, pequeño y especializado en ejecutar aplicaciones de red. Por lo tanto, la cámara IP no necesita estar conectada a un PC para funcionar. Esta es una de sus diferencias con las denominadas cámaras web o webcam. Algunas cámaras IP tienen sensor de movimiento, e incluso pueden ser controladas remotamente a nivel de zoom y rotación para enfocar algún objeto o posición concreta.

Las imágenes se pueden visualizar utilizando un navegador web estándar y pueden almacenarse en cualquier disco duro. Tanto si necesita una solución de vigilancia IP para garantizar la seguridad de personas y lugares, como para supervisar propiedades e instalaciones de modo remoto o retransmitir eventos en la Web con imágenes y sonidos reales, las cámaras IP satisfacen sus necesidades.

Una cámara IP tiene su propia dirección IP y se conecta a la red como cualquier otro dispositivo; incorpora el software necesario de servidor de web, servidor o cliente FTP, de correo electrónico... y tiene la capacidad de ejecutar pequeños programas personalizados (denominados scripts).

- Diseña una infraestructura de cámaras de vigilancia IP inalámbricas, con 4 cámaras que permita controlar la planta de un edificio. Indica los equipos necesarios aparte de las cámaras, espacio de almacenamiento necesario, y períodos de realización de copias de seguridad.
- Crea una tabla con el coste de la instalación desglosado con cada uno de sus componentes así como la mano de obra de instalación y configuración.
- ¿Qué leyes se aplican sobre la filmación de vídeo en espacios públicos y en privados?. A modo de resumen, ¿qué precauciones y recomendaciones se deben tomar a la hora de realizar grabaciones de seguridad? Busca alguna noticia sobre la implantación de cámaras de seguridad en las vías públicas de las ciudades y qué tipo de controversias ha originado.

2.1.4 CONDICIONES AMBIENTALES

Normalmente se reciben por anticipado los avisos de tormentas, tempestades, tifones y catástrofes sísmicas similares. Las condiciones atmosféricas severas se asocian a ciertas partes del mundo y la probabilidad de que ocurran está documentada.

La frecuencia y severidad de su ocurrencia deben ser tenidas en cuenta al decidir la construcción de un edificio. 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.

Incendios

Los incendios son causados por el uso inadecuado de combustibles, fallo 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.

Desgraciadamente los sistemas antifuego dejan mucho que desear, causando casi igual daño que el propio fuego, sobre todo a los elementos electrónicos. El dióxido de carbono, actual alternativa del agua, resulta peligroso para los propios empleados si quedan atrapados.

Los diversos factores a contemplar para reducir los riesgos de incendio a los que se encuentra sometido un centro de procesamiento de datos (CPD) son:

- ✓ El área en la que se encuentran las computadoras debe estar en un local que no sea combustible o inflamable.
- ✓ El local no debe situarse encima, debajo o adyacente a áreas donde se procesen, fabriquen o almacenen materiales inflamables, explosivos, gases tóxicos o sustancias radioactivas.
- ✓ Las paredes deben hacerse de materiales incombustibles y extenderse desde el suelo al techo.
- ✓ Debe construirse un falso suelo instalado sobre el suelo real, con materiales incombustibles y resistentes al fuego.

- ✓ No debe estar permitido fumar en el área de proceso.
- ✓ El suelo y el techo en el recinto del centro de cómputo y de almacenamiento de los medios magnéticos deben ser impermeables.
- ✓ Deben instalarse extintores manuales (portátiles) y/o automáticos (rociadores).

Sistema de aire acondicionado

Se debe proveer un sistema de calefacción, ventilación y aire acondicionado separado, que se dedique al cuarto de computadoras y equipos de proceso de datos en forma exclusiva.

Teniendo en cuenta que los aparatos de aire acondicionado son causa potencial de incendios e inundaciones, es recomendable instalar redes de protección en todo el sistema de cañería al interior y al exterior, detectores y extintores de incendio, monitores y alarmas efectivas.

Inundaciones

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, es una de las causas de mayores desastres en centros de cómputos.

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.

Para evitar este inconveniente se pueden tomar las siguientes medidas: construir un techo impermeable para evitar el paso de agua desde un nivel superior y acondicionar las puertas para contener el agua.

Terremotos

Estos fenómenos sísmicos pueden ser tan poco intensos que solamente instrumentos muy sensibles los detectan, o tan intensos que causan la destrucción de edificios y hasta la pérdida de vidas humanas. El problema es que en la actualidad, estos fenómenos están ocurriendo en lugares donde no se los asociaba. Por fortuna los daños en las zonas improbables suelen ser ligeros.

2.2 SISTEMAS DE ALIMENTACIÓN ININTERRUMPIDA (SAI)

Trabajar con computadoras implica trabajar con electricidad. Por lo tanto, esta es una de las principales áreas a considerar en la seguridad física. Además, es una problemática que abarca desde el usuario hogareño hasta la gran empresa.

En la medida que los sistemas se vuelven más complicados se hace más necesaria la presencia de un especialista para evaluar riesgos particulares y aplicar soluciones que estén de acuerdo con una norma de seguridad industrial.

Un **SAI** (Sistema de Alimentación Ininterrumpida), también conocido por sus siglas en inglés **UPS** (*Uninterruptible Power Supply,* suministro de energía ininterrumpible), es un dispositivo que gracias a sus baterías puede proporcionar energía eléctrica tras un apagón a todos los dispositivos que tenga conectados, durante un tiempo limitado, permitiendo de este modo poder apagar los equipos sin que sufran cortes sus fuentes de alimentación.

Pequeño **SAI** independiente a dos vistas. Los distintos dispositivos hardware no irán enchufados a las tomas de corriente directamente, se enchufarán a la SAI que será la que estará conectada al enchufe, haciendo de este modo de intermediario, entre la red eléctrica y los dispositivos hardware.

Las SAI se ajustan a las necesidades energéticas de los equipos existentes.

Otra de las funciones de los SAI es la de **mejorar la calidad de la energía eléctrica** que llega a los aparatos, **filtrando subidas y bajadas de tensión y eliminando armónicos de la red en el caso de usar corriente alterna,** que tenemos en los enchufes. Los SAI dan energía eléctrica a equipos llamados cargas críticas, como pueden ser aparatos médicos, industriales o informáticos que, como se ha dicho antes, 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).

2.2.1 CAUSAS Y EFECTOS DE LOS PROBLEMAS DE LA RED ELÉCTRICA

El 50% de los problemas ocasionados en los equipos eléctricos e informáticos y las pérdidas de información son debidos a interrupciones y perturbaciones en el suministro de la red eléctrica suponiendo unas pérdidas en el mundo de aproximadamente 26 billones de dólares.

Según un estudio del National Power Quality Laboratory de Canadá, cada año se producen aproximadamente en un edificio de oficinas de cualquier ciudad del mundo unos 36 picos de tensión, 264 bajadas de red, 128 sobre-voltajes o subidas de tensión, 289 microcortes menores a 4 ms y aproximadamente entre 5 a 15 apagones de red mayores a 10 segundos. Realmente de cada 100 perturbaciones 40 causaron pérdidas de datos o incidencias en las cargas conectadas.

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

Los nueve problemas de la energía son:

1. **Cortes de energía o apagones (blackout).**

   Es la pérdida total del suministro eléctrico. Puede ser causado por diversos eventos; relámpagos, fallos de las líneas de energía, exceso de demandas, accidentes y desastres naturales. Puede causar daños en el equipo electrónico (hardware), pérdida de datos o parada total del sistema.

2. **Bajadas de voltaje momentáneo o microcortes (sag).**

   Es la caída momentánea de voltaje, generada por el arranque de grandes cargas, encendido de maquinaria pesada, fallos de equipos. Se presenta de manera similar a los apagones pero en oleadas repetitivas. Las bajadas de voltaje momentáneo pueden causar principalmente daños al hardware y perdida de datos.

3. **Picos de tensión o alto voltaje momentáneo (surge).**

   Los picos pueden ser producidos por una rápida reducción de las cargas, cuando el equipo pesado es apagado, por voltajes que están por encima del 110 % de la nominal. Los resultados pueden ser daños irreversibles al hardware.

4. **Bajadas de tensión sostenida (undervoltage)**.

   Bajo voltaje sostenido en la línea por periodos largos de unos cuantos minutos, horas y hasta días. Pueden ser causados por una reducción intencionada de la tensión para conservar energía durante los periodos de mayor demanda. El bajo voltaje sostenido puede causar daños al hardware principalmente.

5. **Sobrevoltaje o subidas de tensión (overvoltage).**

   Sobrevoltaje en la línea por períodos largos. Puede ser causado por un relámpago y puede incrementar el voltaje de la línea hasta 6.000 voltios en exceso. El sobrevoltaje casi siempre ocasiona pérdida de la información y daños del hardware.

6. **Ruido eléctrico (line noise).**

   Significa interferencias de alta frecuencia causadas por radiofrecuencia (RFI) o interferencia electromagnética (EMI). Pueden ser causadas por interferencias producidas por transmisores, máquinas de soldar, impresoras, relámpagos, etc. Introduce errores en los programas y archivos, así como daños a los componentes electrónicos.

7. **Variación de frecuencia (frequency variation).**

   Se refiere a un cambio en la estabilidad de la frecuencia. Resultado de un generador o pequeños sitios de cogeneración siendo cargados o descargados. La variación de frecuencia puede causar un funcionamiento errático de los equipos, pérdida de información, caídas del sistema y daños de equipos.

8. **Transientes o micropicos (switching transient).**

   Es la caída instantánea del voltaje en el rango de los nanosegundos. La duración normal es más corta que un pico. Puede originar comportamientos extraños del ordenador y proporcionando estrés en los componentes electrónicos quedando propensos a fallos prematuros.

9. **Distorsión armónica (harmonic distortion).**

Es distorsión de la forma de onda normal. Es causada por cargas no lineales conectadas a la misma red que los equipos, ordenadores y/o aplicaciones críticas. Motores, copiadoras, máquinas de fax, etc., son ejemplos de cargas no lineales. Puede provocar sobrecalentamiento en los ordenadores, errores de comunicación y daño del hardware.

CONSECUENCIAS

Un mal suministro de energía eléctrica afecta la productividad de las empresas, ya que:

1. **Destruyen la información:**

   Una variación en el flujo de energía eléctrica puede dañar datos confidenciales, documentos de operación diaria, estadísticas e información financiera.

2. **Dañan las infraestructuras:**

   Cada variación en el voltaje va disminuyendo la vida útil de ordenadores personales, servidores, controles de máquinas, estaciones de trabajo y redes informáticas entre otros.

3. **Generan estrés:**

   Las constantes interrupciones en la continuidad laboral y consecuente caída de productividad genera estrés y desmotivación en los recursos humanos.

4. **Afecta a la productividad:**

   Las interrupciones de operación de las compañías afectan la productividad y la generación de ingresos.

5. **Generan pérdidas:**

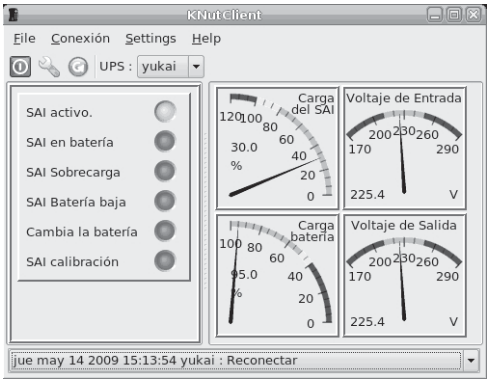
   Los problemas eléctricos interrumpen la continuidad de operación, ocasionando importantes pérdidas en las empresas.

2.2.2 TIPOS DE SAI

Habitualmente, los fabricantes de SAI clasifican los equipos en función del tipo de energía eléctrica (alterna o continua) que producen a su salida:

- **SAI de continua**. Los equipos o cargas conectadas a los SAI requieren una alimentación de corriente continua, por lo tanto éstos transformarán la corriente alterna de la red comercial a corriente continua y la usarán para alimentar a la carga y almacenarla en sus baterías. Por lo tanto no requieren convertidores entre las baterías y las cargas.

- **SAI de alterna**. Estos SAI obtienen a su salida una señal alterna, por lo que necesitan un inversor para transformar la señal continua que proviene de las baterías en una señal alterna. Habitualmente es el tipo de SAI que se comercializa, ya que los equipos informáticos requieren para su funcionamiento enchufes de corriente alterna como los disponibles en cualquier hogar u oficina. La mayoría de las SAI comerciales permiten conexión USB o de red local, entre el PC y la SAI, para monitorizar su estado en el PC mediante software.



Según los fallos eléctricos que corrigen, disponibilidad, fiabilidad, etc., se pueden clasificar en:

- **SAI off-line o interactivo no senoidal (protección nivel 3 - equipos básicos)**: es un equipo que por su precio es el que más extendido está, sobre todo para la protección de pequeñas cargas (PC, cajas registradoras, TPV, etc.). Este tipo de SAI alimenta a las cargas críticas, que tiene que proteger, con una seguridad y protección relativa dependiendo del tipo de off-line (estabilizados y con o sin filtros) dentro de una escala de 1 a 100 los off-line estarían entre 40 y 60 puntos en relación a la protección que deberían de tener los equipos informáticos, por supuesto siempre en consonancia con el tipo de equipos a proteger y la zona (industrial, oficinas, muy conflictiva en tormentas o en cortes de suministro, etc.). Básicamente los equipos off-line actúan en el momento en que la red desaparece o baja por debajo de la nominal 220 voltios, produciéndose en el cambio de red a baterías un pequeño micro-corte el cual para una mayoría de equipos eléctricos e informáticos es inapreciable, no así para equipos muy sofisticados.

- **SAI on-line y line interactive (protección nivel 5)**: El SAI on-line cumple verdaderamente para casi todos los problemas ocasionados por fallos en la compañía eléctrica tanto como por otros problemas ocasionados por las líneas eléctricas dentro de polígonos industriales y oficinas, como ruido eléctrico etc. Los equipos ON-LINE suelen dar una protección del orden de entre 70 y 90 puntos en una escala de protección de 1 a 100, convirtiéndose por tanto en muy fiables. Existen diferentes tipos de topología en los equipos ON-LINE pero todas cumplen francamente con su función dejando pocas ventanas abiertas a los posibles problemas.

- **SAI on-line doble conversión (protección nivel 9)**: La verdadera diferencia entre los SAI se encuentra en los equipos **on-line de doble conversión** ya que los equipos **off-Line**, **línea interactiva** y **on-line de una conversión** están siempre dependientes de una manera u otra de que la entrada eléctrica al equipo cumpla unas mínimas condiciones para el correcto funcionamiento de los equipos. En los equipos de **doble conversión** no dependen de la línea de entrada para trabajar con una protección de más del 95% eliminando por completo todos los problemas ocasionados por las líneas eléctricas y las compañías de electricidad además de problemas normalmente metereológicos que son inesperados.

2.2.3 POTENCIA NECESARIA

Para ajustar las dimensiones y capacidad eléctrica de la SAI a la que enchufar nuestros equipos, es necesario realizar un cálculo de la potencia que consumimos y por tanto que necesitamos suministrar.

La **potencia eléctrica** se define como la cantidad de energía eléctrica o trabajo que se transporta o que se consume en una determinada unidad de tiempo.

Si la tensión eléctrica (voltaje medido en voltios, V) se mantiene constante, la potencia es directamente proporcional a la corriente eléctrica (intensidad medida en amperios, A). Ésta aumenta si la corriente aumenta.

Cuando se trata de corriente continua (CC) la potencia eléctrica desarrollada en un cierto instante por un dispositivo de dos terminales, es el producto de la diferencia de potencial entre dichos terminales y la intensidad de corriente que pasa a través del dispositivo. Esto es, **P = V x I.**

Donde **I** es el valor instantáneo de la corriente y **V** es el valor instantáneo del voltaje. Si **I** se expresa en amperios y **V** en voltios, **P** estará expresada en watts (vatios). Igual definición se aplica cuando se consideran valores promedio para **I**, **V** y **P**.

En circuitos eléctricos de corriente alterna (CA), como son las tomas de corriente (enchufes), se emplean medidas de potencia eficaz o aparente y potencia real. La unidad de potencia para configurar un SAI es el voltiamperio (VA), que es **potencia aparente**, también denominada potencia efectiva o eficaz, consumida por el sistema. Para calcular cuanta energía requiere tu equipo, busca el consumo en la parte trasera del aparato o en el manual del

usuario. Si tenemos la potencia en vatios (W) (**potencia real**), multiplica la cantidad de vatios por 1,4 para tener en cuenta el pico máximo de potencia que puede alcanzar su equipo, por ejemplo: 200 W x 1,4 = 280 VA. En ocasiones el factor 1,4, puede ser 1,33 o 1,6 o factor divisor 0,7 o 0,75.

Si lo que se encuentra es la tensión y la corriente nominales, para calcular la potencia aparente (VA) hay que multiplicar la corriente (amperios) por la tensión (voltios), obteniéndose la potencia en W, para luego multiplicarla por factor 1,4. Por ejemplo: 3 amperios x 220 voltios = 660 W. 660 W x 1,4 = 924 VA.

ACTIVIDADES

En la web www.newsai.es/fqa.htm podrás encontrar la mayor parte de las cuestiones técnicas referentes a una SAI.

- Encuentra una SAI, justificando tu respuesta, para un equipo que tiene una fuente de alimentación ATX de 450 W, y un monitor de 17", de consumo 75 W, teniendo en cuenta que se quiere dimensionar para que el consumo de equipos alcance el 75% de la potencia suministrada por la SAI, que se pueda monitorizar el estado en el PC y el tiempo de suministro bajo corte eléctrico sea de 1 hora permitiendo apagar el PC y guardar los trabajos abiertos con tiempo suficiente.

ACTIVIDADES

- Lista las características de potencia del equipamiento informático de aula, ordenadores, monitores, otros periféricos (altavoces, impresoras, etc.), dispositivos de red (como switches, puntos de acceso, etc.), buscando la potencia consumida de cada uno, ayudándote de los manuales o con un software de diagnóstico como Everest o Aida32. Indica qué dispositivos necesitarían estar enchufados a la SAI por ser críticos, y estima el número de tomas de corriente y la potencia necesaria de una SAI.
- A continuación busca una solución comercial e indica sus características y el coste.
- Contesta a las siguientes cuestiones:
- ¿Qué potencia suministra la fuente de alimentación de tu torre de sobremesa?

- ¿Es necesario disponer una SAI para un portátil o un notebook?¿Por qué? ¿Qué función realiza el transformador de corriente?¿Y las celdas de baterías?

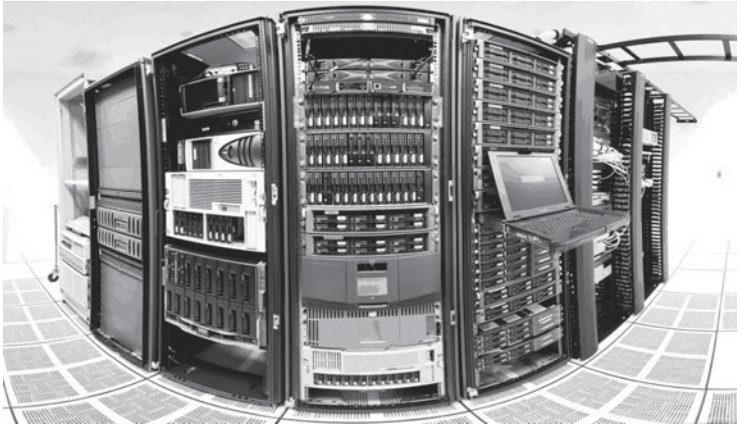
Ayudate de estas estimaciones de consumo medio de potencia. EJEMPLOS DE CONSUMO MEDIO en Volt Amperios:

- ✓ Pentium II 190 VA
- ✓ Pentium III y IV 240 VA
- ✓ Monitor 14" - 15" 70 VA
- ✓ Monitor 17" - 20" 180 VA
- ✓ Impresora de tinta 90 VA
- ✓ Impresora láser 400 VA
- ✓ Hub, Switch, Bridge, FAX o Router 150 VA
- ✓ Ecáner 160 VA

2.3 CENTROS DE PROCESADO DE DATOS (CPD)

Se denomina procesamiento de datos o CPD a aquella ubicación donde se concentran todos los recursos necesarios para el procesamiento de la información de una organización. También se conoce como **centro de cómputo** (Iberoamérica) o **centro de cálculo** (España) o centro de datos por su equivalente en inglés **data center.**

Dichos recursos consisten esencialmente en unas dependencias debidamente acondicionadas, servidores y redes de comunicaciones.



2.3.1 EQUIPAMIENTO DE UN CPD

Un CPD, por tanto, es un edificio o sala de gran tamaño usada para mantener en él una gran cantidad de equipamiento electrónico. Suelen ser creados y mantenidos por grandes organizaciones con objeto de tener acceso a la información necesaria para sus operaciones.

Por ejemplo, un banco puede tener un data center con el propósito de almacenar todos los datos de sus clientes y las operaciones que éstos realizan sobre sus cuentas. Prácticamente todas las compañías que son medianas o grandes tienen algún tipo de CPD, mientras que las más grandes llegan a tener varios interconectados, en distintas ubicaciones geográficas.

Entre los factores más importantes que motivan la creación de un CPD se puede destacar el **garantizar la continuidad y disponibilidad** del servicio a clientes, empleados, ciudadanos, proveedores y empresas colaboradoras, pues en estos ámbitos es muy importante la protección física de los equipos informáticos o de comunicaciones implicados, así como servidores de bases de datos que puedan contener información crítica. Requisitos generales:

- **Disponibilidad y monitorización "24x 7x 365"**: un centro de datos diseñado apropiadamente proporcionara disponibilidad, accesibilidad y confianza 24 horas al día, 7 días a la semana, 365 días al año.
- **Fiabilidad infalible (5 nueves):** Es decir, con un 99,999% de disponibilidad, lo que se traduce en una única hora de no disponibilidad al año. Los centros de datos deben tener redes y equipos altamente robustos y comprobados.
- **Seguridad, redundancia y diversificación:** Almacenaje exterior de datos, tomas de alimentación eléctrica totalmente independientes y de servicios de telecomunicaciones para la misma configuración, equilibrio de cargas, SAI o sistemas de alimentación ininterrumpida), control de acceso, etc.
- **Control ambiental / prevención de incendios:** El control del ambiente trata de la calidad del aire, temperatura, humedad inundación, electricidad, control de fuego, y por supuesto, acceso físico.
- **Acceso a Internet y conectividad a redes de área extensa WAN para conectividad a Internet:** Los centros de datos deben ser capaces de hacer frente a las mejoras y avances en los equipos, estándares y anchos de banda requeridos, pero sin dejar de ser manejables y fiables.

El diseño de un centro de procesamiento de datos comienza por la elección de su **ubicación geográfica**, y requiere un balance entre diversos factores:

- ✓ Coste económico: coste del terreno, impuestos municipales, seguros, etc.
- ✓ Infraestructuras disponibles en las cercanías: energía eléctrica, carreteras, acometidas de electricidad, centralitas de telecomunicaciones, bomberos, etc.
- ✓ Riesgo: posibilidad de inundaciones, incendios, robos, terremotos, etc.

Una vez seleccionada la ubicación geográfica es necesario encontrar unas dependencias adecuadas para su finalidad, ya se trate de un local de nueva construcción u otro ya existente a comprar o alquilar. Algunos **requisitos de las dependencias son**:

- ✓ Una buena ubicación son las plantas intermedias o ubicaciones centrales en entornos de campus.
- ✓ Una planta con altura de suelo a techo mínima de 3 m, preferiblemente más. Esto será suficiente para un piso con un falso suelo de 300 a 600 milímetros y proporcionará el suficiente espacio libre para los equipos y racks.
- ✓ Una ruta de acceso amplia para canalizaciones. La ruta debe ser grande y bastante fuerte para servir como toma de aire, material informático o para módulos de fuente de alimentación continua.
- ✓ Espacio para salas posibles de extensión.

Aún cuando se disponga del local adecuado, siempre es necesario algún **despliegue de infraestructuras en su interior**:

- Falsos suelos y falsos techos, con placas de fibra de vidrio.
- Cableado de red y teléfono. Todos los cables tendidos bajo el suelo deberían ser LSZH (Low Smoke Zero Halogen).
- Doble cableado eléctrico.
- Generadores y cuadros de distribución eléctrica.
- Acondicionamiento de salas.
  - Las paredes del CPD deben tener un grado mínimo de resistencia al fuego de una hora (RF-60) aunque se recomienda un grado RF-120, y deben proporcionar barrera frente al humo.
  - Todas las puertas de acceso deben tener una ventana con cierre propio.
  - Todos los materiales usados en la construcción de la sala de ordenadores deben ser incombustibles.
  - Para controlar el daño por agua, todas las entradas del piso, de la pared y del techo deben estar selladas.
  - Los extintores manuales contra el fuego deben ser de dióxido de carbono u otros gases con agentes de extinción.
  - No debe haber componentes químicos de extinción por polvo seco en el área de ordenadores.
- Instalación de alarmas, control de temperatura y humedad con avisos SNMP (mensajes a una base de datos de gestión remota) o SMTP (mediante envío de correo electrónico) o SMS/MMS vía teléfono móvil.

Generalmente en un CPD, todos los grandes servidores se suelen concentrar en una sala denominada sala fría, nevera o pecera. Esta sala requiere un sistema específico de refrigeración para mantener una temperatura baja (entre 21 y 23 grados centígrados), necesaria para evitar averías en las computadoras a causa del sobrecalentamiento.

Según las normas internacionales, la temperatura exacta debe ser **22,3 grados centígrados.**

La pecera suele contar con medidas estrictas de seguridad en el acceso físico, así como medidas de extinción de incendios adecuadas al material eléctrico, tales como extinción por agua nebulizada o bien por gas INERGEN, dióxido de carbono o nitrógeno.

Una parte especialmente importante de estas infraestructuras son aquellas destinadas a la **seguridad física de la instalación**, lo que incluye:

- ✓ Cerraduras electromagnéticas, controladas por algún mecanismo de control de acceso por tarjeta, pin o biometría.
- ✓ Tornos.
- ✓ Cámaras de seguridad.
- ✓ Detectores de movimiento.
- ✓ Tarjetas de identificación.

Una vez acondicionado el habitáculo se procede a la instalación de las computadoras, las redes de área local, etc. Esta tarea requiere un **diseño lógico** de redes y entornos, sobre todo en aras a la seguridad. Algunas actuaciones son:

- ✓ Instalación y configuración de los servidores y periféricos.
- ✓ Despliegue del cableado y configuración de la electrónica de red: pasarelas, encaminadores, conmutadores, etc.
- ✓ Segmentación de redes locales y creación de redes virtuales (VLAN).
- ✓ Creación de zonas desmilitarizadas (DMZ), mediante cortafuegos (firewalls).
- ✓ Creación de la red de almacenamiento de información (SAN).
- ✓ Creación de los entornos de explotación, pre-explotación, desarrollo de aplicaciones y gestión en red.

ACTIVIDADES

ANÁLISIS DE CPD EN UNA SOLUCIÓN REAL

Solución integral de CPD altamente seguro para Supermercados Condis

Condis es una empresa familiar de distribución de productos de alimentación y supermercados, con presencia principalmente en Cataluña y Madrid. Con más de 4.000 empleados, practica el denominado comercio de proximidad, con tiendas de barrio y supermercados de unos 600 m^2 que sirven como alternativa a las grandes superficies. Cuenta con cuatro plataformas logísticas desde las que dan servicio a sus más de 400 establecimientos, agrupados bajo las marcas Condis y Distop.

En 2005 la empresa ha facturado unos 660 millones de euros y espera continuar su crecimiento. Fue además la primera cadena de supermercados en ofrecer a sus clientes la opción de realizar sus compras directamente por Internet y recibirlas en su domicilio, a través del servicio denominado condisline.com.

La cadena de supermercados Condis se ha dotado de una nueva infraestructura física para su Centro de Proceso de Datos que proporciona a su información una mayor seguridad y protección ante riesgos no deseados. Abast Grup se ha encargado de la dirección del proyecto y propuso una solución de cerramiento modular que proporciona la máxima protección con una instalación mucho más rápida y limpia. El traslado técnico se realizó "en caliente", en un tiempo récord de un fin de semana, permitiendo así mantener los compromisos de disponibilidad de Condis.

Garantizar los criterios de seguridad

El CPD de Condis estaba antiguamente situado en una sala del departamento de informática cuyas paredes eran mamparas de madera y vidrio, idénticas a las que componían el resto de separaciones de las oficinas. Esta situación preocupaba a los responsables de TI, conscientes de que esa infraestructura física no proporcionaba suficientes garantías de seguridad frente a los riesgos de incendio, inundaciones o accesos no autorizados.

Jordi Roig Julià, jefe del departamento de sistemas corporativos de Condis, nos detalla la situación: "Algunas auditorías periódicas de calidad que realizábamos valoraban bastante bien las instalaciones del CPD, pero

nosotros sabíamos que había puntos mejorables. Por ejemplo, como las estadísticas hablan de un 1% de posibilidades de que se produzca algún incidente con fuego en un CPD, ya habíamos dotado a la sala de un sistema de detección y extinción de incendios propio, pero nos preocupaba que el riesgo de incendio pudiera venir del exterior, un entorno de oficina en el que casi todo es papel y madera. El riesgo de inundaciones también era pequeño pues ni por las paredes ni por el techo de la sala pasaban canalizaciones de agua, pero estaba bajo cubierta y en alguna otra zona del edificio se habían producido problemas de goteras en caso de lluvias torrenciales. En cuanto a los accesos no autorizados, lo cierto es que en Condis nunca hemos tenido ninguna situación de sabotaje por parte de personal interno, pero la auditoría sobre el cumplimiento de la LOPD nos alertó sobre la necesidad de proteger mejor el acceso a los datos y los sistemas de información".

Dicha auditoría sirvió como desencadenante del proyecto de mejora de la infraestructura física del CPD. "Nos dimos cuenta de que era ya el momento de abordar el problema y no aplazar más tiempo la solución", explica Roig. Las inquietudes del departamento de IT encontraron respuesta por parte del Consejo de Administración y la Dirección General de Condis, muy concienciados con todos los asuntos referentes a la seguridad, y se aprobó incluir el proyecto de una nueva sala CPD en los presupuestos del siguiente año fiscal.

Cerramiento modular, la opción más adecuada

Los primeros pasos fueron buscar cuál sería la ubicación más adecuada para la nueva sala de CPD y escoger un tipo de cerramiento totalmente estanco e ignífugo que proporcionase total protección frente a los riesgos de agua y fuego.

El lugar finalmente escogido fue una zona del almacén situada no demasiado lejos de las oficinas del departamento de IT, y en la que se encontraban ya instalados los SAI que proporcionan protección a los equipos frente a caídas o alteraciones de la red eléctrica. Para la elección del cerramiento se dejaron aconsejar por Abast Grup, con quien, según palabras del propio Roig "trabajamos juntos desde hace bastantes años y hemos establecido una relación de confianza".

La solución propuesta fue un cerramiento modular de la marca AST del tipo RF120 según la normativa EN1047, que cumplía todos los criterios de tiempo de resistencia al fuego, dureza, estanqueidad y resistencia al agua, etc.

El jefe del departamento de sistemas de Condis nos comenta algunas de las cualidades que vieron en esta propuesta: "Un cerramiento de este tipo presenta ventajas tanto a la hora de realizar el proyecto como más adelante si se han de abordar futuras ampliaciones. El proceso de instalación es mucho más rápido y limpio, y en caso de necesitar más metros cuadrados para nuevos equipos no sería necesario derribar ninguna pared, con el riesgo que esto supondría de polvo y escombros que podrían dañar los sistemas instalados, sino simplemente desmontar algunos paneles y ampliar".

Roig también destaca que el hecho de tratarse de una solución modular les permitió planificar el proyecto en dos fases y poder de esta manera ajustarse mejor a sus presupuestos anuales. En la primera fase se realizó la sala que alberga los equipos informáticos y en la segunda se hizo un cerramiento para proteger los SAI.

CPD altamente seguros

Para garantizar la seguridad frente a sabotajes o accesos no deseados se tomaron varias medidas. La sala del CPD se estructuró en dos zonas separadas, una para los equipos informáticos y otra para los sistemas de climatización, cuadro eléctrico y sistema de extinción de incendios. Cada una cuenta con una entrada propia con sistemas de control de acceso, y se han definido permisos diferentes para cada una, de forma que, por ejemplo, operarios responsables del mantenimiento pueden acceder a la zona de servicios pero no a la de sistemas. La sala de sistemas cuenta además con una cámara de vigilancia que graba todos los accesos. Tanto la cámara como el sistema de iluminación están diseñados para activarse a partir de sensores de movimiento.

El sistema de extinción de incendios es mediante gas, la opción que, garantizando la integridad de los equipos, resultaba más adecuada para las medidas de la sala. En una de las paredes se ha habilitado una válvula que permite que si se activa el sistema la primera acometida de gas a alta presión tenga una vía de salida que después queda sellada. De esta forma se evitan posibles daños tanto en los equipos como en la estructura debidos al aumento súbito de presión.

Abast Grup se encargó de la dirección de todo el proyecto, coordinando tanto los apartados de los que era responsable directo (estructura de sala, sistema eléctrico, cableado…) como los realizados por otras empresas (sistemas de climatización, detección y extinción de incendios), que Condis contrató directamente para reutilizar los sistemas que ya disponía en su antigua sala CPD.

La importancia de las comunicaciones

Parte de la electrónica de red de la LAN de Condis se dejó en la ubicación de la antigua sala CPD, pues desde allí salían los troncales que iban a los otros armarios de distribución. Para el nuevo CPD se adquirieron dos nuevos switches HP ProCurve 5308xl con 48 puertos Gigabit cada uno, y capacidad de expansión hasta 128 + 128 puertos Gb. Toda la electrónica de red de la LAN es ProCurve Networking, "porque cuando fue creciendo la red ya teníamos confianza en HP, que es la marca de la mayoría de los sistemas que tenemos, y porque los productos de ProCurve han tenido históricamente una excelente calidad relación/precio", comenta Jordi Roig.

Como proveedor de cableado, Condis confió en AMP Netconnect, una división del grupo Tyco Electrónics. Roig explica que "cuando el cableado dependía de Servicios Generales para cada ampliación se habían utilizado soluciones de proveedores diferentes. Cuando pasó a depender de nosotros consideramos que para evitar problemas era mejor homologar a un solo proveedor que realmente cubriera todas nuestras necesidades de cables y conectores dentro de su gama y nos diese total confianza en cuanto a calidad de producto, y escogimos a AMP Netconnect. Lo que hicimos entonces fue auditar el cableado existente, reemplazar el que no cumplía los criterios, y para todas las nuevas instalaciones utilizar soluciones de este fabricante".

Traslado técnico en tiempo récord

Mover todos los equipos de la antigua sala CPD a las nuevas instalaciones sin que el servicio a los usuarios se vea afectado suele ser uno de los puntos críticos de este tipo de proyectos. En el traslado del CPD de Condis, minuciosamente planificado, participaron ocho personas, cuatro de ellas de su departamento de IT y otras cuatro personal de Abast Grup.

Los equipos a trasladar eran un *rack* con la SAN (1 HP StorageWorks EVA 3000 con 2 controladoras y 4 bandejas de discos, 2 *switches* de fibra y 1 *appliance*) y 5 *racks* más de servidores con 8 sistemas HP900, 8 HP Proliant, 2 HP Netservers, 2 HP Integrity Servers (Itanium), 2 HASS (High Available Storage Systems) y una librería de cintas MSL, así como varias estaciones de trabajo, PC y sistemas de comunicaciones (*switches*, *routers*…).

El proceso se inició un viernes por la tarde, momento en el que se pudieron comenzar a parar servicios y trasladar equipos, como los del *data warehouse* o los utilizados para desarrollo. Jordi Roig explica que "La parte más crítica era la que hacía referencia a la SAN y los servidores

que soportan las aplicaciones relacionadas con la logística. Nuestros almacenes dejan de trabajar el sábado al mediodía y retoman su actividad por la tarde del domingo, por lo que la ventana de tiempo que teníamos para parar, desconectar, trasladar, volver a conectar y reiniciar estos equipos era bastante estrecha". Los últimos equipos en moverse fueron los relacionados con los supermercados, aunque Roig aclara que "los dejamos para la noche del sábado coincidiendo con el horario de cierre de nuestros establecimientos, pero en este caso el proceso era más simple porque, al contrario de lo que ocurre con oficinas y almacenes, la mayoría de las aplicaciones que se utilizan en las tiendas no son centralizadas. Además, otros servicios como el correo electrónico podían detenerse antes porque, como los supermercados lo utilizan solamente como correo interno con la central, el tráfico de mensajes de un sábado es muy escaso".

El traslado se realizó finalmente sin ningún imprevisto, y todo el proceso se completó el domingo sobre las 12 h de la mañana, unas horas incluso antes de lo esperado. La rapidez con que se llevó a término permitió que esta fase del proyecto no tuviese ninguna incidencia negativa en el cumplimiento de los criterios de disponibilidad de los servicios TI de Condis.

Fuente: http://www.abast.es/cs_condis_cpd.shtml

- ¿Qué se considera un "traslado en caliente"?
- ¿Cuáles eran los riesgos que corrían y que podrían poner en peligro su anterior CPD? ¿Qué es una auditoría?
- ¿Quién tomó la decisión de cambio?
- ¿Cómo se podrían resumir las soluciones adoptadas por la empresa en los distintos ámbitos?
- ¿Los SAI y los equipos se encuentran en la misma sala?¿Por qué?

2.4 REFERENCIAS WEB

- ✓ Sitio web sobre SAI.
  http://www.newsai.es/
- ✓ Catálogo, manuales y documentación de SAI.
  http://www.apc.com/es/
- ✓ Noticias y medidas de seguridad para CPD.
  http://www.seguridadcpd.com/
- ✓ Seguridad física. Red – Iris.
  http://www.rediris.es/cert/doc/unixsec/node7.html
- ✓ Soluciones técnicas para el control de acceso.
  http://www.accesor.com/
- ✓ Soluciones técnicas de biometría.
  http://www.biometriaaplicada.com/

RESUMEN DEL CAPÍTULO

En este capítulo hemos analizado los principios de la seguridad física: ***aplicación de barreras físicas y procedimientos de control, como medidas de prevención y contramedidas ante amenazas a los recursos e información confidencial***

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

- Amenazas ocasionadas por el hombre, como robos, destrucción de información o equipos, etc.

Para ello se adoptarán medidas con respecto a la vigilancia, detección de intrusos y control de acceso, y a las **credenciales de identificación: mediante** algo que se posee, llave, tarjeta de identificación o inteligente (SmartCard), algo que se sabe (número de identificación o una password). Actualmente, por **lo que se es**, biometría que realiza mediciones en forma electrónica, guarda y compara características únicas físicas (voz, huella, manos, características del ojo, etc.) para la identificación de personas.

- Desastres naturales, alteraciones y cortes de suministro eléctrico, incendios accidentales, tormentas e inundaciones.

  Para evitar cortes bruscos y otros efectos indeseados como picos de tensión en el suministro eléctrico, se emplearán **SAI** (Sistema de Alimentación Ininterrumpida), o **UPS** (dispositivo con baterías), que puede proporcionar energía eléctrica tras un apagón a todos los dispositivos que tenga conectados, durante un tiempo limitado, permitiendo de este modo poder apagar los equipos sin que sufran cortes sus fuentes de alimentación. También mejora la calidad de la energía eléctrica que llega a los dispositivos, filtrando subidas y bajadas de tensión de los enchufes.

  La unidad de potencia para adquirir un SAI es el voltiamperio (VA), **potencia aparente**, o eficaz. Para calcular cuánta energía requiere, si tenemos la potencia en vatios (W) (**potencia real**) se multiplica por 1,4 para tener en cuenta el pico máximo de potencia que puede alcanzar el equipo.

  Con respecto a los centros de procesado de datos (CPD) y la ubicación donde se concentran todos los recursos necesarios para el procesamiento de la información de una organización, tendremos especial cuidado de la seguridad física, con desastres como incendios, inundaciones, etc.

  Evaluar y controlar permanentemente la seguridad física del edificio, sala o cualquiera que sea la ubicación de los dispositivos informáticos, es la base para comenzar a integrar la seguridad como una función primordial dentro de cualquier organismo.

EJERCICIOS PROPUESTOS

1. A lo largo del curso se realizará un **manual de buenas prácticas y recomendaciones** a modo de resumen en dos ámbitos, calculando siempre el coste de la solución óptima:

A. A nivel de usuario, qué medidas y recomendaciones de equipamiento y uso tomarías.

B. A nivel de pequeña y mediana empresa, PYME, qué medidas y recomendaciones darías a un cliente, propietario de una PYME.

Las soluciones y recomendaciones se tomarán con respecto al Capítulo 2 en base a:

- Control de acceso físico a equipamiento informático.
- SAI o UPS.
- Condiciones ambientales, temperatura fundamentalmente.

TEST DE CONOCIMIENTOS

1 Las medidas de seguridad biométricas son:
- **a)** Permitir el acceso a un sistema mediante contraseña asimétrica.
- **b)** Emplear la biología para medir parámetros de seguridad.
- **c)** Emplear características biológicas para identificar usuarios.
- **d)** El fundamento de la identificación mediante certificado digital.

2 La unidad de potencia para configurar un SAI es el:
- **a)** Vatio (W) o potencia real.
- **b)** Voltiamperio (VA) o potencia aparente.
- **c)** Vatio (W) o potencia aparente.
- **d)** Voltiamperio (VA) o potencia real.

3 En un CPD el ancho de los armarios para comunicaciones y servidores tienen un ancho:

a) No normalizado, normalmente de 19".
b) Normalizado de 18".
c) No normalizado, normalmente de 18".
d) Normalizado a 19".

4 Los SAI:

a) Permiten conectarse ininterrumpidamente a la red eléctrica.
b) Suministran corriente eléctrica frente a cortes de luz.
c) Son dispositivos de almacenamiento de alta disponibilidad.
d) Son programas que permiten mantener confidencialidad.

5 Indicar la sentencia falsa. Los servicios de vigilancia mediante cámaras IP:

a) Se pueden monitorizar remotamente desde una red.
b) La cámara IP no puede funcionar sin alimentación de red eléctrica.
c) Se puede ver solo una imagen simultáneamente mediante una web, de una sola cámara.
d) Se pueden ver varias imágenes, de varias cámaras simultáneamente.

3 Seguridad lógica

Objetivos del capítulo

- ✓ Profundizar en aspectos de seguridad lógica.
- ✓ Garantizar el acceso restingido de los usuarios, mediante políticas de seguridad.
- ✓ Valorar la importancia del uso de contraseñas seguras.
- ✓ Restringir el acceso autorizado a ficheros, carpetas, aplicaciones y sistemas operativos.
- ✓ Analizar las ventajas de disponer el sistema y aplicaciones actualizadas.

3.1 PRINCIPIOS DE LA SEGURIDAD LÓGICA

Es importante recalcar que la mayoría de los daños que puede sufrir un sistema informático no será sobre los medios físicos sino contra información por él almacenada y procesada.

Así, la seguridad física sólo es una parte del amplio espectro que se debe cubrir para no vivir con una sensación ficticia de seguridad. Como ya se ha mencionado, el activo más importante que se posee es la **información**, y por lo tanto deben existir técnicas, más allá de la seguridad física, que la aseguren. Estas técnicas las brinda la seguridad lógica.

Es decir que la **seguridad lógica** consiste en la *aplicación de barreras y procedimientos que resguarden el acceso a los datos y sólo se permita acceder a ellos a las personas autorizadas para hacerlo*.

Existe un viejo dicho en la seguridad informática que dicta que todo lo que no está permitido debe estar prohibido y esto es lo que debe asegurar la seguridad lógica.

Los objetivos que se plantean serán:

- ✓ Restringir el acceso al arranque (desde la BIOS), al sistema operativo, los programas y archivos.
- ✓ Asegurar que los usuarios puedan trabajar sin una supervisión minuciosa y no puedan modificar los programas ni los archivos que no correspondan.
- ✓ Asegurar que se estén utilizando los datos, archivos y programas correctos en y por el procedimiento correcto, actualizando periódicamente los mismos.

3.2 CONTROLES DE ACCESO

Estos controles pueden implementarse en la BIOS, el sistema operativo, sobre los sistemas de aplicación, en bases de datos, en un paquete específico de seguridad o en cualquier otra aplicación.

Constituyen una importante ayuda para proteger al sistema operativo de la red, al sistema de aplicación y demás software de la utilización o modificaciones no autorizadas; para mantener la integridad de la información (restringiendo la cantidad de usuarios y procesos con acceso permitido) y para resguardar la información confidencial de accesos no autorizados.

Asimismo, es conveniente tener en cuenta otras consideraciones referidas a la seguridad lógica, como por ejemplo las relacionadas al procedimiento que se lleva a cabo para determinar si corresponde un permiso de acceso (solicitado por un usuario) a un determinado recurso.

3.2.1 IDENTIFICACIÓN Y AUTENTIFICACIÓN

Es la primera línea de defensa para la mayoría de los sistemas computarizados, permitiendo prevenir el ingreso de personas no autorizadas. Es la base para la mayor parte de los controles de acceso y para el seguimiento de las actividades de los usuarios.

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.

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:

- ✓ Algo que solamente el individuo **conoce**: por ejemplo una clave secreta de acceso o password, una clave criptográfica, un número de identificación personal o PIN, etc.
- ✓ Algo que la persona **posee:** por ejemplo una tarjeta magnética.

- ✓ Algo que el individuo **es** y que lo identifica unívocamente: por ejemplo las huellas digitales o la voz.
- ✓ Algo que el individuo es capaz de **hacer**, por ejemplo los patrones de escritura.

Para cada una de estas técnicas vale lo mencionado en el caso de la seguridad física en cuanto a sus ventajas y desventajas. Se destaca que en los dos primeros casos enunciados, es frecuente que las claves sean olvidadas o que las tarjetas o dispositivos se pierdan, mientras que por otro lado, los controles de autenticación biométricos serían los más apropiados y fáciles de administrar, resultando ser también los más costosos por lo dificultoso de su implementación eficiente.

Desde el punto de vista de la eficiencia, es conveniente que los usuarios sean identificados y autenticados solamente una vez, pudiendo acceder a partir de allí a todas las aplicaciones y datos a los que su perfil les permita, tanto en sistemas locales como en sistemas a los que deba acceder en forma remota. Esto se denomina *single login* o sincronización de passwords.

Una de las posibles técnicas para implementar esta única identificación de usuarios sería la utilización de un **servidor de autenticaciones** sobre el cual los usuarios se identifican, y que se encarga luego de autenticar al usuario sobre los restantes equipos a los que éste pueda acceder. Este servidor de autenticaciones no debe ser necesariamente un equipo independiente y puede tener sus funciones distribuidas tanto geográfica como lógicamente, de acuerdo con los requerimientos de carga de tareas. Es el caso de servidores LDAP en GNU/Linux y Active Directory sobre Windows Server.

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.

ACTIVIDADES

- Busca dentro de las opciones de configuración de la BIOS de tu placa base, si es posible asignar una contraseña en el arranque. ¿Cómo se puede retear dicha contraseña? ¿Crees que es útil y totalmente seguro este sistema de control de acceso? ¿Por qué?

3.2.2 ROLES

El acceso a la información también puede controlarse a través de la función, perfil o rol del usuario que requiere dicho acceso.

Algunos ejemplos de roles serían los siguientes: programador, líder de proyecto, gerente de un área usuaria, administrador del sistema, etc. En este caso los derechos de acceso y políticas de seguridad asociadas pueden agruparse de acuerdo con el rol de los usuarios.

3.2.3 LIMITACIONES A LOS SERVICIOS

Estos controles se refieren a las restricciones que dependen de parámetros propios de la utilización de la aplicación o preestablecidos por el administrador del sistema.

Un ejemplo podría ser que en la organización se disponga de licencias para la utilización simultánea de un determinado producto de software para cinco personas, en donde exista un control a nivel sistema que no permita la utilización del producto a un sexto usuario.

3.2.4 MODALIDAD DE ACCESO

Se refiere al modo de acceso que se permite al usuario sobre los recursos y a la información. Esta modalidad puede ser:

- **Lectura:** el usuario puede únicamente leer o visualizar la información pero no puede alterarla. Debe considerarse que la información puede ser copiada o impresa.
- **Escritura:** este tipo de acceso permite agregar datos, modificar o borrar información.
- **Ejecución:** este acceso otorga al usuario el privilegio de ejecutar programas.
- **Borrado:** permite al usuario eliminar recursos del sistema (como programas, campos de datos o archivos). El borrado es considerado una forma de modificación.
- **Todas las anteriores**.

Además, existen otras modalidades de acceso especiales, que generalmente se incluyen en los sistemas de aplicación:

- **Creación:** permite al usuario crear nuevos archivos, registros o campos.
- **Búsqueda:** permite listar los archivos de un directorio determinado.

ACTIVIDADES

PERMISOS EN EL SISTEMA DE ARCHIVOS GNU/LINUX

Para brindar algo de privacidad y protección cada archivo o directorio tiene asociados permisos diferentes para el dueño, para el grupo y para los demás usuarios. En el caso de archivos, los permisos que pueden darse o quitarse son: (r) lectura, (w) escritura y (x) ejecución. En el caso de directorios, los permisos son: (r) para listar los archivos, (w) para escribir, crear o borrar archivos y (x) para acceder a archivos del directorio.

Desde un administrador de archivos, puede ver los permisos de un archivo con el botón derecho del ratón cuando el puntero está sobre el archivo, escogiendo la opción apropiada del menú que aparece. Desde un intérprete de comandos o consola se puede emplear el comando **ls** con la opción -l. Un ejemplo del resultado de este comando se presenta a continuación:

```
 drwxr-xr-x    5 pepe   users       4096 Feb 21 06:31 graficas
 -rw-r-----    1 pepe   users      62561 May 13 18:13 c.tar.gz
lrwxrwxrwx    1 pepe   users         12 Nov 12  2000 a -> /etc/hosts
```

La primera línea presenta un directorio (la d al principio de la línea lo indica), la segunda presenta un archivo (el guión inicial lo indica) y la tercera un enlace. El nombre del directorio graficas, tiene 5 archivos, fue modificado por última vez el 21 de febrero del año en curso a las 6:31AM, el dueño es pepe, el grupo es users y el tamaño es 4096 bytes, en realidad el tamaño cobra sentido sólo en el caso de archivos como c.tar.gz cuyo tamaño es 62.561 bytes. Los tres caracteres rwx que siguen a la d inicial indican los permisos para el dueño, los tres siguientes r-x indican los permisos para el grupo y los tres siguientes r-x indican los permisos para el resto de usuarios. Como el orden de estos permisos es siempre el mismo (primero lectura r, después escritura w y después ejecución x), resulta que el archivo c.tar.gz no es ejecutable, que puede ser leído por el dueño y el grupo pero no por los demás usuarios, además puede ser escrito sólo por pepe. Del enlace podemos destacar que se llama a,

que enlaza al archivo /etc/hosts y que su tamaño y permisos reales los heredará de /etc/hosts.

Los permisos de un archivo pueden ser modificados por el dueño, propietario o por el administrador del sistema con el comando **chmod** que espera dos parámetros: cambio por realizar al permiso y nombre del archivo por cambiar. Los permisos se pueden especificar en octal o con una o más letras para identificar al usuario (u para el usuario, g para el grupo, o para los demás usuarios y a para todos), un +, un - o un = y después letras para identificar los permisos (r, w o x). Por ejemplo:

chmod og+x sube.sh

Da a los demás usuarios y al grupo permiso de ejecución del archivo sube.sh que debe estar en el directorio desde el cual se da el comando.

chmod a-w deu.txt

Quita el permiso de escritura en el archivo deu.txt, tanto al dueño como al grupo, como a los demás usuarios. Este mismo resultado puede obtenerse con el comando **chmod -w deu.txt**. Cuando no se especifican usuarios **chmod** toma por defecto todos los usuarios.

chmod u=rxw,g=rx,o= textos

Cambia permisos del archivo (o directorio), textos, el usuario puede leer, ejecutar y escribir, el grupo puede leer y ejecutar mientras que los demás usuarios no tienen permisos.

El dueño de un archivo puede ser modificado sólo por el administrador del sistema con el programa **chown**. Un usuario que pertenezca a varios grupos puede cambiar el grupo de uno de sus archivos a alguno de los grupos a los que perteneza con el programa o comando **chgrp**, por ejemplo:

chgrp estudiantes tarea1.txt

Cambiará el grupo del archivo tarea1.txt a estudiantes. Los grupos a los cuales un usuario pertenece son mostrados por el comando groups.

- Busca información sobre los archivos de configuración /etc/passwd, /etc/group y /etc/shadow. ¿Qué información proporcionan al sistema?
- Bajo sistemas Windows, ¿se puede modificar el propietario de un archivo?¿Qué opciones de seguridad existen sobre cada uno de los archivos?
- ¿Crees que el sistema de protección de archivos en GNU/Linux es más fiable y controlable que bajo sistemas Windows? ¿Por qué?

ACTIVIDADES

Un nivel de seguridad en los sistemas Windows se proporciona con la opción de encriptación que cada usuario puede hacer sobre determinados archivos. Busca información y contesta a las siguientes cuestiones:

- ¿De qué color aparece el texto de los archivos encriptados?
- ¿Qué usuario tiene acceso a ese archivo?¿Cómo se controla dicho hecho?
- ¿Cada usuario puede acceder a todo el sistema de archivos o tiene ciertas restricciones?
- ¿Pueden emplearlos otros usuarios?
- Si pongo contraseña a una cuenta de usuario ¿es posible conectar el disco duro a otra torre, arrancar con otro sistema Windows y leer los archivos?. Pruébalo y comenta el resultado.

3.2.5 UBICACIÓN Y HORARIO

El acceso a determinados recursos del sistema puede estar basado en la ubicación física o lógica de los datos o personas.

En cuanto a los horarios, este tipo de controles permite limitar el acceso de los usuarios a determinadas horas de día o a determinados días de la semana.

De esta forma se mantiene un control más restringido de los usuarios y zonas de ingreso.

Se debe mencionar que estos dos tipos de controles siempre deben ir acompañados de alguno de los controles anteriormente mencionados.

3.2.6 ADMINISTRACIÓN

Una vez establecidos los controles de acceso sobre los sistemas y la aplicación, es necesario realizar una eficiente administración de estas medidas de seguridad lógica, lo que involucra la implementación, seguimientos, pruebas y modificaciones sobre los accesos de los usuarios de los sistemas.

La política de seguridad que se desarrolle respecto a la seguridad lógica debe guiar a las decisiones referidas a la determinación de los controles de accesos especificando las consideraciones necesarias para el establecimiento de perfiles de usuarios.

La definición de los permisos de acceso requiere determinar cuál será el nivel de seguridad necesario sobre los datos, por lo que es imprescindible clasificar la información, determinando el riesgo que produciría una eventual exposición de la misma a usuarios no autorizados.

Así los diversos niveles de la información requerirán diferentes medidas y niveles de seguridad.

Para empezar la implementación, es conveniente comenzar definiendo las medidas de seguridad sobre la **información más sensible o las aplicaciones más críticas**, y avanzar de acuerdo a un orden de prioridad descendiente, establecido alrededor de las aplicaciones.

Una vez clasificados los datos, deberán establecerse las medidas de seguridad para cada uno de los niveles.

Un programa específico para la administración de los usuarios informáticos desarrollado sobre la base de las consideraciones expuestas, puede constituir un compromiso vacío, si no existe una conciencia de la seguridad organizacional por parte de todos los empleados. Esta conciencia de la seguridad puede alcanzarse mediante el ejemplo del personal directivo en el cumplimiento de las políticas y el establecimiento de compromisos firmados por el personal, donde se especifique la responsabilidad de cada uno.

Pero además de este compromiso debe existir una concienciación por parte de la administración hacia el personal en donde se remarque la importancia de la información y las consecuencias posibles de su pérdida o apropiación de la misma por agentes extraños a la organización.

3.2.7 ADMINISTRACIÓN DEL PERSONAL Y USUARIOS - ORGANIZACIÓN DEL PERSONAL

Este proceso lleva generalmente cuatro pasos:

1 Definición de puestos: debe contemplarse la máxima separación de funciones posibles y el otorgamiento del mínimo permiso de acceso requerido por cada puesto para la ejecución de las tareas asignadas.

2 Determinación de la sensibilidad del puesto: para esto es necesario determinar si la función requiere permisos arriesgados que le permitan alterar procesos, perpetrar fraudes o visualizar información confidencial.

3 Elección de la persona para cada puesto: requiere considerar los requerimientos de experiencia y conocimientos técnicos necesarios para cada puesto. Asimismo, para los puestos definidos como críticos puede requerirse una verificación de los antecedentes personales.

4 Entrenamiento inicial y continuo del empleado: cuando la persona seleccionada ingresa a la organización, además de sus responsabilidades individuales para la ejecución de las tares que se asignen, deben comunicárseles las políticas organizacionales, haciendo hincapié en la política de seguridad. El individuo debe conocer las disposiciones organizacionales, su responsabilidad en cuanto a la seguridad informática y lo que se espera de él.

Esta formación debe orientarse a incrementar la **conciencia** de la necesidad de proteger los recursos informáticos y a entrenar a los usuarios en la utilización de los sistemas y equipos para que ellos puedan llevar a cabo sus funciones en forma segura, minimizando la ocurrencia de errores (principal riesgo relativo a la tecnología informática).

Sólo cuando los usuarios están capacitados y tienen una conciencia formada respecto de la seguridad pueden asumir su responsabilidad individual. Para esto, el ejemplo de la gerencia constituye la base fundamental para que el entrenamiento sea efectivo: el personal debe sentir que la seguridad es un elemento prioritario dentro de la organización.

ACTIVIDADES

- Analiza el siguiente artículo y explica cuáles son las ventajas e inconvenientes de las cuentas de tipo, perfil o rol administrador y limitadas, indicando las limitaciones de uso de éstas, y crea una cuenta de usuario limitada para acceder a tu sistema. Encripta una carpeta y todos sus archivos, con las propiedades del botón derecho, desde un usuario con rol administrador e intenta acceder desde el usuario con rol limitado.
- ¿Puede el usuario con rol limitado acceder a la carpeta de usuario Mis documentos del usuario con rol administrador y abrir sus archivos?, ¿y viceversa?

- Después de leer el artículo, ¿crees que es útil tener un sistema que tenga dos cuentas de usuario, una como administrador y otra como limitada? Indica el uso que realizarías del sistema con cada rol.

Debido al uso más extendido de los sistemas informáticos basados en el sistema Windows de Microsoft, éstos constituyen un objetivo de ataque más prioritario para los ciberdelincuentes a la hora de extender *malware*.

En la Tabla 1 se puede ver el nivel de uso de los diferentes sistemas operativos así como el nivel de infección de cada uno de ellos. Dentro de los basados en el sistema Windows, el análisis muestra un 70,5% de penetración y un 66,4% de equipos infectados por parte de Windows XP, convirtiéndolo en el SO más extendido a la vez que el más compatible con el *malware* actual.

Tabla 1: Tasa de utilización de cada sistema operativo e infecciones por sistema operativo en septiembre de 2009 (%)

Sistema Operativo	Uso (sep'09)	Equipos infectados (sep'09)
Microsoft Windows XP	70,5	66,4
Microsoft Windows Vista	25,7	31,6
Otros Microsoft Windows	1,8	70,7
Mac	1,3	0,0
Linux	0,7	0,0

Fuente: INTECO

Ahora bien, ¿cuál es la diferencia entre Windows Vista y Windows XP que motiva el desnivel tan notable en el porcentaje de equipos que alojan *malware*?

El motivo principal es que Windows Vista fuerza un control más estricto de los privilegios del usuario mediante su gestor de usuarios UAC *(User Access Control)*. Con UAC se evita que se usen los privilegios elevados si no son absolutamente necesarios.

Por esta razón, y dado que el impacto sobre la seguridad del sistema es evidente en términos de infección, a continuación se orienta al usuario a configurar Windows XP para adquirir un nivel de restricción similar al de Windows Vista. Esta restricción constituye una de las capas más efectivas contra el código malicioso y otro tipo de atacantes. Se trata de una recomendación general de seguridad que es conveniente seguir: *Realizar los cambios necesarios en el sistema para conseguir una configuración más robusta, eliminando las cuentas y los servicios innecesarios y cambiando los permisos y privilegios por defecto.*

Microsoft Windows XP es un sistema multiperfil (aunque no siempre es usado como tal). Cada perfil se corresponde con un usuario, que tiene ciertas capacidades sobre el sistema operativo.

Cuantos más privilegios tiene un usuario sobre el sistema, más riesgo existe en la realización de tareas bajo ese perfil, ya que cualquier acción que realice pone en peligro las partes más delicadas de la configuración de Windows.

Tabla 2: Tareas permitidas con cada tipo de cuenta de usuario

Cuenta Administrador	Cuenta Limitada
Instalación del sistema y del hardware y software inicial.	Crear, modificar o eliminar archivos de la propia cuenta.
Parametrización de preferencias (fecha y hora, fondo de escritorio, etc.) y reparación de problemas (modificación del registro, etc.)	Programas cotidianos de tratamiento de datos: procesadores de texto, hojas de cálculo, bases de datos, navegador, programas de descarga, lectores de correo electrónico, reproductores de video y audio, edición de fotografías, etc.
Adición de nuevo software (ej. programas de descarga) y hardware (ej. impresora).	Ver archivos de la carpeta Documentos compartidos.
Todas las tareas que permite una cuenta limitada: uso de procesadores de texto, navegador web, etc.	Guardar documentos, leer documentos del propio usuario.
Crear, modificar y eliminar cuentas.	Cambiar o quitar sus propias contraseñas
Tener acceso a todos los archivos del sistema.	Cambiar su imagen, tema y otras configuraciones de su escritorio.

Fuente: INTECO

PRINCIPIO DE MÍNIMO PRIVILEGIO

En el ámbito de la seguridad existe un principio básico que se ha de aplicar a todo proceso: el **principio de mínimo privilegio**. Se trata de una de las piedras angulares de la seguridad: realizar las tareas necesarias con los mínimos privilegios; así cualquier fallo, accidente o vulnerabilidad tiene también un impacto mínimo.

En base a este principio, es recomendable que el usuario mantenga, al menos, dos cuentas: una con privilegios de administrador (para la gestión del sistema e instalación de software) y otra cuenta con permisos reducidos (para su uso cotidiano). Todo usuario adicional que se agregue (personas que comparten el uso del mismo equipo) debe añadirse como cuenta limitada.

Las cuentas de usuario limitadas tienen como limitaciones:

- No pueden acceder a la carpeta de Mis Documentos de otros usuarios.
- No pueden escribir sobre la carpeta del sistema operativo Windows.
- Imposibilidad de instalar un *driver*.

No se puede modificar el registro de Windows, el cual alberga la configuración del sistema operativo y de algunos de los programas instalados. Para persistir en el sistema y comprometer programas, el malware ha de realizar ciertas modificaciones en el registro. Con la utilización de un usuario limitado, muchas de estas acciones están denegadas, reduciendo drásticamente el impacto del malware.

Para crear una cuenta de usuario y gestionar las cuentas existentes iremos al Panel de Control / Cuentas de usuario.

¿Cuál es el problema principal que se va a encontrar el usuario al operar con una cuenta limitada? El usuario no va a poder instalar programas que realicen cambios sobre el sistema y/o que afecten a otros usuarios (la mayoría del software de hoy día).

Adquisición puntual de privilegios de administrador: Existen opciones para adquirir puntualmente privilegios de administrador de cara a instalar un determinado programa o realizar una determinada tarea. Se detallan a continuación.

Cambio rápido de usuario: Para no tener que reiniciar el sistema ni perder el contexto en el que se está trabajando con la cuenta de usuario limitado, lo más sencillo es realizar un cambio de usuario. Para ello es suficiente con seleccionar la opción "Cerrar sesión de (nombre de usuario)" del menú desplegable "Inicio". Así en "Cambiar de usuario" se accede a la opción de cambio a la cuenta de administrador. Para volver a la cuenta limitada se sigue el mismo proceso.

Instalar aplicación "Ejecutar como" administrador: Para instalar un programa desde una cuenta limitada se puede seleccionar el ejecutable, y pulsar el botón secundario del ratón. Entre las opciones disponibles, se visualiza una nueva denominada "Ejecutar como", que permite ejecutar un programa como un usuario distinto al de la cuenta que se está utilizando.

Se selecciona ejecutar como "El siguiente usuario", se introducen los datos de la cuenta de administrador, y el programa es instalado como si lo estuviera haciendo el administrador.

Ejecución desde la consola del sistema: La última opción (quizá la más compleja) consiste en ejecutar la aplicación deseada desde la consola con los privilegios del usuario administrador. Para ello se utiliza la herramienta del sistema operativo RunAs.exe (como el comando *su* en Linux).

Se ha de abrir el símbolo del sistema (Inicio > Programas > Accesorios > Símbolo del Sistema) y allí se teclea lo siguiente:

runas /user:*nombre_de_usuario_administrador "ruta_completa_a_fichero"*

RunAs.exe solicita la contraseña del usuario administrador para poder llevar a cabo la aplicación deseada.

- Por cierto, ¿crees que si proteges tus cuentas de Windows con contraseñas son irreductibles y no puedes acceder a ellas? Busca información de cómo resetear los parámetros de las cuentas de usuario y explica el proceso.

ACTIVIDADES

CONFIGURAR DIRECTIVAS DE SEGURIDAD DE USUARIOS:

En la siguiente actividad vamos a configurar algunos aspectos básicos de seguridad local y asignación de permisos a usuarios en sistemas Windows.

Para modificar la configuración de seguridad local:

Abre Configuración de seguridad local. Haz clic en Inicio, selecciona Configuración, haz clic en Panel de control, haz doble clic en Herramientas administrativas y, a continuación, haz doble clic en Directiva de seguridad local.

Realiza una de estas acciones:

- Para modificar Directiva de contraseñas o Directiva de bloqueo de cuentas, en el árbol de la consola haz clic en Directivas de cuenta. Veremos una actividad en el siguiente apartado de control de contraseñas de acceso al sistema.
- Para modificar Directiva de auditoría, Asignación de derechos de usuario u Opciones de seguridad, en el árbol de la consola haz clic en Directivas locales.

En el árbol de la consola, haz clic en la carpeta que contiene la directiva que deseas modificar y, a continuación, en el panel de detalles, haz doble clic en la directiva que deseas modificar.

Realiza los cambios que desees y haz clic en Aceptar.

Para cambiar otras directivas, repite los tres pasos anteriores.

Para el caso de **Directivas locales**, estas directivas se aplican a un equipo y contienen tres subconjuntos:

- **Directiva de auditoría**. Determina si los sucesos de seguridad se registran en el registro de seguridad del equipo. También especifica si se registran los intentos de inicio de sesión correctos, los fallidos o ambos. El registro de seguridad forma parte del Visor de sucesos.
- **Asignación de derechos de usuario**. Determina qué usuarios o grupos tienen derechos de inicio de sesión o privilegios en el equipo.
  - Ajustar cuotas de memoria para un proceso.
  - Permitir el inicio de sesión local.
  - Hacer copias de seguridad de archivos y directorios.
  - Cambiar la hora del sistema.
  - Crear objetos compartidos permanentes.
  - Depurar programas.
  - Denegar el acceso desde la red a este equipo.
  - Denegar el inicio de sesión localmente.
  - Generar auditorías de seguridad.
  - Cargar y descargar controladores de dispositivo.
  - Restaurar archivos y directorios.
  - Apagar el sistema.
  - Tomar posesión de archivos y otros objetos.
- **Opciones de seguridad**. Habilita o deshabilita la configuración de seguridad del equipo, como la firma digital de datos, nombres de las cuentas Administrador e Invitado, acceso a CD-ROM y unidades de disco, instalación de controladores y solicitudes de inicio de sesión.

Por ejemplo, desde el usuario con rol administrador, agregar la posibilidad a la cuenta limitada creada anteriormente de cambiar la fecha/hora, revocarle el privilegio de acceso al CD-ROM, que pueda instalar controladores de dispositivo. Activar el archivo de sucesos o log de sucesos asociados a esos privilegios.

Acceder como usuario rol-limitado y verificar privilegios y limitaciones.

Acceder como usuario rol-administrador y verificar el archivo de suceso o log.

¿Los usuarios con cuenta limitada pueden acceder a la configuración de directivas locales?¿Es lógico?

Advertencia: La modificación de las directivas locales debe hacerse con conocimiento de causa, control y precaución, ya que puede ocasionar resultados indeseados.

3.3 IDENTIFICACIÓN

Las contraseñas son las claves que se utilizan para obtener acceso a información personal que se ha almacenado en el equipo y en sus cuentas en línea.

Si algún delincuente o un usuario malintencionado consigue apoderarse de esa información, podría utilizar su nombre, por ejemplo, para abrir nuevas cuentas de tarjetas de crédito, solicitar una hipoteca o suplantarle en transacciones en línea. En muchos casos, podría ocurrir que no se dé cuenta del ataque hasta que ya es demasiado tarde.

Por suerte, no es difícil crear contraseñas seguras y mantenerlas bien protegidas.

3.3.1 ¿QUÉ HACE QUE UNA CONTRASEÑA SEA SEGURA?

Para un atacante, una contraseña segura debe parecerse a una cadena aleatoria de caracteres. Puede conseguir que su contraseña sea segura si se guía por los siguientes criterios:

- **Que no sea corta.** Cada carácter que agrega a su contraseña aumenta exponencialmente el grado de protección que ésta ofrece. Las contraseñas deben contener un mínimo de 8 caracteres; lo ideal es que tenga 14 caracteres o más.

  Muchos sistemas también admiten el uso de la barra espaciadora para las contraseñas, de modo que pueden crearse frases compuestas de varias palabras (una frase codificada). Por lo general, una frase codificada resulta más fácil de recordar que una contraseña simple, además de ser más larga y más difícil de adivinar.

- **Combina letras, números y símbolos.** Cuanto más diversos sean los tipos de caracteres de la contraseña, más difícil será adivinarla. Entre otros detalles importantes cabe citar los siguientes:

  - **Cuantos menos tipos de caracteres haya en la contraseña, más larga deberá ser ésta**. Una contraseña de 15 caracteres formada únicamente por letras y números aleatorios es unas 33.000

veces más segura que una contraseña de 8 caracteres compuesta de caracteres de todo tipo. Si la contraseña no puede contener símbolos, deberá ser considerablemente más larga para conseguir el mismo grado de protección. Una contraseña ideal combinaría una mayor longitud y distintos tipos de símbolos.

- **Utiliza todo tipo de teclas**, no te limites a los caracteres más comunes. Los símbolos que necesitan que se presione la tecla "Mayús" junto con un número son muy habituales en las contraseñas. Tu contraseña será mucho más segura si eliges entre todos los símbolos del teclado, incluidos los de puntuación que no aparecen en la fila superior del teclado, así como los símbolos exclusivos de tu idioma.

- **Utiliza palabras y frases que te resulten fáciles de recordar, pero que a otras personas les sea difícil adivinar**. La manera más sencilla de recordar tus contraseñas y frases codificadas consiste en anotarlas. Al contrario que lo que se cree habitualmente, no hay nada malo en anotar las contraseñas, si bien estas anotaciones deben estar debidamente protegidas para que resulten seguras y eficaces.

Por lo general, las contraseñas escritas en un trozo de papel suponen un riesgo menor en Internet que un administrador de contraseñas, un sitio web u otra herramienta de almacenamiento basada en software.

3.3.2 ESTRATEGIAS QUE DEBEN EVITARSE CON RESPECTO A LAS CONTRASEÑAS

Algunos métodos que suelen emplearse para crear contraseñas resultan fáciles de adivinar para un delincuente. A fin de evitar contraseñas poco seguras, fáciles de averiguar:

- **No incluyas secuencias ni caracteres repetidos.** Cadenas como "12345678", "222222", "abcdefg" o el uso de letras adyacentes en el teclado no ayudan a crear contraseñas seguras.

- **Evita utilizar únicamente sustituciones de letras por números o símbolos similares.** Los delincuentes y otros usuarios malintencionados que tienen experiencia en descifrar contraseñas no se dejarán engañar fácilmente por reemplazos de letras por números o símbolos parecidos; por ejemplo, i por 1 o a por @, como en "M1cr0$0ft" o en "C0ntr@señ@". Pero estas sustituciones pueden ser eficaces cuando se combinan con

otras medidas, como una mayor longitud, errores ortográficos voluntarios o variaciones entre mayúsculas y minúsculas, que permiten aumentar la seguridad de las contraseñas.

- **No utilices el nombre de inicio de sesión.** Cualquier parte del nombre, fecha de nacimiento, número de la seguridad social o datos similares propios o de tus familiares constituye una mala elección para definir una contraseña. Son algunas de las primeras claves que probarán los delincuentes.

- **No utilices palabras de diccionario de ningún idioma.** Los delincuentes emplean herramientas complejas capaces de descifrar rápidamente contraseñas basadas en palabras de distintos diccionarios, que también abarcan palabras inversas, errores ortográficos comunes y sustituciones. Esto incluye todo tipo de blasfemias y cualquier palabra que no diría en presencia de sus hijos.

- **Utiliza varias contraseñas para distintos entornos.** Si alguno de los equipos o sistemas en línea que utilizan esta contraseña queda expuesto, toda la información protegida por esa contraseña también deberá considerarse en peligro. Es muy importante utilizar contraseñas diferentes para distintos sistemas.

- **Evita utilizar sistemas de almacenamiento en línea.** Si algún usuario malintencionado encuentra estas contraseñas almacenadas en línea o en un equipo conectado a una red, tendrá acceso a toda su información.

- **Opción de "contraseña en blanco".** Una contraseña en blanco (ausencia de contraseña) en su cuenta es más segura que una contraseña poco segura, como "1234". Los delincuentes pueden adivinar fácilmente una contraseña simple, pero en equipos que utilizan Windows XP no es posible el acceso remoto a una cuenta a través de una red o de Internet, por ejemplo. (Esta opción no está disponible para Microsoft Windows 2000, Windows Me o versiones anteriores).

Puedes optar por usar una contraseña en blanco en la cuenta del equipo si se cumplen estos criterios:

- ✓ Tienes sólo un equipo, o bien tienes varios equipos pero no necesitas obtener acceso a la información de un equipo desde los otros.

- ✓ El equipo es físicamente seguro (confías en todas las personas que tienen acceso físico al equipo).

No siempre es buena idea utilizar una contraseña en blanco. Por ejemplo, es probable que un equipo portátil que lleves contigo no sea físicamente seguro, por lo que en ese caso debes utilizar una contraseña segura.

Cuida tus contraseñas y frases codificadas tanto como de la información que protegen.

- ✓ **No las reveles a nadie.**
- ✓ **Proteje las contraseñas registradas.**
- ✓ **No facilites nunca tu contraseña por correo electrónico ni porque se te pida por ese medio.**
- ✓ **Cambia tus contraseñas con regularidad.**
- ✓ **No escribas contraseñas en equipos que no controlas.**

ACTIVIDADES

CREA UNA CONTRASEÑA SEGURA Y FÁCIL DE RECORDAR EN SEIS PASOS

Sigue estos pasos para crear una contraseña segura:

1. **Piensa en una frase que puedas recordar.** Ésta será la base de tu contraseña segura o frase codificada. Piensa en una frase que puedas memorizar sin problemas, como "Mi hermano Ángel tiene tres años".
2. **Comprueba si el equipo o el sistema en línea admite directamente la frase codificada.** Si puede utilizar una frase codificada (con espacios entre caracteres) en el equipo o en el sistema en línea, hazlo.
3. **Si el equipo o el sistema en línea no admite frases codificadas, conviértelas en contraseñas.** Utiliza la primera letra de cada palabra de la frase que has creado para definir una palabra nueva sin sentido. Si tomamos la frase del ejemplo anterior, tendríamos: "mhátta".
4. **Aumenta la complejidad** combinando mayúsculas, minúsculas y números. También resulta de utilidad cambiar letras o cometer

errores ortográficos voluntariamente. Por ejemplo, en la frase anterior, considera la posibilidad de escribir incorrectamente el nombre Ángel o sustituya la palabra tres por el número 3. Hay muchas posibles sustituciones y, cuanto más larga sea la frase, más compleja será la contraseña. La frase codificada podría convertirse finalmente en "Mi Hermano Áng3l tiene 3 añiOs". Si el equipo o el sistema en línea no admite frases codificadas, utiliza la misma técnica para la contraseña abreviada. El resultado podría ser una contraseña como "MhÁt3a".

5. **Por último, realiza sustituciones con algunos caracteres especiales.** Puedes utilizar símbolos que parezcan letras, combinar palabras (quitar espacios) y recurrir a otros medios que permitan crear contraseñas más complejas. Mediante estos trucos, podemos crear una frase codificada como "MiH3rmanO @ng3l ti3n3 3 añiO$" o una contraseña abreviada (con las primeras letras de cada palabra) como "MiH3@t3a".

6. **Prueba la contraseña con un comprobador de contraseñas.** El comprobador de contraseñas te ayudará a determinar el nivel de seguridad que ofrece una contraseña a medida que la escribes (esos datos no se registran).

   Comprobador de contraseñas de Microsoft. ¿Has conseguido una contraseña segura?

   https://www.microsoft.com/latam/protect/yourself/password/checker.mspx

   ¿Por qué crees que es una web https?

ACTIVIDADES

Configura directivas de seguridad de usuarios, sobre contraseñas y bloqueos de cuenta:

En la siguiente actividad vamos a configurar algunos aspectos básicos de seguridad y asignación de permisos a usuarios.

Cómo configurar las directivas de cuentas en Windows XP.

Las directivas de cuentas nos permiten configurar el comportamiento que van a tener éstas ante una serie de sucesos. La importancia de una correcta configuración de estas directivas radica en que desde ellas vamos a poder controlar de una forma más eficiente la forma de acceder a nuestro ordenador.

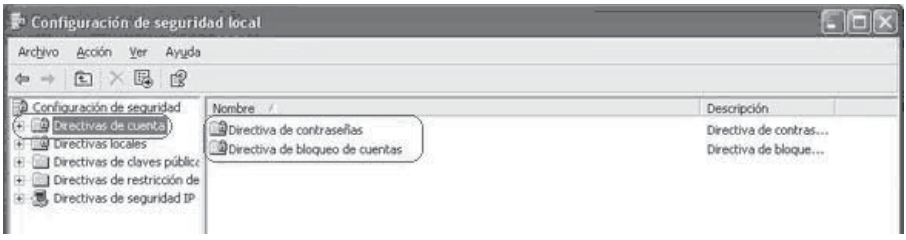
Vamos a ver cómo podemos configurar estas directivas en Windows XP Professional SP2.

Ante todo, estamos ante unas configuraciones **administrativas**. Esto quiere decir dos cosas. En primer lugar, que sólo los administradores de equipos pueden acceder a ellas, y en segundo lugar, que cuando toquemos algún parámetro dentro de este apartado debemos estar **muy seguros** de lo que estamos haciendo. No se trata de una parte de configuración con la que se puedan hacer experimentos, ya que podemos dejar inaccesible nuestro sistema operativo.

Dicho esto, vamos a ver en primer lugar cómo accedemos a la ventana de **Directivas de seguridad de cuentas**.

En primer lugar entramos en el **Panel de control** (es conveniente activarlo en modo *Vista clásica*).

Una vez que entramos en **Herramientas administrativas**, tenemos el apartado **Directivas de seguridad local**.



Una vez en la ventana de las **Directivas de seguridad local** nos encontramos a la izquierda con varias directivas. Estas son:

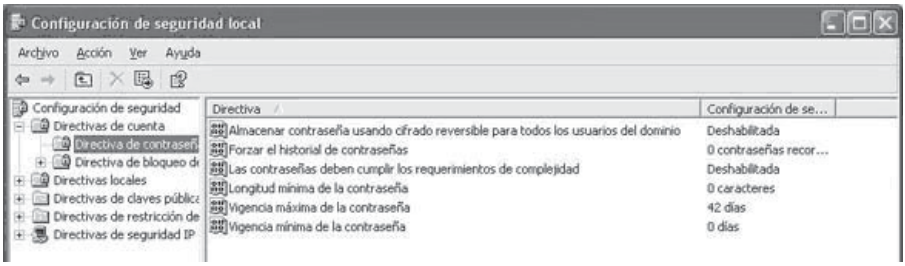
Directivas de cuentas:

- Directivas locales.
- Directivas de claves públicas.
- Directivas de restricción de software.
- Directivas de seguridad IP en equipo local.

Vamos a tratar la primera de ellas, que son las **Directivas de cuentas**.

Como podemos ver, en este grupo de directivas tenemos dos subgrupos, **Directiva de contraseñas** y **Directiva de bloqueo de cuentas**. Vamos a ver qué podemos hacer en cada uno de ellos:

Directiva de contraseñas:



Dentro de las directivas de contraseña nos encontramos con una serie de directivas, que vamos a estudiar a continuación. Bien, veamos cuáles son estas directivas:

- **Almacenar contraseña usando cifrado reversible para todos los usuarios del dominio.** Su mismo nombre indica para qué se utiliza. Las opciones son **Habilitado** o **Deshabilitado**.
- **Forzar el historial de contraseñas.** Establece el número de contraseñas a recordar.
- **Las contraseñas deben cumplir los requerimientos de complejidad.** Obliga a que las contraseñas cumplan unos requisitos de complejidad.
- **Longitud mínima de la contraseña.** Obliga a que las contraseñas tengan un mínimo de caracteres, estableciendo este mínimo.
- **Vigencia máxima de la contraseña.** Establece el número de días máximo que una contraseña va a estar activa.
- **Vigencia mínima de la contraseña.** Establece el número de días mínimos que una contraseña va a estar activa.

Directiva de bloqueo de cuentas:

- **Duración del bloqueo de cuentas.** Establece, en minutos, el tiempo que una cuenta debe permanecer bloqueada.
- **Restablecer la cuenta de bloqueos después de.** Establece, en minutos, el tiempo que ha de pasar para restablecer la cuenta de bloqueos.
- **Umbral de bloqueos de la cuenta.** Establece el número de intentos fallidos para bloquear el acceso a una cuenta.

Como podemos ver es un apartado que, si bien no tiene grandes complicaciones en su configuración, sí que hay que saber lo que se está haciendo y, sobre todo, los resultados que se quieren obtener.

- Configurar la política de contraseñas para que la longitud mínima sea de 14 caracteres, tenga las características de complejidad requeridas y haya que modificarlas cada mes.
- En caso de más de 3 intentos fallidos bloquear la cuenta 15 minutos.
- Comprobar la nueva política de contraseñas creada y documentar los resultados y limitaciones que aparezcan.

ACTIVIDADES

- Leer el artículo sobre Recomendaciones para la creación y uso de contraseñas seguras de Inteco. En la siguiente página web http://www.inteco.es/Seguridad/Observatorio/Estudios_e_Informes/Notas_y_Articulos/recomendaciones_creacion_uso_contrasenas
- Contesta a las siguientes cuestiones:
  - **a.** ¿Qué es un ataque de fuerza bruta? ¿Y uno de diccionario?
  - **b.** ¿Qué porcentaje de usuarios emplea contraseñas para el acceso a sus sistemas de archivos?
  - **c.** ¿Qué porcentaje de usuarios en EEUU apunta su contraseña en papel o archivo electrónico en el PC?
  - **d.** ¿Qué porcentaje de usuarios emplea la misma contraseña en distintos servicios?
  - **e.** ¿Qué es un keylogger? Instala un keylogger gratuito en tu PC y verifica el registro que realiza cuando accedes a tu correo electrónico?

ACTIVIDADES

- Busca información acerca de los archivos etc/passwd, etc/groups y etc/shadow de los sistemas GNU/Linux responsables de la administración de usuario y grupos, así como contraseñas. Indica qué encriptación posee el archivo etc/shadow. Si encontraras una máquina con usuario logado root, y visualizaras el contenido del archivo mediante el comando cat etc/shadow:

```
root:HZ5xf2h5BJ8$u:0:0:root:/root:/bin/bash
bin:*:1:1:bin:/bin:
daemon:*:2:2:daemon:/sbin:
adm:*:4:7:lp:/var/spool/lpd:
sync:*:5:0:sync:/sbin: /bin/sync
shutdown:*:6:0:shutdown:/sbin:/sbin/shutdown
halt:*:7:0:halt:sbin:/sbin/halt
mail:*:8:12:mail:/var/spool/mail:
news:*:9:13:news:/var/spool/news:
uucp:*:10:14:uucp:/var/spool/uucp:
operator:*:11:0:operator:/root:
games:*:12:100:games:/usr/games:
gopher:*:13:30:gopher:/usr/lib/gopher-data:
ftp:*:14:50:FTP User:/home/ftp:
guest::405:100:Guest:/home/guest:/bin/bash
nobody:*:99:99:Nobody:/:
jose:Rf$rt96yy$OIJ:0:0:Jose Garcia:/home/jose:/bin/ksh
maria:kd6$fak8754Hu:407:100::/home/maria:/bin/bash
```

- ¿Qué contraseña poseen los usuarios: root, jose y maria? ¿Qué privilegios tiene el usuario root?
- Descarga el software John The Ripper, investiga sobre su uso y encuentra la respuesta.

3.4 ACTUALIZACIÓN DE SISTEMAS Y APLICACIONES

¿Por qué debemos actualizar regularmente nuestro sistema y aplicaciones?

Mientras hacemos uso de Internet y sus servicios, los ciberdelincuentes, de forma análoga a como haría un ladrón al intentar entrar a robar a una casa, desarrollan virus y otros programas maliciosos para aprovechar cualquier vulnerabilidad en el sistema a través del cual infectarlo. Suelen aprovechar las vulnerabilidades más recientes que requieren una actualización inmediata de los sistemas.

Los fabricantes de software, conocedores de que los atacantes andan al acecho, actualizan sus programas cada vez que se descubre un agujero de seguridad.

Es de vital importancia **actualizar los sistemas**, **tanto el sistema operativo como el resto de aplicaciones, tan pronto como sea posible.**

Hay que tener en cuenta que cuanto más tiempo tardemos en hacerlo más tiempo estaremos expuestos a que un virus pueda entrar en el equipo, y el ordenador quede bajo el control del atacante.

Para facilitar esta tarea, la mayoría de **aplicaciones** tienen la opción de que las **actualizaciones se realicen automáticamente**, lo que permite tener los programas actualizados sin la necesidad de comprobar manual y periódicamente si la versión utilizada es la última disponible, y por tanto la más segura.

Recomendamos activar las actualizaciones automáticas, sobre todo de las aplicaciones más utilizadas y más expuestas a un ataque, sistema operativo, navegadores, programas de ofimática, reproductores multimedia, etc.

3.4.1 ACTUALIZACIONES AUTOMÁTICAS

¿Qué hacen y cómo se realizan las actualizaciones automáticas?

Estas actualizaciones de software vienen justificadas por diferentes motivos:

- ✓ Reparar las vulnerabilidades detectadas.
- ✓ Proporcionar nuevas funcionalidades o mejoras respecto a las versiones anteriores.
- ✓ El proceso de actualización consiste básicamente en descargar de la página web del fabricante del programa los ficheros necesarios.

Aunque es posible hacer la actualización de forma manual, lo más sencillo es hacerlo de forma automática. De esta forma el propio sistema busca las actualizaciones, las descarga e instala sin que nosotros tengamos que intervenir en el proceso.

A continuación se detalla cómo activar las actualizaciones automáticas, también puedes utilizar esta información para verificar si ya tienes activas las actualizaciones automáticas, para las aplicaciones más críticas.

Actualización automática del sistema operativo, en función del fabricante tenemos:

Sistemas Microsoft

Microsoft, publica actualizaciones los segundos martes de cada mes, salvo casos en los que el problema sea crítico y requiera de una actualización más inminente. En la página de Microsoft, tenemos explicado cómo realizar este proceso.

ACTIVIDADES

Comprueba el estado de tu sistema operativo con respecto a actualizaciones.

Las actualizaciones de sistema operativo contienen software nuevo que permite mantener actualizado el equipo.

Estos son algunos ejemplos de actualizaciones: *service packs*, actualizaciones de versión, actualizaciones de seguridad y controladores (*drivers*).

Las actualizaciones importantes y de alta prioridad son críticas para la seguridad y la confiabilidad del equipo. Ofrecen la protección más reciente contra las actividades malintencionadas en línea.

Debes actualizar todos los programas, incluidos Windows, Internet Explorer, Microsoft Office, etc.

Visita Microsoft Update, http://update.microsoft.com, con un navegador Internet Explorer para examinar tu equipo y ver una lista de actualizaciones, que podrás decidir si deseas o no descargar e instalar.

Es importante instalar las nuevas actualizaciones de seguridad en cuanto se encuentran disponibles, y los service pack o paquetes de seguridad con un conjunto de actualizaciones verificadas.

La forma más fácil de realizar esto consiste en activar actualizaciones automáticas y utilizar la configuración proporcionada, que descarga e instala las actualizaciones recomendadas según su conveniencia.

En Windows Vista, puedes controlar la configuración de las actualizaciones automáticas mediante el Panel de control de Windows Update. Para obtener más información, consulta Activar o desactivar las actualizaciones automáticas.

En el caso, por ejemplo, de disponer de Windows XP, se recomienda tener instalado el Service Pack 2 (SP2). Para actualizar el sistema operativo, la mejor forma de actualizarlo es controlando las actualizaciones automáticas. Las actualizaciones automáticas permiten descargar e instalar actualizaciones importantes para la seguridad y de alta prioridad automáticamente en función de la programación que establezca.

Para ver el estado de las actualizaciones automáticas en Windows XP (SP2):

1. Haz clic en Inicio y, a continuación, en Panel de control.
2. Haz clic en Centro de seguridad y, a continuación, en Actualizaciones automáticas.
3. Podrás seleccionar:
   - Automáticas, descarga e instala actualizaciones automáticamente.
   - Descargar actualizaciones y notificar si deseas instalarlas.
   - Notificar, pero no descargar ni instalar, máximo control por parte del usuario.
   - Desactivar actualizaciones automáticas, no recomendable.

Para usuarios más experimentados se debe seleccionar Notificar.

Indica en qué estado de actualización se encuentra tu sistema y qué modo de actualización tiene configurado. Explica sus ventajas e inconvenientes.

Advertencia: Algunos programas, como programas antivirus o de supervisión de spyware, proporcionan un vínculo para buscar actualizaciones desde el programa. Algunos editores de software también ofrecen servicios de suscripción y pueden enviarle una notificación cuando haya nuevas actualizaciones disponibles. Es recomendable buscar actualizaciones para los programas relativos a la seguridad primero y, después, para los programas o los dispositivos que más uses.

Sistemas Apple

A partir de la versión Mac OS X v10.4, podemos configurar las actualizaciones para que se realicen de forma automática diariamente, es lo más recomendable, semanal o mensualmente.

En las versiones anteriores del sistema operativo, estas actualizaciones automáticas no aparecen, hemos de forzar la descarga de las mismas.

Distribuciones GNU/Linux basadas en Ubuntu

Por defecto, Ubuntu **avisa de la disponibilidad de nuevas actualizaciones**, y es necesario que el usuario inicie la acción de actualizar. También **se pueden configurar para que se actualicen de forma automática.**

Se puede actualizar Ubuntu a través del "Gestor de Actualizaciones" (update-manager), para acceder a él ve a "Menú -> Sistema -> Administración".

Por defecto, Ubuntu tiene activadas las actualizaciones automáticas, si deseas comprobar si tienes activada esta opción o modificar sus parámetros, sigue estos pasos:

- ✓ Ve a "Menú -> Sistema -> Administración".
- ✓ Pulsa en la opción de "Orígenes del software " (software-properties-gtk).
- ✓ O bien, a través de una consola teclea: gksudo "software-properties-gtk".

Una vez se accede a "Orígenes del software", seleccionando la pestaña de "Actualizaciones", se puede comprobar con qué frecuencia tiene configuradas las actualizaciones automáticas y, si lo deseas, modificarla.

Es importante que, a parte de tener el sistema operativo y sus productos actualizados, también actualices la distribución de Ubuntu que utilizas, cuando salga una nueva, la forma más rápida de hacerlo es tecleando en una consola el comando:

```
gksudo "update-manager -c"
```

3.4.2 ACTUALIZACIÓN AUTOMÁTICA DEL NAVEGADOR WEB

El navegador, al ser el programa que utilizamos para visitar las páginas web, es de uno de los más expuestos a posibles amenazas. Los más comunes son Internet Explorer, Mozilla Firefox y Safari.

Internet Explorer

En Windows, el navegador se actualiza a través del mismo mecanismo del sistema operativo, esto es, activando las actualizaciones automáticas.

Cuando la actualización es de una nueva versión del navegador, como el paso de Internet Explorer 6 a Internet Explorer 7, necesitaremos confirmar el proceso. Recomendamos aceptarlo ya que la última versión es más robusta.

Mozilla Firefox

Se actualiza de forma automática por defecto. Cuando abrimos el programa, busca actualizaciones, no sólo del navegador, sino de todos los accesorios, complementos o plugins, que tengamos instalados. Lo descarga y nos pide permiso para reiniciarlo.

Safari

Se actualiza de forma automática por defecto. Cuando lo ejecutamos, busca las actualizaciones, si las encuentra nos muestra una ventana con información acerca de la actualización, y con las indicaciones para instalarla.

La otra forma de actualizarlo, forzarlo a buscar la actualización, se haría del mismo modo que al actualizar el software del sistema operativo. A través de este enlace se explica cómo actualizar el software.

3.4.3 ACTUALIZACIÓN DEL RESTO DE APLICACIONES

Aunque se han explicado las aplicaciones más expuestas a las amenazas, no nos debemos olvidar del resto. Aunque cada una de las aplicaciones tiene su propia configuración, en Opciones o Preferencias de la mayoría de las aplicaciones existe la posibilidad de actualizar en línea. Para revisar la versión y estado de actualización, solemos encontrar la opción en los menús de Ayuda.

Volviendo a la analogía del ladrón de casas, para protegernos del robo, la puerta de entrada y ventanas que dan a la calle, sistema operativo y navegador web, deben estar bien cerradas. Pero no por ello hay que descuidar otros pequeños puntos de entrada, lo que serían el resto de aplicaciones.

Para comprobar el nivel de actualización del resto de programas recomendamos utilizar **Secunia Online Software Inspector**.

Este servicio gratuito de la firma danesa Secunia, que no requiere instalar nada en el ordenador, analiza las aplicaciones más comunes en el sistema para detectar las que no están correctamente actualizadas, y facilitar su puesta al día.

ACTIVIDADES

- Comprueba el estado de actualización de tus navegadores web y de aplicaciones.
- Realiza un análisis desde la web de Secunia con su inspector online:

  http://secunia.com/vulnerability_scanning/online/?lang=es
- ¿Qué aplicaciones disponían vulnerabilidades?

ACTIVIDADES

- **Analiza la siguiente noticia, y explica qué novedosa vulnerabilidad existe con las actualizaciones de software.**

- **¿Crees que el grado de automatización en las actualizaciones beneficia la despreocupación de los usuarios y por tanto los ataques?**

Por primera vez los investigadores de seguridad han localizado un tipo de software malicioso que **sobreescribe las actualizaciones para otras aplicaciones**, lo que podría suponer un riesgo a largo plazo para los usuarios.

El malware, que infecta a ordenadores de Windows, se sobreescribe como una actualización para los productos de Adobe y otros software como Java. Al menos es lo que afirma Nguyen Cong Cuong, un analista de Bach Khoa Internetwork Security (BKIS), compañía de seguridad de Vietnam, en su blog.

BKIS ha mostrado imágenes de una **variante del malware que imita Adobe Reader 9** y sobreescribe el AdobeUpdater.exe, que se encarga de comprobar si está disponible una nueva versión del software.

Los usuarios pueden instalar el software sin darse cuenta simplemente abriendo un correo electrónico malicioso o visitando páginas web que aprovechen vulneralidades de software.

Después de que esta clase de malware entre en la máquina, abre el cliente DHCP (*Dynamic Host Configuration Protocol*), un DNS (*Domain Name System*), una red compartida y un puerto para poder percibir los comandos.

3.5 REFERENCIAS WEB

- ✓ Comprueba la fortaleza y generador de claves. Password tools bund. Disponible en Sourceforge:

  http://sourceforge.net/projects/pwdstr/

- ✓ Comprueba la seguridad de tus claves. Microsoft:

  https://www.e-typedesign.co.uk/latam/protect/yourself/password/checker.mspx

- ✓ Actualización de sistemas Microsoft:

  http://update.microsoft.com

- ✓ Administración de usuarios en GNU/Linux:

  http://www.linuxtotal.com.mx/index.php?cont=info_admon_008

- ✓ Administración de usuarios en Windows:

  https://www.microsoft.com/latam/protect/yourself/password/checker.mspx

RESUMEN DEL CAPÍTULO

La seguridad lógica consiste en la *"aplicación de barreras y procedimientos que resguarden el acceso a los datos y sólo se permita acceder a ellos a las personas autorizadas para hacerlo"*.

Para ello se emplean técnicas como el control de acceso mediante contraseña desde la BIOS, al sistema operativo el cual es capaz de gestionar usuarios y sus privilegios o procedimientos autorizados, incluso las aplicaciones y archivos.

Una contraseña segura debe parecerle a un atacante una cadena aleatoria de caracteres. Debe tener 14 caracteres o más (como mínimo, ocho caracteres). Debe incluir una combinación de letras mayúsculas y minúsculas, números y símbolos, y se deben cambiar regularmente.

El principio de la seguridad lógica en cuanto a permisos debe ser *"todo lo que no está permitido debe estar prohibido"*.

Los fabricantes de software, conocedores de que los atacantes andan al acecho, actualizan sus programas cada vez que se descubre un agujero de seguridad.

Es de vital importancia **actualizar los sistemas**, **tanto el sistema operativo como el resto de aplicaciones, tan pronto como sea posible.**

Recientemente, aprovechando el proceso de actualización automático del sistema operativo y aplicaciones, han aparecido nuevos frentes de ataque, ofreciendo al usuario actualizaciones falsas que en realidad se tratan de virus o malware.

EJERCICIOS PROPUESTOS

1. A lo largo del curso se realizará un **manual de buenas prácticas y recomendaciones** a modo de resumen en dos ámbitos, calculando siempre el coste de la solución óptima, y la periodicidad de cambio o uso de las mismas:

A. A nivel de usuario, qué medidas y recomendaciones de equipamiento y uso tomarías.

B. A nivel de pequeña y mediana empresa, PYME, qué medidas y recomendaciones darías a un cliente, propietario de una PYME.

Complétalo con soluciones y recomendaciones tomadas con respecto al Capítulo 3 en base a:

- Política de usuarios: Usuarios del sistema operativo y privilegios.
- Fortaleza y seguridad de contraseñas en BIOS, acceso a sistema operativo, acceso a aplicaciones y acceso a datos.
- Actualización periódica del sistema operativo y de las aplicaciones.
- Comprobación del grado de actualización del sistema y aplicaciones.

TEST DE CONOCIMIENTOS

1 Para qué sirve el comando runas:
- **a)** Ejecuta un proceso con los permisos de un usuario que se le indican al comando.
- **b)** Permite un login de usuario y la ejecución de procesos y acceso a archivos.
- **c)** Sirve para ejecutar procesos en un segundo plano.
- **d)** Permite ver los permisos de un usuario privilegiado.

2 Una contraseña segura, no debe tener:
- **a)** Más de 10 caracteres.
- **b)** El propio nombre de usuario contenido.
- **c)** Caracteres mayúsculas, minúsculas y símbolos.
- **d)** Frases fáciles de recordar por ti.

3 ¿Qué es la identificación?
- **a)** Momento en que el usuario se da a conocer en el sistema.
- **b)** Verificación que realiza el sistema sobre el intento de login.
- **c)** Un número de intentos de login.
- **d)** Un proceso de creación de contraseñas.

4 ¿Qué es un agujero de seguridad en una aplicación?
- **a)** Un parche malware.
- **b)** Una actualización no verificada.
- **c)** Una vulnerabilidad.
- **d)** Una posible entrada con contraseña segura.

5 Para un usuario experimentado como tú, las actualizaciones deben ser:
- **a)** Automáticas, descargar e instalar actualizaciones automáticamente.
- **b)** Descargar actualizaciones y notificar si deseas instalarlas.
- **c)** Notificar, pero no descargar ni instalar.
- **d)** Desactivar actualizaciones automáticas.