Ciclo Formativo de Grado Superior de Administración de Sistemas Informáticos en red

Módulo Profesional: SAD

U.T. 2.- Conceptos Básicos. Principios de seguridad y alta disponibilidad

Departamento de Informática y Comunicación
IES San Juan Bosco (Lorca-Murcia)
Profesor: Juan Antonio López Quesada


INTRODUCCIÓN A LA
SEGURIDAD INFORMATICA
security
computer

I ES
SAN JUAN BOSCO

Índice de Contenidos

Objetivos de la Unidad de TRabajo:

- Analizar la problemática general de la seguridad informática
- Conocer los principios sobre los que se sustentan
- Conocer el significado de alta disponibilidad
- Identificar las principales vulnerabilidades, ataques y medidas de seguridad a adoptar sobre los sistemas
- Diferencias la seguridad física y lógica, y la pasiva de la activa

Abstract/Resumen:

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

Introducción a la Seguridad Informática

El espectacular auge de Internet y de los servicios telemáticos ha hecho que los ordenadores y las redes se conviertan en un elemento cotidiano en nuestras casas y en un instrumento imprescindible en las tareas de las empresas.

Ya no tenemos necesidad de ir al banco para conocer los movimientos realizados en nuestra cuenta bancaria, ni para realizar transferencias… directamente podemos realizar dichas operaciones desde el ordenador de casa. Lo mismo ocurre con las empresas (sea cual sea su tamaño), disponen de **equipos conectados a Internet** que les ayudan en sus procesos productivos.

Cualquier fallo en los mismos puede suponer una gran pérdida económica ocasionada por el parón producido, bien por la pérdida de información o por el mal funcionamiento de los equipos informáticos, de modo que es muy importante asegurar un **correcto funcionamiento de los sistemas y redes informáticas**.

Uno de los principales problemas a los que se enfrenta la seguridad informática es la creencia de muchos usuarios de que a ellos nunca les va a pasar lo que a otros. Es impensable que nos vayamos de casa y nos dejemos la puerta abierta. Lo mismo ocurre con la **seguridad de la información**.

Introducción a la Seguridad Informática

Con unas **buenas políticas de seguridad**, tanto **físicas** como **lógicas,** conseguiremos que nuestros sistemas sean menos vulnerables a las distintas amenazas. Ya que, nadie puede asegurar que su sistema sea cien por cien seguro, hasta la seguridad de la NASA y el Pentágono han sido violadas por hackers. Hay una lucha permanente entre los técnicos protectores del sistema y los que buscan rendimientos económicos fáciles, o simplemente su minuto de gloria al superar el reto de asomarse al otro lado de la barrera de protección.

Tenemos que intentar lograr un nivel de seguridad razonable y estar preparado para que, cuando se produzcan los ataques, los daños puedan ser evitados en unos porcentajes que se aproximen al ciento por cien o en caso contrario haber sido lo suficientemente precavidos para realizar las **copias de seguridad** y de esta manera volver a poner en funcionamiento los sistemas en el menor tiempo posible.

Introducción a la Seguridad Informática

La **seguridad informática** consiste en asegurar que los recursos del sistema de información de una organización sean utilizados de la manera que se decidió y que el acceso a la información allí contenida, así como su modificación, solo sea posible a las personas que se encuentren acreditadas y dentro de los límites de sus autorización

Introducción a la Seguridad Informática

Los principales objetivos de la seguridad informática por tanto son:

- Detectar los posibles problemas y amenazas a la seguridad, minimizando y gestionando los riesgos.
- Garantizar la adecuada utilización de los recursos y de las aplicaciones de los sistemas.
- Limitar las perdidas y conseguir la adecuada recuperación del sistema en caso de un incidente de seguridad.
- Cumplir con el marco legal y con los requisitos impuestos a nivel organizativo

Introducción a la Seguridad Informática

Un pequeño ejemplo de ataque contra contraseñas:

Existen en Internet multitud de programas dedicados a descubrir las contraseñas - ***craqueo de passwords*** - haciendo uso del método de fuerza bruta, que consiste en ir probando todas y cada una de las posibles contraseñas. **Brutus** o **John the Ripper** son aplicaciones clásicas capaces de descubrir contraseñas.

Brutus es un craqueador de passwords, es bastante rápido y muy fácil de manejar, los pass que puede craquear son: HTTP (Autentificación Básica), HTTP (HTML Form/CGI), POP3, Ftp, SMB, Telnet, otros tipos tales como IMAP, NNTP, NetBus etc .

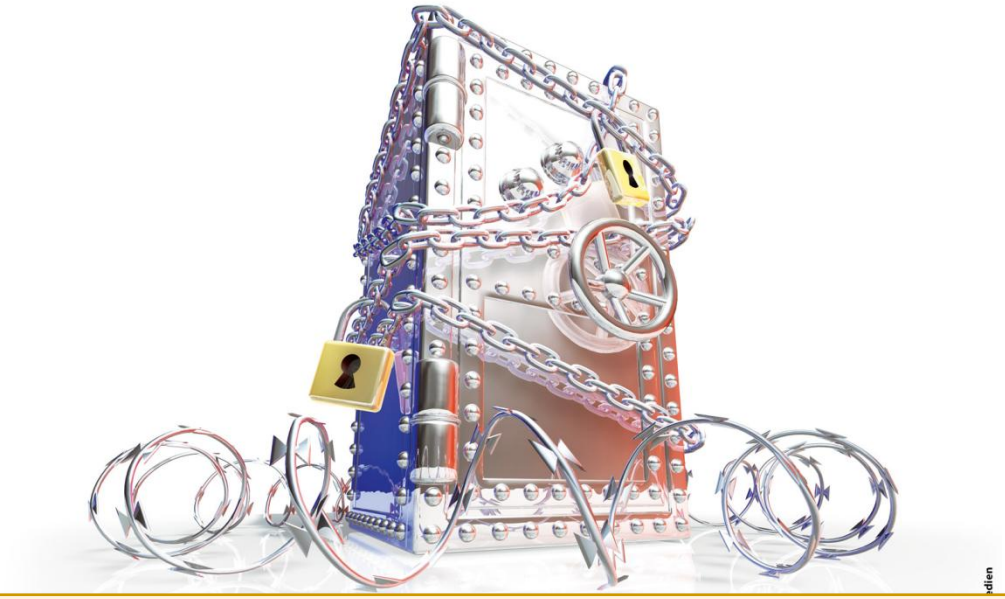
John the Ripper es un programa de criptografía que aplica fuerza bruta para descifrar contraseñas. Es capaz de romper varios algoritmos de cifrado o hash, como DES, SHA-1 y otros. Es una herramienta de seguridad muy popular, ya que permite a los administradores de sistemas comprobar que las contraseñas de los usuarios son suficientemente buenas.

Fiabilidad, Confidencialidad, Integridad y disponibilidad

Seguridad es un concepto asociado a la certeza o falta de riesgo . Conviene aclarar que no siendo posible la certeza absoluta, el elemento de riesgo está siempre presente, independientemente de las medidas de seguridad que se tomen, 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

Podemos entender como seguridad una característica de cualquier sistema que nos indica que ese sistema está libre de todo peligro, daño o riesgo, y que es, en cierta manera, infalible. Como esta característica, particularizando para el caso de sistemas informáticos, sistemas operativos o redes de computadores, es muy difícil de conseguir (según la mayoría de expertos, imposible), se suaviza la definición de seguridad y se pasa a hablar de fiabilidad, probabilidad de que un sistema se comporte tal y como se espera de él. ***Por tanto, se habla de tener sistemas fiables en lugar de sistemas seguros.***

Fiabilidad, Confidencialidad, Integridad y disponibilidad



El experto Eugene H. Spafford cita en su frase célebre: "el único sistema que es totalmente seguro es aquel que se encuentra apagado y desconectado, guardado en una caja fuerte de titanio que está enterrada en cemento, rodeada de gas nervioso y de un grupo de guardias fuertemente armados. Aún así, no apostaría mi vida en ello".

Fiabilidad, Confidencialidad, Integridad y disponibilidad

Si estudiamos las múltiples definiciones que de seguridad informática dan las distintas entidades, deduciremos los objetivos de la seguridad informática.

Según la **ISO27002**, la seguridad de la información se **puede caracterizar por prevenir las actividades que atentan contra la**:

- Confidencialidad: asegura que el acceso a la información está adecuadamente autorizado.
- Integridad: salvaguarda la precisión y completitud de la información y sus métodos de proceso.
- Disponibilidad: asegura que los usuarios autorizados pueden acceder a la información cuando la necesitan.

Fiabilidad, Confidencialidad, Integridad y disponibilidad

Otra de las definiciones de la seguridad informática dada por **INFOSEC Glorassry 2000**: "*Seguridad informática son las medidas y controles que aseguran la confidencialidad, integridad y disponibilidad de los activos de los sistemas de información, incluyendo hardware, software, firmware y aquella información que procesan, almacenan y comunican*"

A grandes rasgos se entiende que mantener un sistema seguro (o fiable) consiste básicamente en garantizar tres aspectos: ***confidencialidad, integridad y disponibilidad***

Fiabilidad, Confidencialidad, Integridad y disponibilidad

Confidencialidad: la capacidad de garantizar que la información, almacenada en el sistema informático o transmitida por la red, solamente va a estar disponible para aquellas personas autorizadas a acceder a dicha información, es decir, que si los contenidos cayesen en manos ajenas, estas no podrían acceder a la información o a su interpretación.

Este es uno de los principales problemas a los que se enfrentan muchas empresas, en los últimos años se ha incrementado el robo de los portátiles con la consecuente pérdida de información confidencial, de clientes, líneas de negocio…

En relación a éste objetivo, más adelante -en la UT10- analizaremos la ley de Protección de Datos de Carácter Personal.

Fiabilidad, Confidencialidad, Integridad y disponibilidad

Disponibilidad: la capacidad de garantizar que tanto el sistema como los datos van a estar disponibles al usuario en todo momento.

Pensemos, por ejemplo, en la importancia que tiene este objetivo para una empresa encargada de impartir ciclos formativos a distancia. Constantemente está recibiendo consultas, descargas a su sitio Web, etc., por lo que siempre deberá estar disponible para los usuarios.

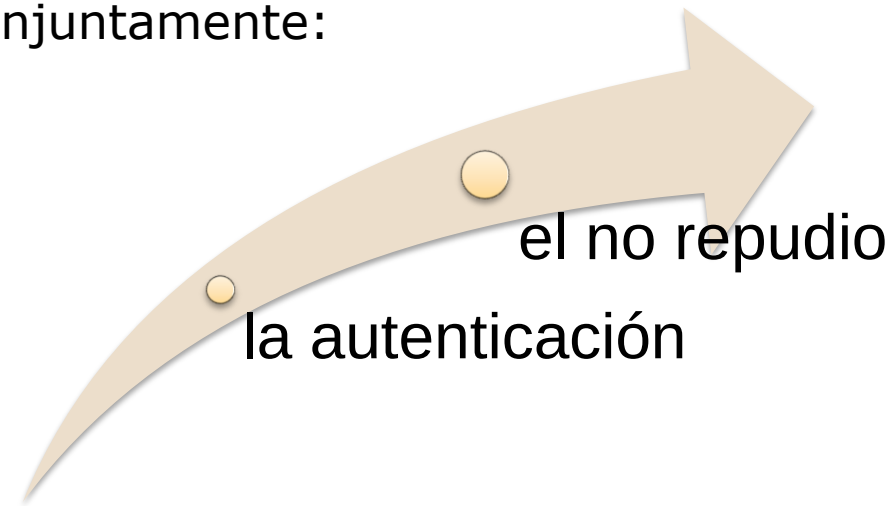
Integridad: la capacidad de garantizar que los datos no han sido modificados desde su creación sin autorización. La información que disponemos es válida y consistente.

Este objetivo es muy importante cuando estamos realizando trámites bancarios por Internet. Se deberá garantizar que ningún intruso pueda capturar y modificar los datos en tránsito.

Fiabilidad, Confidencialidad, Integridad y disponibilidad

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 perdida de integridad. Generalmente tienen que existir los tres aspectos descritos para que haya seguridad.

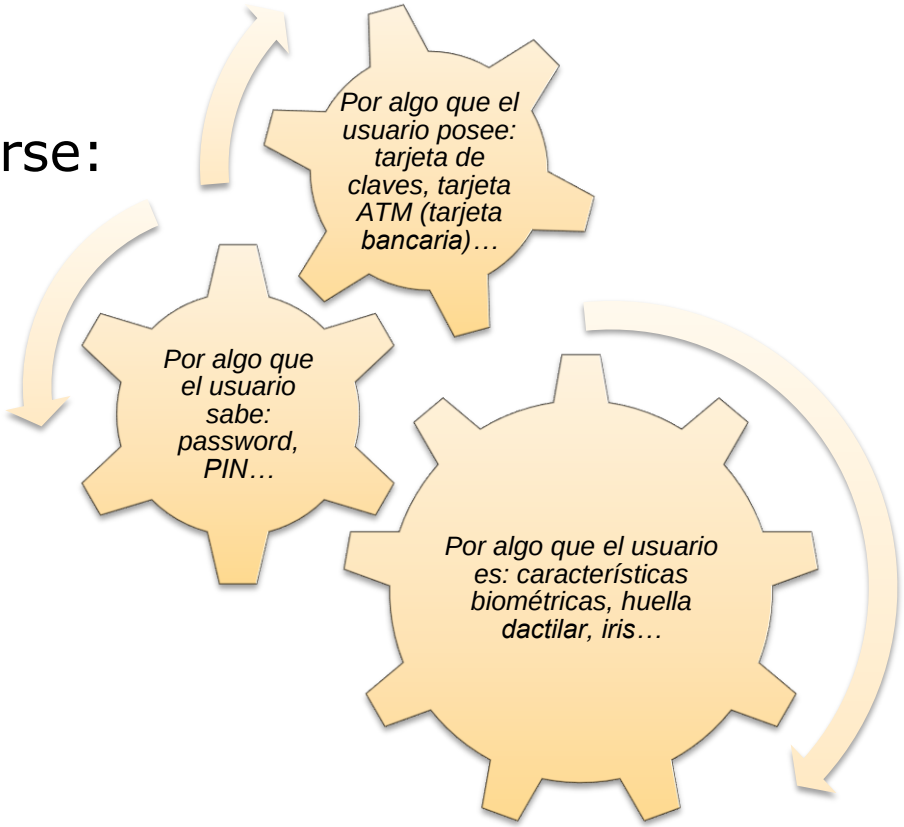
Junto con dichos aspecto u objetivos de la seguridad informática, se suelen estudiar conjuntamente:



Fiabilidad, Confidencialidad, Integridad y disponibilidad

Autenticación: Permite identificar al emisor de un mensaje, al creador de un documento o al equipo que se conecta a una red o a un servicio.

Formas de autenticarse:



Fiabilidad, Confidencialidad, Integridad y disponibilidad

No repudio: garantiza la participación de las partes en una comunicación. En toda comunicación, existe un emisor y un receptor, por lo que podemos distinguir dos tipos de no repudio:

***No repudio en origen**: garantiza que la persona que envía el mensaje no puede negar que es el emisor del mismo, ya que el receptor tendrá pruebas del envío.*

***No repudio en destino**: el receptor no puede negar que recibió el mensaje, porque el emisor tiene pruebas de la recepción del mismo.*

Si la autenticación prueba quién es el autor o propietario 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).

Fiabilidad, Confidencialidad, Integridad y disponibilidad

Al grupo de estas características y objetivos de la seguridad se les conoce como **CIDAN**, nombre sacado de la inicial de cada característica.

Fiabilidad, Confidencialidad, Integridad y disponibilidad

Para conseguir los objetivos mostrados en la anterior figura se utilizan los siguientes mecanismos:

Autenticación, que permite identificar al emisor de un mensaje, al creador de un documento o al equipo que se conecta a una red o a un servicio.

Autorización, que controla el acceso de los usuarios a zonas restringidas, a distintos equipos y servicios después de haber superado el proceso de autenticación.

Auditoría, que verifica el correcto funcionamiento de las políticas o medidas de seguridad tomadas.

Encriptación, que ayuda a ocultar la información transmitida por la red o almacenada en los equipos, para que cualquier persona ajena no autorizada, sin el algoritmo y clave de descifrado, pueda acceder a los datos que se quieren proteger.

Fiabilidad, Confidencialidad, Integridad y disponibilidad

Realización de copias de seguridad e imágenes de respaldo, para que en caso de fallos nos permita la recuperación de la información perdida o dañada.

Antivirus, como su nombre indica, consiste en un programa que permite estar protegido contra las amenazas de los virus.

Cortafuegos o firewall, programa que audita y evita los intentos de conexión no deseados en ambos sentidos, desde los equipos hacia la red y viceversa.

Servidores proxys, consiste en ordenadores con software especial, que hacen de intermediario entre la red interna de una empresa y una red externa, como pueda ser Internet. Estos servidores, entre otras acciones, auditan y autorizan los accesos de los usuarios a distintos tipos de servicios como el de FTP (transferencia de ficheros), o el Web (acceso a páginas de Internet).

Fiabilidad, Confidencialidad, Integridad y disponibilidad

Utilización firma electrónica o certificado digital, son mecanismos que garantizan la identidad de una persona o entidad evitando el no repudio en las comunicaciones o en la firma de documentos. También se utilizan mucho hoy en día para establecer comunicaciones seguras entre el PC del usuario y los servidores de Internet como las páginas Web de los bancos.

Conjunto de leyes encaminadas a la protección de datos personales que obligan a las empresas a asegurar su confidencialidad.

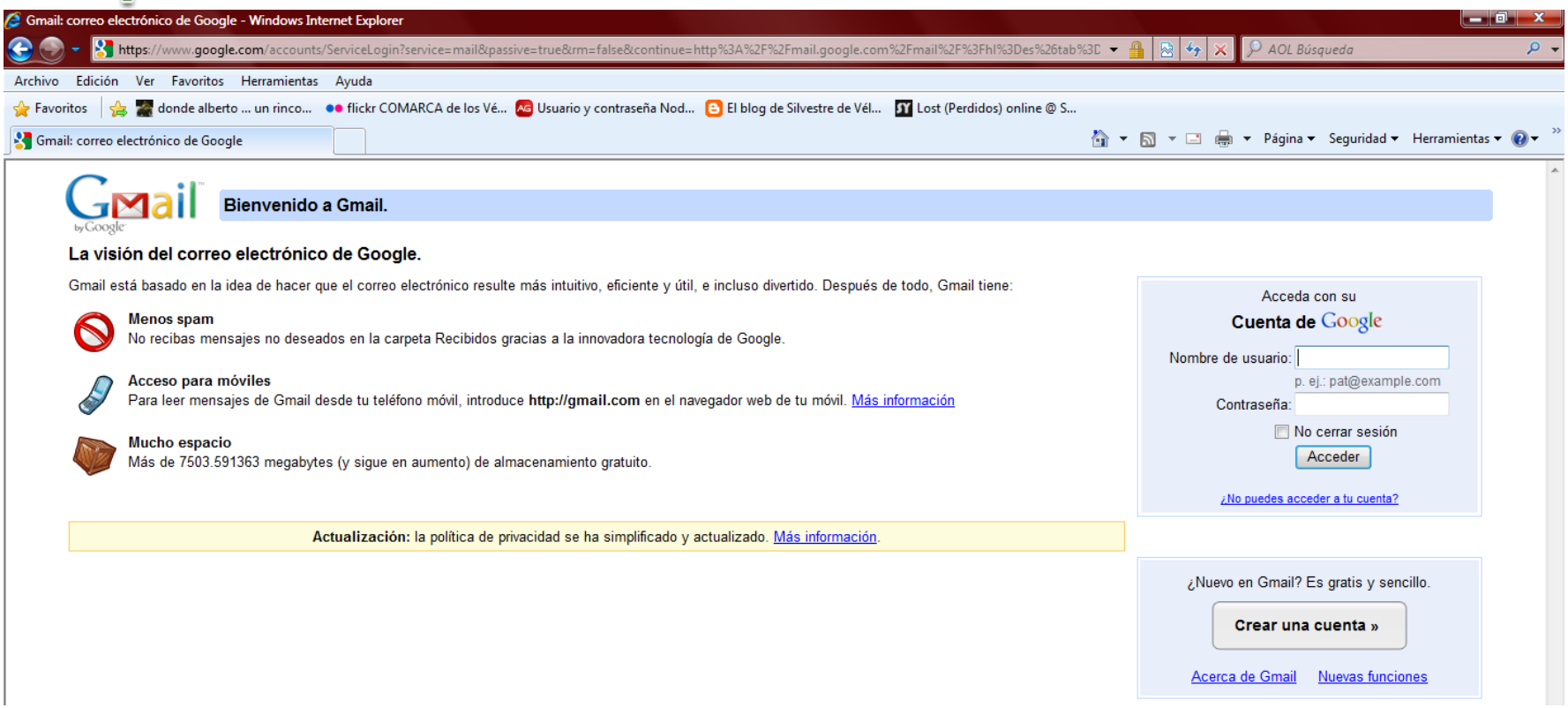
Fiabilidad, Confidencialidad, Integridad y disponibilidad

Ejemplo de Mecanismos:

Observemos el *certificado digital* que utiliza Gmail a la hora de autenticar a los usuarios mediante el nombre y la contraseña del mismo. Para realizar esta actividad se ha utilizado la aplicación Internet Explorer.

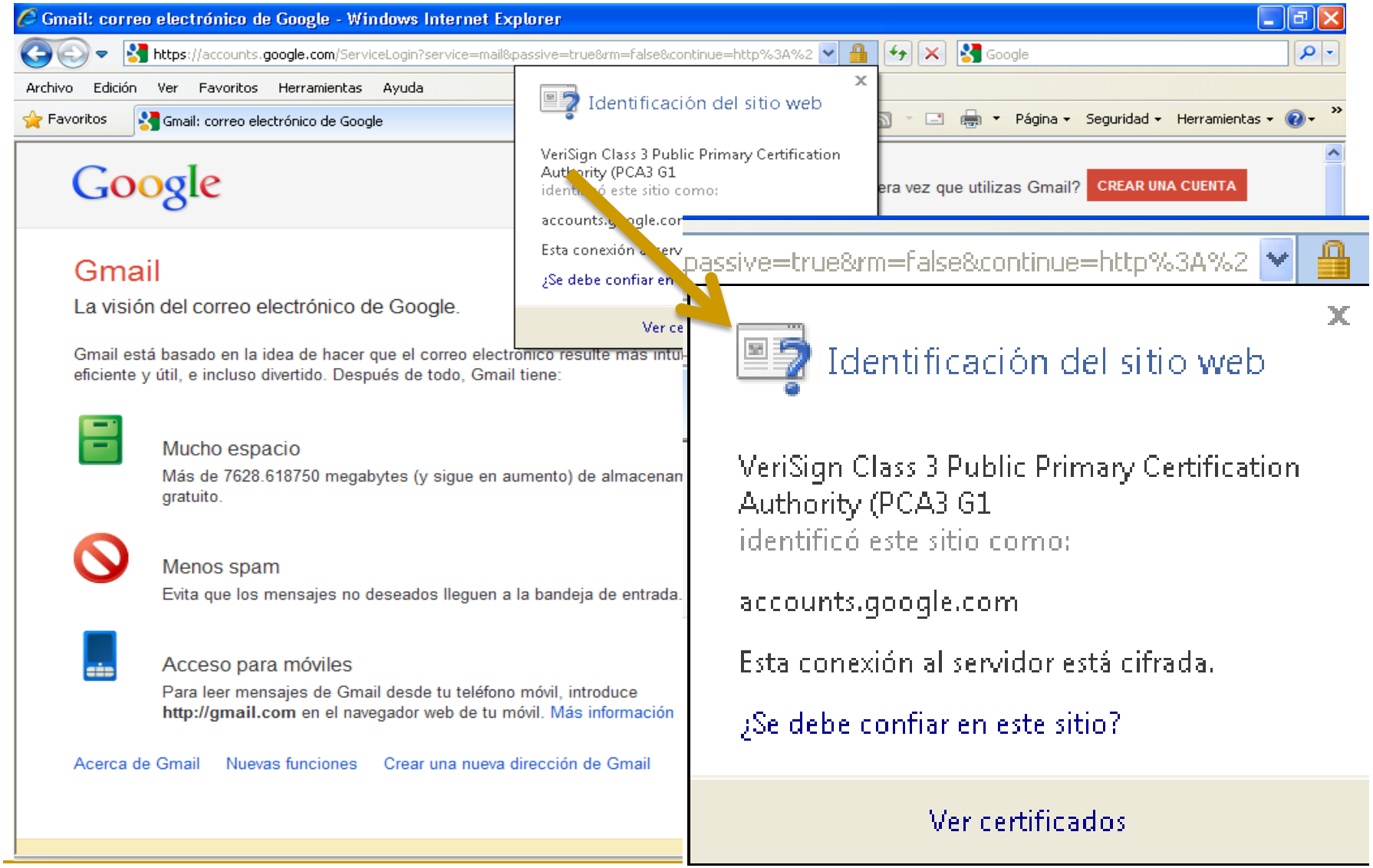
En la zona reservada para las direcciones, podemos observar que el protocolo utilizado es HTTPS en lugar de HTTP, que suele ser más habitual. En este caso se está utilizando un protocolo de transferencia de hipertexto seguro.

Fiabilidad, Confidencialidad, Integridad y disponibilidad



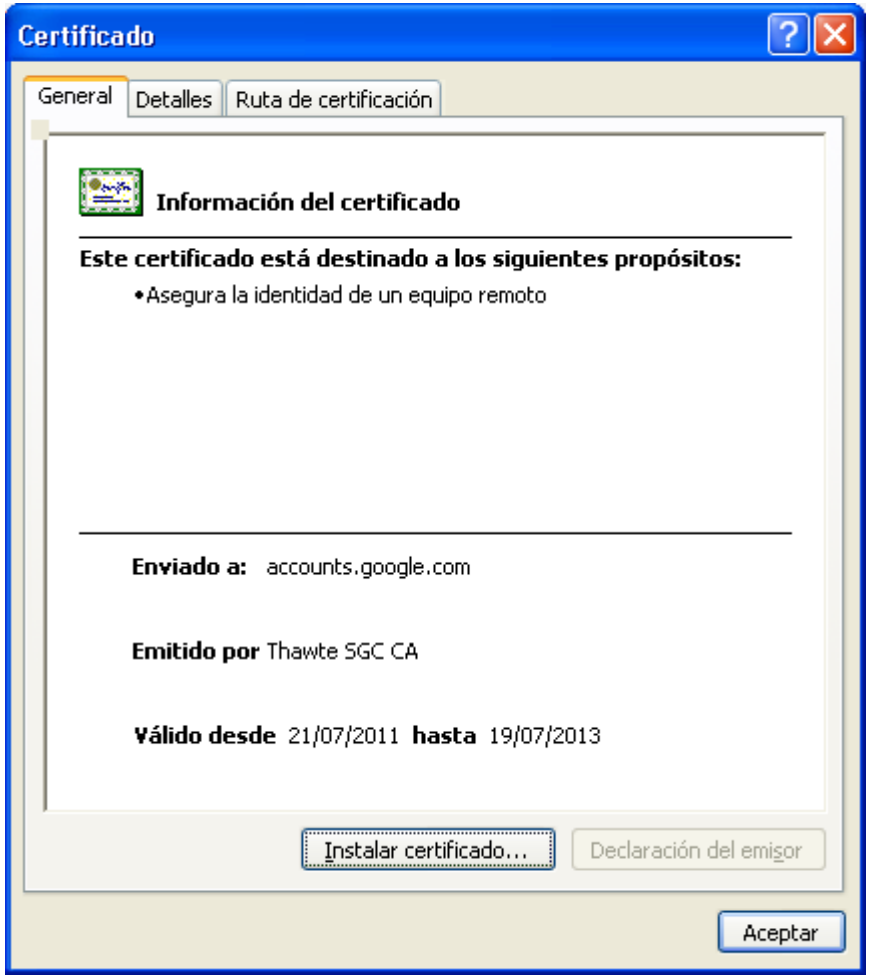
Si hacemos clic sobre el **candado**, que se muestra en la parte derecha de la URL, podemos verificar que la conexión estará cifrada usando un certificado digital de Google.

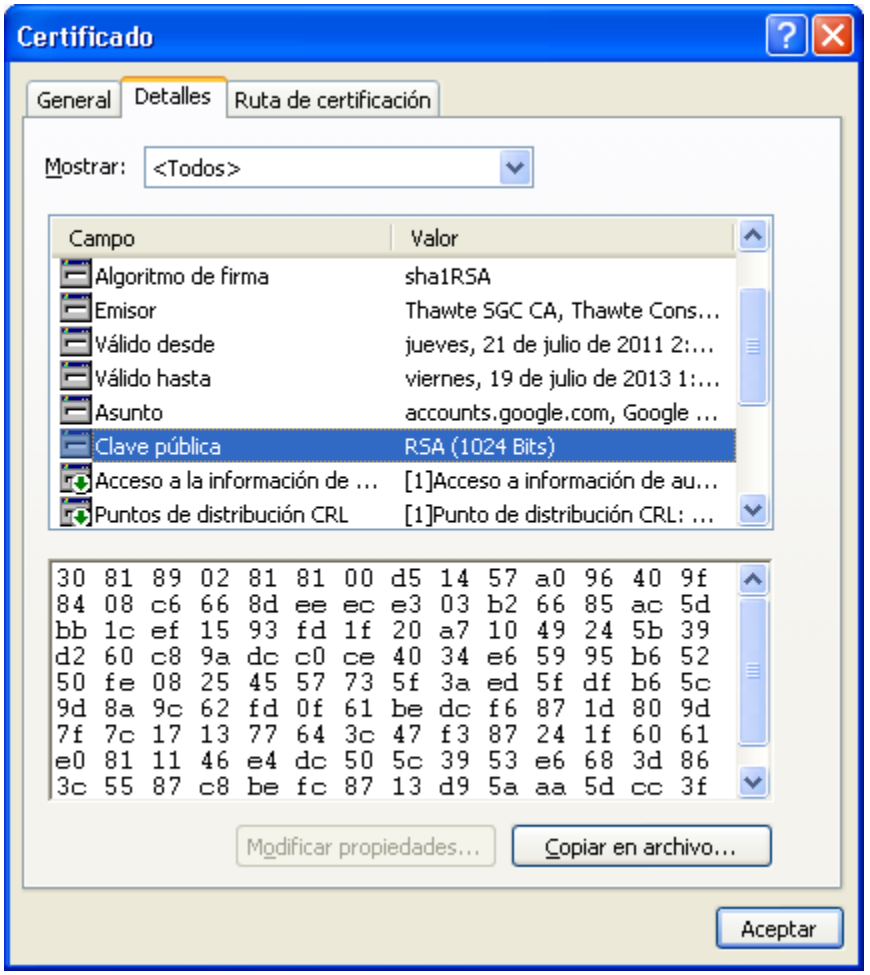
Fiabilidad, Confidencialidad, Integridad y disponibilidad



Fiabilidad, Confidencialidad, Integridad y disponibilidad

Si hacemos clic sobre **Ver Certificados** veremos información más detallada del certificado.





Fiabilidad, Confidencialidad, Integridad y disponibilidad

Práctica/cuestión sobre Confidencialidad

En esta práctica guiada estudiaremos cómo se puede asegurar la confidencialidad de los datos en sistema Windows, mediante la encriptación de archivos y carpetas.

La confidencialidad o privacidad de datos es uno de los aspectos críticos de la seguridad, por esto Microsoft incluyó a partir de su sistema Windows 2000, y posteriores, el método de archivos encriptados conocido como **EFS *(Encrypted File System) que cumple este propósito.***

Fiabilidad, Confidencialidad, Integridad y disponibilidad

Práctica/cuestión sobre Confidencialidad

Encrypting File System (EFS) es un sistema de archivos que, trabajando sobre NTFS, permite cifrado de archivos a nivel de sistema. Permite a los ***archivos administrados por el sistema operativo ser cifrados en las particiones NTFS en donde esté habilitado, para proteger datos confidenciales. EFS es incompatible con la compresión de*** carpetas.

El usuario que realice la encriptación de archivos será el único que dispondrá de acceso a su contenido, y al único que se le permitirá modificar, copiar o borrar el archivo, **controlado todo ello por el sistema operativo.**

Fiabilidad, Confidencialidad, Integridad y disponibilidad

Práctica/cuestión sobre Confidencialidad

Amenaza o vulnerabilidad

Como veremos en contenidos posteriores, en un sistema de información es posible obtener acceso al sistema de ficheros si podemos arrancar desde una distribución USB o CD/DVD Live, o incluso acceder localmente como administrador, teniendo de este modo acceso completo al contenido y por tanto incluso a carpetas restringidas por el sistema operativo. Para evitar la apertura , lectura o modificación de información privada bajo windows podemos utilizar las opciones de encriptación EFS.

Fiabilidad, Confidencialidad, Integridad y disponibilidad

Práctica/cuestión sobre Confidencialidad

Proceso de encriptación

EFS es un sistema de cifrado transparente (que sólo puede usarse bajo NTFS) para Windows.
Desde las propiedades de archivos o carpetas, opciones avanzadas, es posible acceder a un menú donde se le puede indicar al sistema que el directorio o unidad será empleado para almacenar archivos cifrados (con lo que todo lo que se almacene en él se cifrará) o se puede indicar también el cifrado de un archivo, cosa poco recomendable.
También es posible utilizar la herramienta de línea de comando ***cipher.exe*** *con el mismo efecto.*

Fiabilidad, Confidencialidad, Integridad y disponibilidad

Práctica/cuestión sobre Confidencialidad

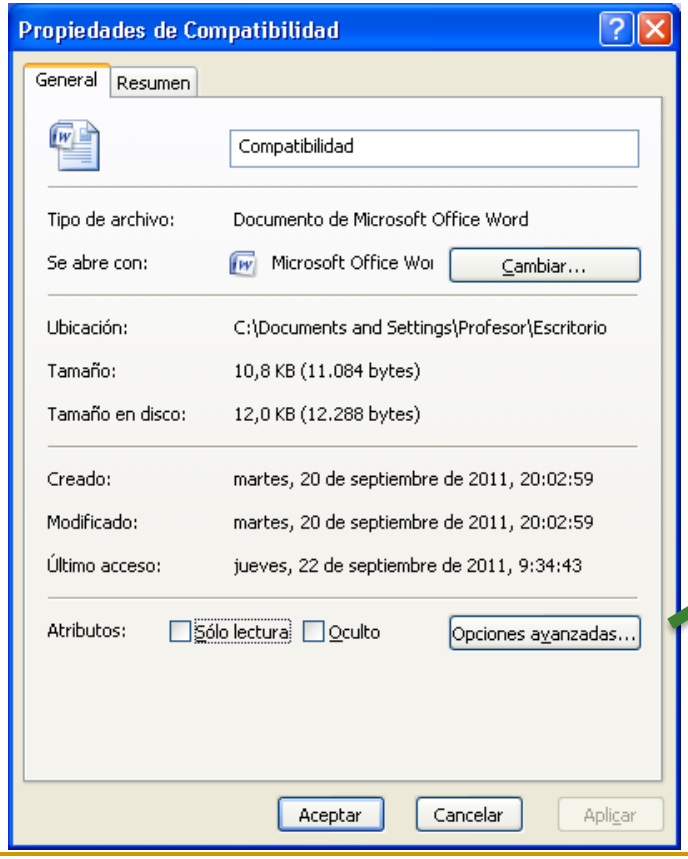
Proceso de encriptación

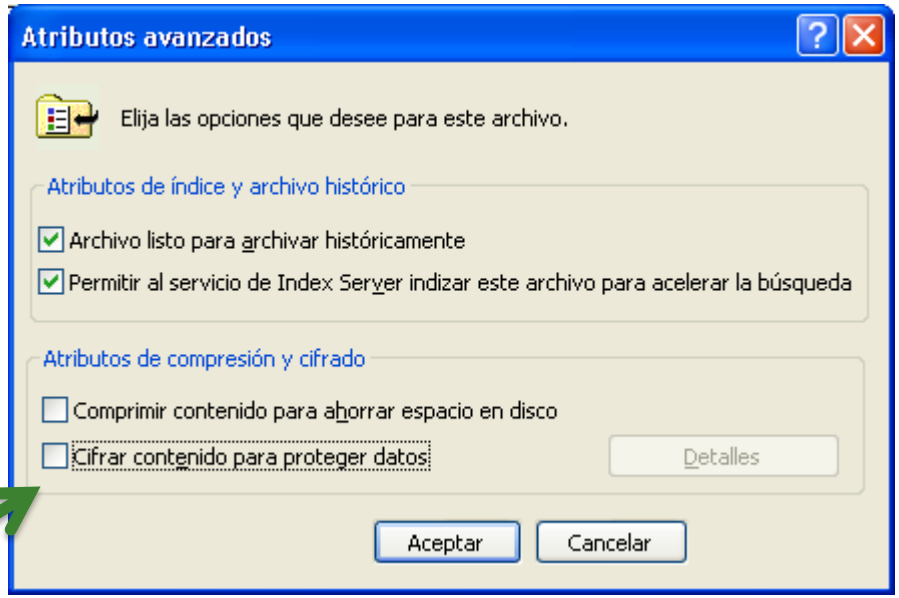
Una vez marcada una unidad o directorio como cifrado, todo lo que se almacene en él quedará cifrado (incluso para el administrador del sistema), pero no lo que ya hubiese dentro. El usuario no tendrá que preocuparse de nada más. Cada vez que inicie sesión, los datos estarán ahí para poder ser manipulados, pero una vez cerrada la sesión o si otro usuario diferente se presenta en el sistema (incluso con otro sistema operativo leyendo el disco duro) los datos aparecerán inaccesibles. En el explorer los archivos y carpetas cifrados se colorearán de verde.

Podemos probarlo creando un fichero de texto plano con información confidencial en su interior y cifrarlo.

Fiabilidad, Confidencialidad, Integridad y disponibilidad

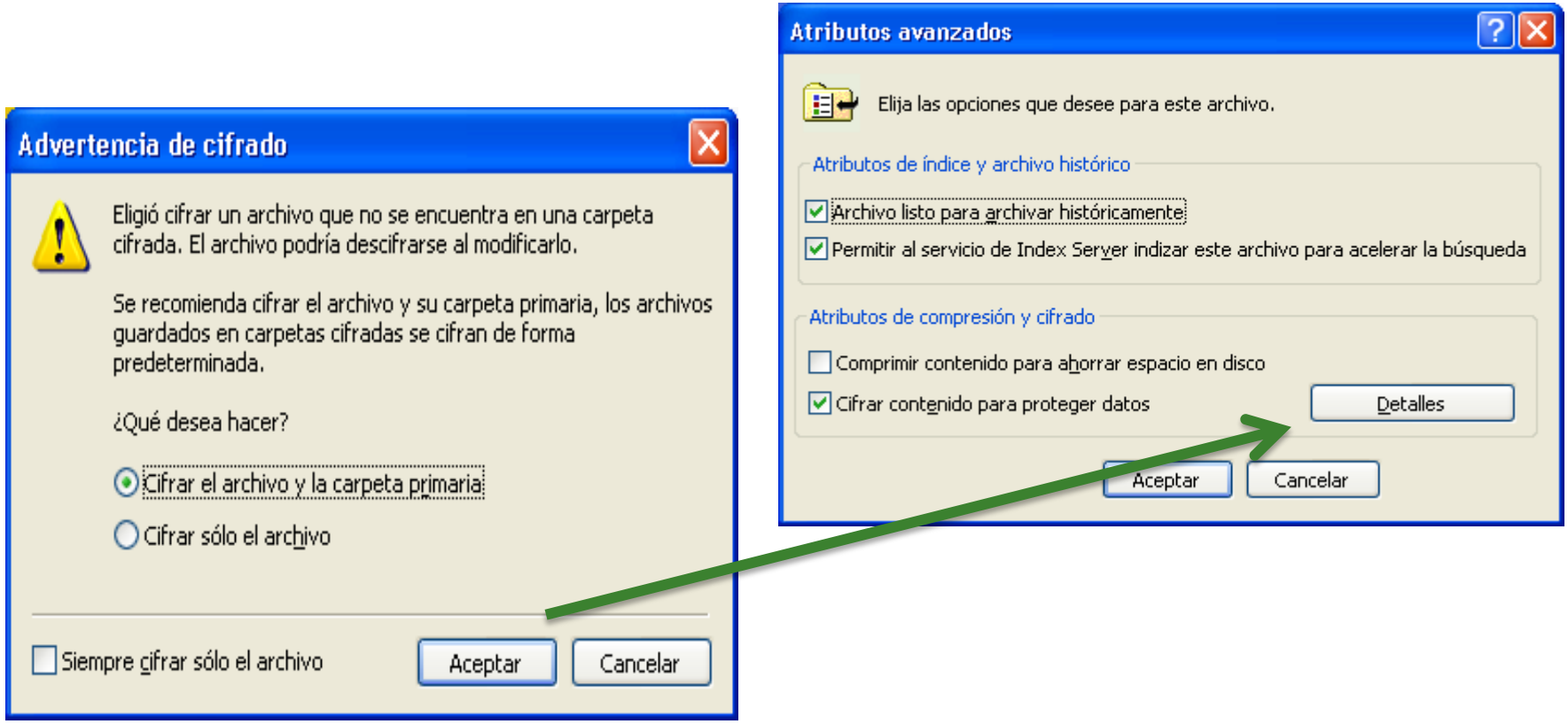
Práctica/cuestión sobre Confidencialidad





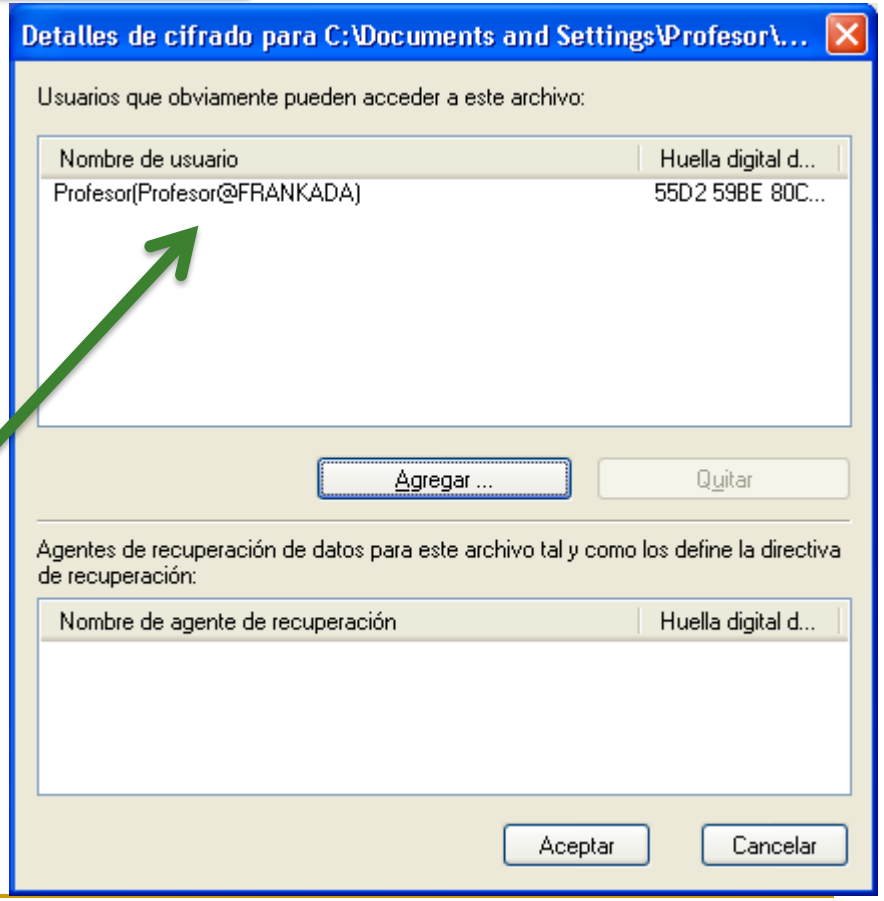
Fiabilidad, Confidencialidad, Integridad y disponibilidad

Práctica/cuestión sobre Confidencialidad



Fiabilidad, Confidencialidad, Integridad y disponibilidad

Práctica/cuestión sobre Confidencialidad



Fiabilidad, Confidencialidad, Integridad y disponibilidad

Práctica/cuestión sobre Confidencialidad

Verificaciones:

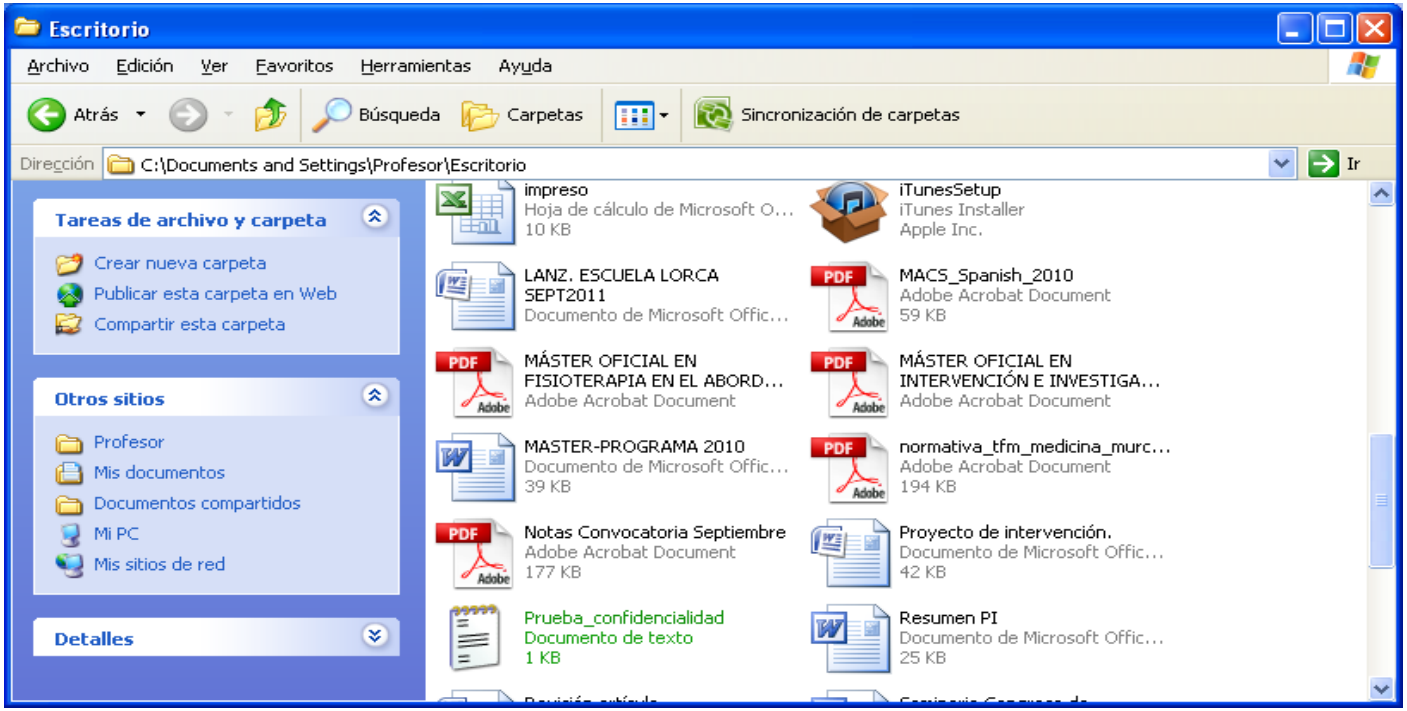
Si accedemos con otro usuario al sistema que tenga permisos para acceder a todo el sistema de archivos, por ejemplo desde una cuenta de tipo administrador (distinta a la que ha cifrado el archivo), podemos ver que el nombre del archivo nos aparecerá en color verde y, al intentar acceder a él, nos indicará acceso denegado. Igualmente si intentamos modificar el archivo para que deje de estar cifrado y aplicamos los cambios nos indicará error al aplicar los atributos. Aunque no es posible leer ni modificar su contenido, sí es posible borrarlo.

Fiabilidad, Confidencialidad, Integridad y disponibilidad

Práctica/cuestión sobre Confidencialidad

Verificaciones:

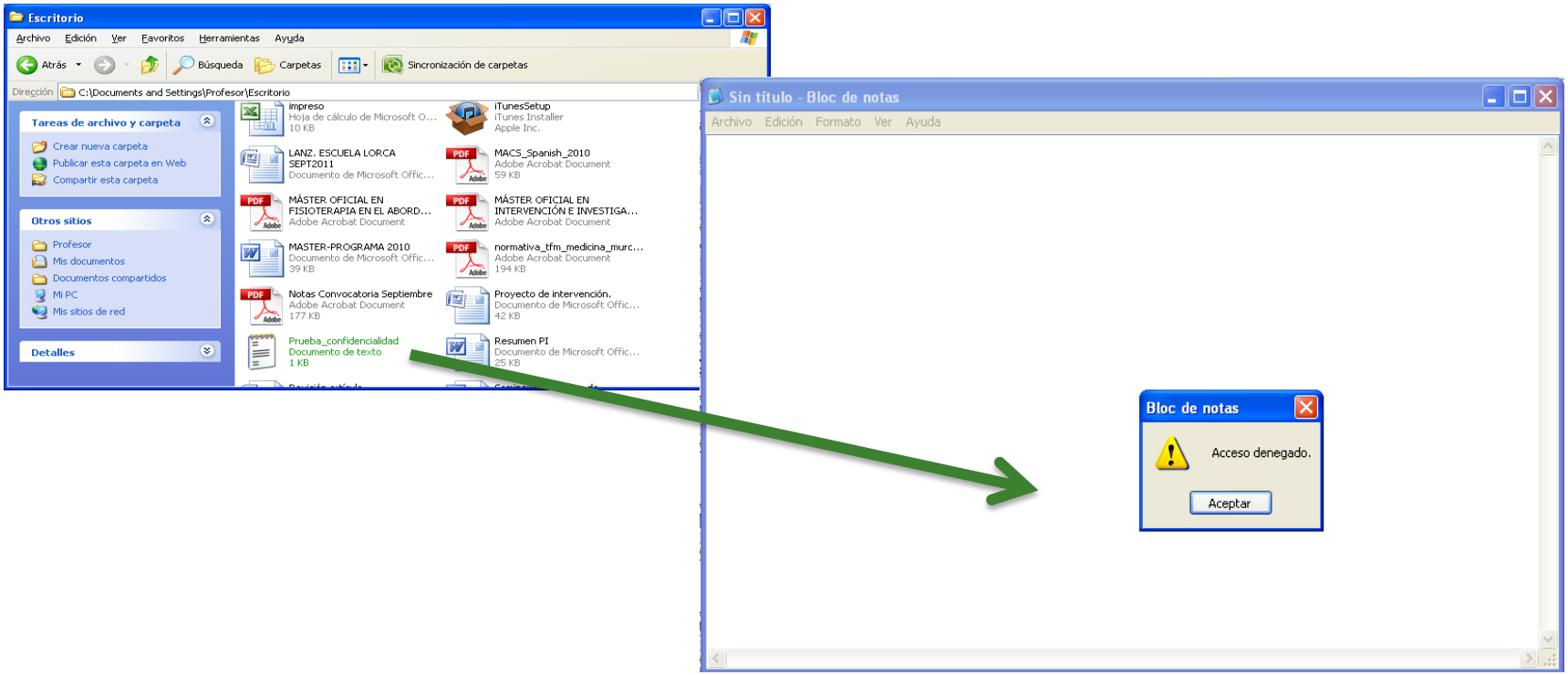
Usuario con permisos para acceder al sistema de archivos



Fiabilidad, Confidencialidad, Integridad y disponibilidad

Práctica/cuestión sobre Confidencialidad

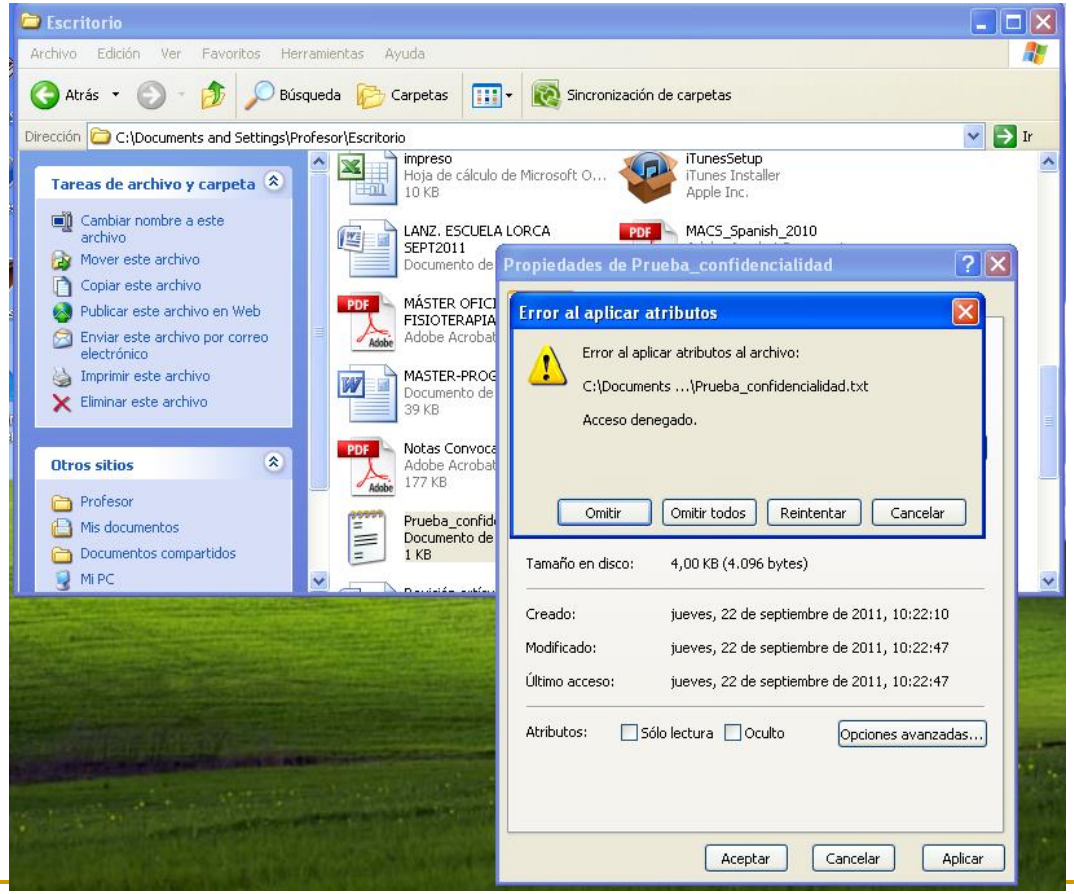
Verificaciones:



Fiabilidad, Confidencialidad, Integridad y disponibilidad

Práctica/cuestión sobre Confidencialidad

Verificaciones:

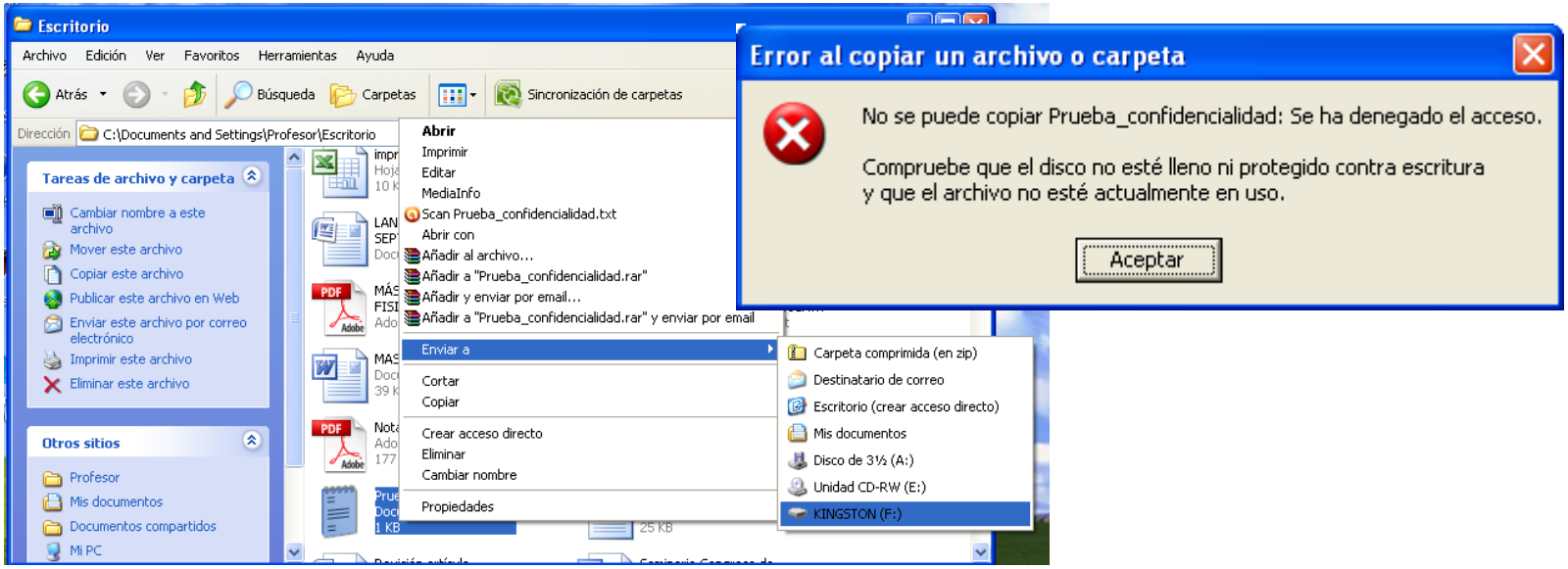


Fiabilidad, Confidencialidad, Integridad y disponibilidad

Práctica/cuestión sobre Confidencialidad

Verificaciones:

El archivo cifrado no es portable o copiable a una unidad externa ya que el sistema operativo pierde el control de su cifrado:



Fiabilidad, Confidencialidad, Integridad y disponibilidad

Práctica/cuestión sobre Confidencialidad

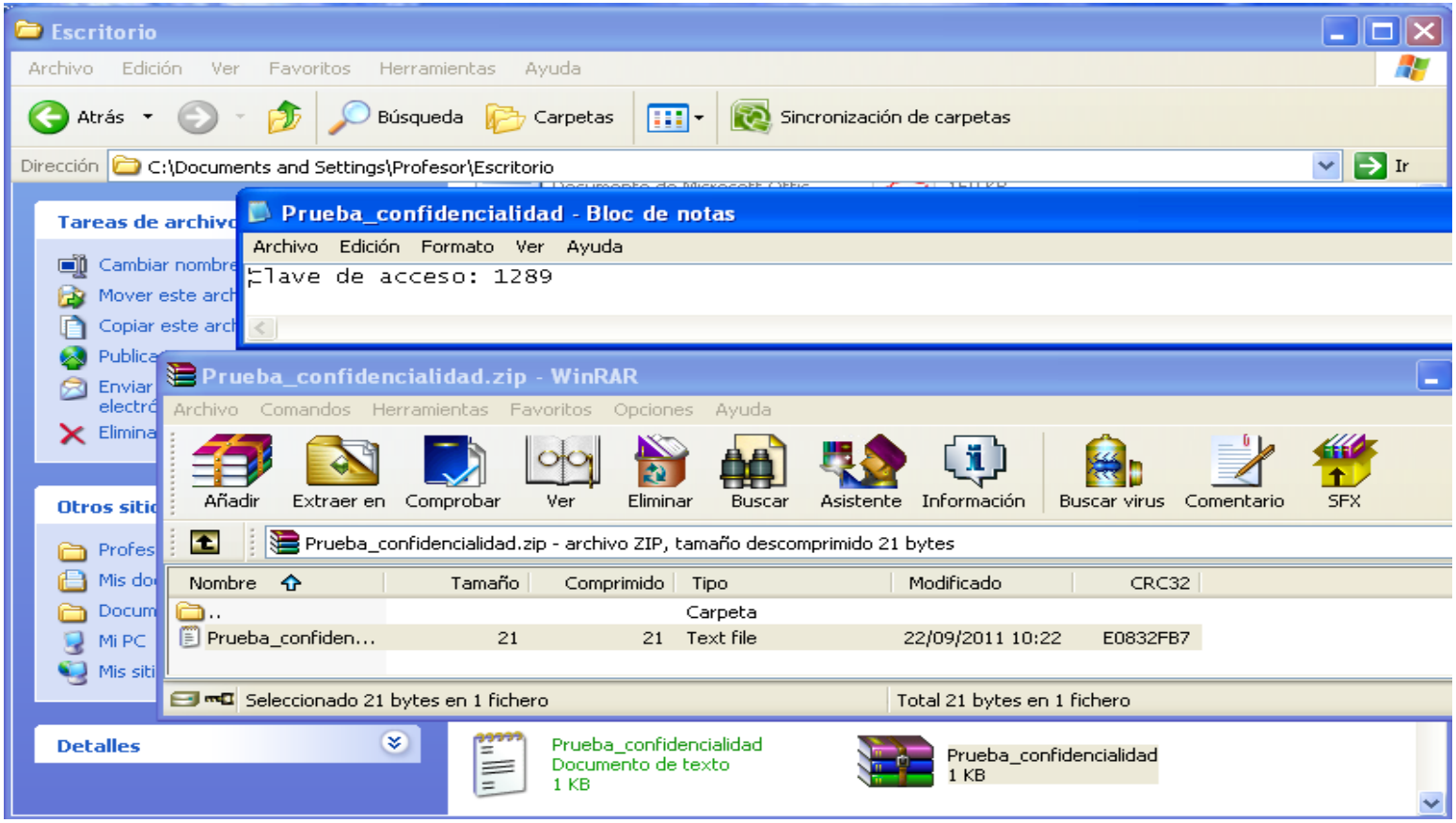
Verificaciones:

En caso de tener acceso al sistema de archivos con un arranque desde una distribución modo Live (en nuestro ejemplo Ubuntu), montando la partición correspondiente (en este caso el punto de montaje */mnt/win) podremos borrar el archivo, pero no se nos permitirá ni copiarlo ni leer la información contenida.*

Si hemos comprimido el archivo en zip desde Windows, sí podremos acceder a su contenido confidencial.

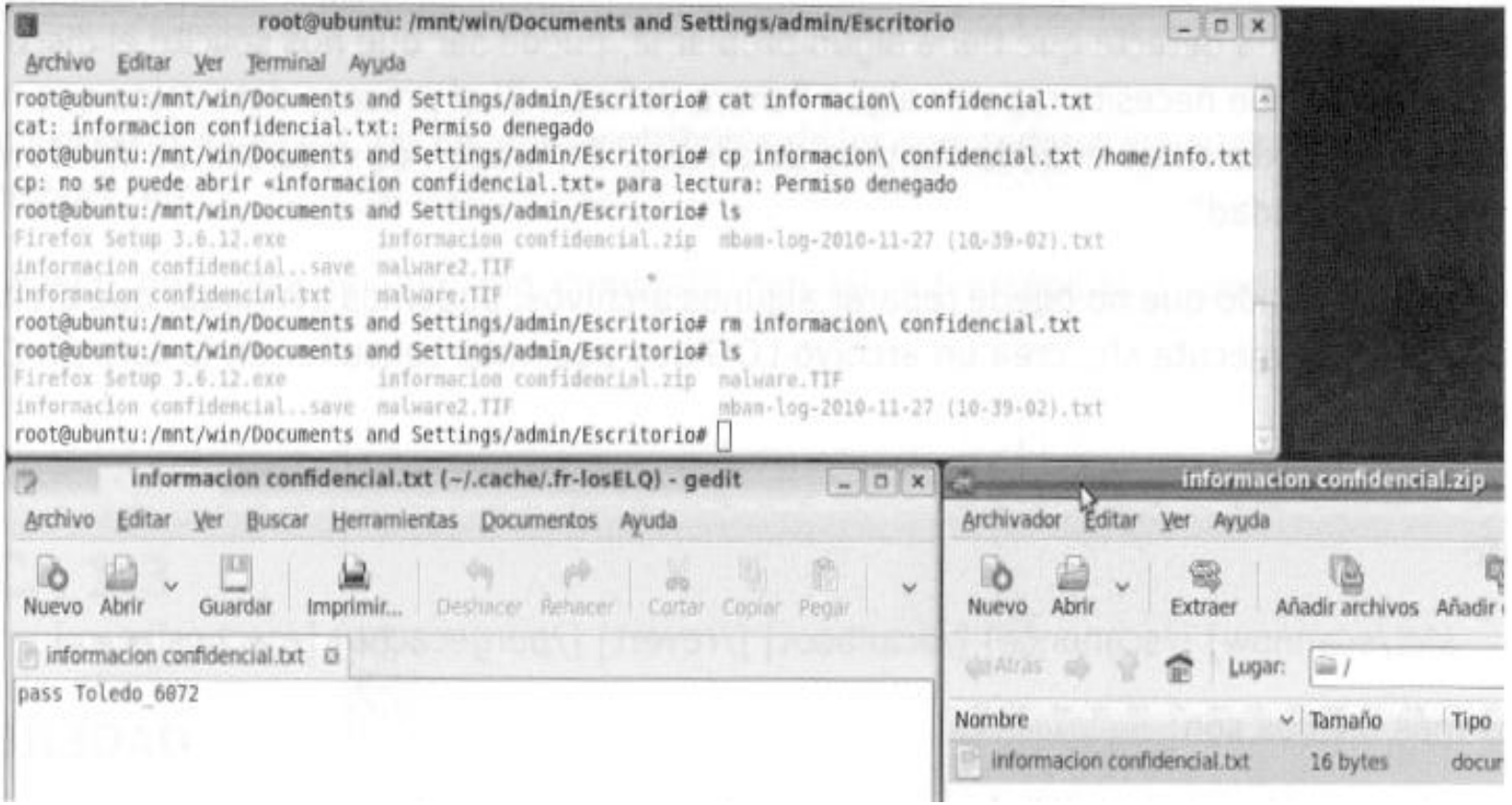
Fiabilidad, Confidencialidad, Integridad y disponibilidad

Práctica/cuestión sobre Confidencialidad



Fiabilidad, Confidencialidad, Integridad y disponibilidad

Práctica/cuestión sobre Confidencialidad



Fiabilidad, Confidencialidad, Integridad y disponibilidad

Práctica/cuestión sobre Integridad

Amenaza o vulnerabilidad

En caso de que algún tipo de *malware reemplace o falsifique archivos del sistema operativo, ocultándose para realizar tareas no autorizadas, la búsqueda y detección del mismo se complica ya que los análisis antimalware y de los procesos sospechosos por parte de administradores de sistemas, no dudarán de la veracidad de dichos archivos y procesos.*

A este tipo de malware se le denomina ***rootkit, programa que sustituye los ejecutables binarios del sistema para ocultarse mejor, pudiendo servir de puertas trasera o backdoor para la ejecución malware remota.***

Fiabilidad, Confidencialidad, Integridad y disponibilidad

Práctica/cuestión sobre Integridad

Amenaza o vulnerabilidad

- *System File Checker (SFC) es una utilidad de los sistemas Windows que comprueba la integridad de los archivos de sistema.*

- ***Rootkit hunter es una de las herramientas más completa bajo GNU/Linux que entre otras tareas puede, examinar los permisos de los ejecutables del sistema, buscar rootkits conocidos rastreando ficheros ocultos, realiza la comprobación de integridad de los archivos de sistema, es decir, verifica que no han sido modificados.***

Un **rootkit** es una herramienta o un grupo de ellas, que tiene como finalidad esconderse a sí misma y esconder otros programas, procesos, archivos, directorios, claves de registro, y puertos que permiten al intruso mantener el acceso a un sistema para remotamente comandar acciones o extraer información sensible.

http://es.wikipedia.org/wiki/Rootkit

Fiabilidad, Confidencialidad, Integridad y disponibilidad

Práctica/cuestión sobre Integridad

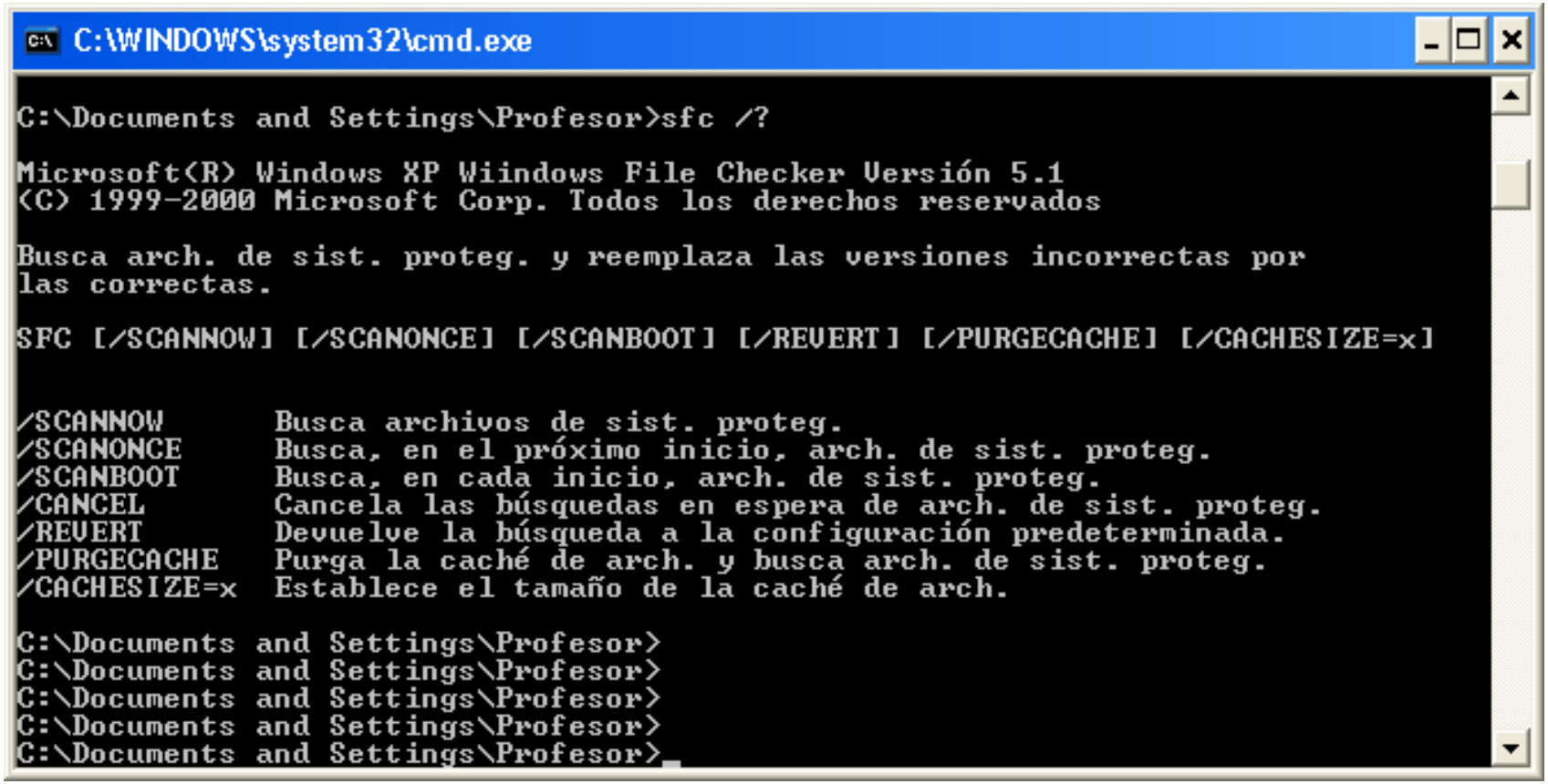
Verificación Windows

SFC examina la integridad de todos los archivos de sistema protegidos de Windows y reemplaza los que están corruptos dañados por versiones correctas, si es posible.

En este proceso, si el sistema detecta que tiene algún problema, puede ser que nos solicite el disco de instalación de Windows en el caso de que necesite reparar algún fichero dañado. Si el proceso determina que no hay errores, al final nos mostrará un texto como el de la ventana de arriba, "Protección de recursos de Windows no encontró alguna infracción de integridad".

Fiabilidad, Confidencialidad, Integridad y disponibilidad

Práctica/cuestión sobre Integridad



Fiabilidad, Confidencialidad, Integridad y disponibilidad

Práctica/cuestión sobre Integridad

Verificación GNU/Linux

1. *Rootkit Hunter se puede instalar mediante el comando:*

```
sudo aptitude install rkhunter
```

Se recomienda antes de ejecutarlo, como todo software de seguridad actualizará a la versión más actual:

```
sudo rkhunter --update
```

2. Para la ejecución sobre el sistema, verificando todas sus opciones:

```
sudo rkhunter --checkall
```

Fiabilidad, Confidencialidad, Integridad y disponibilidad

Práctica/cuestión sobre Integridad

Verificación GNU/Linux


```
Archivo  Editar  Ver  Terminal  Ayuda
root@ubuntu:/home/alumno# rkhunter --checkall
[ Rootkit Hunter version 1.3.2 ]

Checking system commands...

  Performing 'strings' command checks
    Checking 'strings' command                          [ OK ]

  Performing 'shared libraries' checks
    Checking for preloading variables                   [ None found ]
    Checking for preload file                           [ Not found ]
    Checking LD_LIBRARY_PATH variable                   [ Not found ]

  Performing file properties checks
    Checking for prerequisites                          [ OK ]
    /bin/bash                                           [ OK ]
    /bin/cat                                            [ OK ]
    /bin/chmod                                          [ OK ]
    /bin/chown                                          [ OK ]
    /bin/cp                                             [ OK ]
    /bin/date                                           [ OK ]
    /bin/df                                             [ OK ]
    /bin/dmesg                                          [ OK ]
    /bin/echo                                           [ OK ]
```

http://www.rootkit.nl/projects/rootkit_hunter.html

Fiabilidad, Confidencialidad, Integridad y disponibilidad

Práctica/cuestión sobre Disponibilidad

Identificar y analizar la **disponibilidad de servicios o servidores, puertos** abiertos y versiones de sistemas operativos que los soportan, supone la información base para el estudio de las innumerables vulnerabilidades los sistemas en red. De este modo se podrán tomar medidas frente a estos puntos débiles de nuestros sistemas.

Como ejemplo podemos mencionar ***Nmap ("mapeador de redes")***. Es una herramienta de código abierto para exploración de red y auditoría de seguridad. Utiliza paquetes IP para determinar qué equipos se encuentran disponibles en una red, qué servicios ofrecen, mediante qué aplicaciones (nombre y versión de la aplicación), qué sistemas operativos (y sus versiones) ejecutan, qué tipo de filtros de paquetes o cortafuegos se están utilizando, así como otras características.

Fiabilidad, Confidencialidad, Integridad y disponibilidad

Práctica/cuestión sobre Disponibilidad

Amenaza o vulnerabilidad

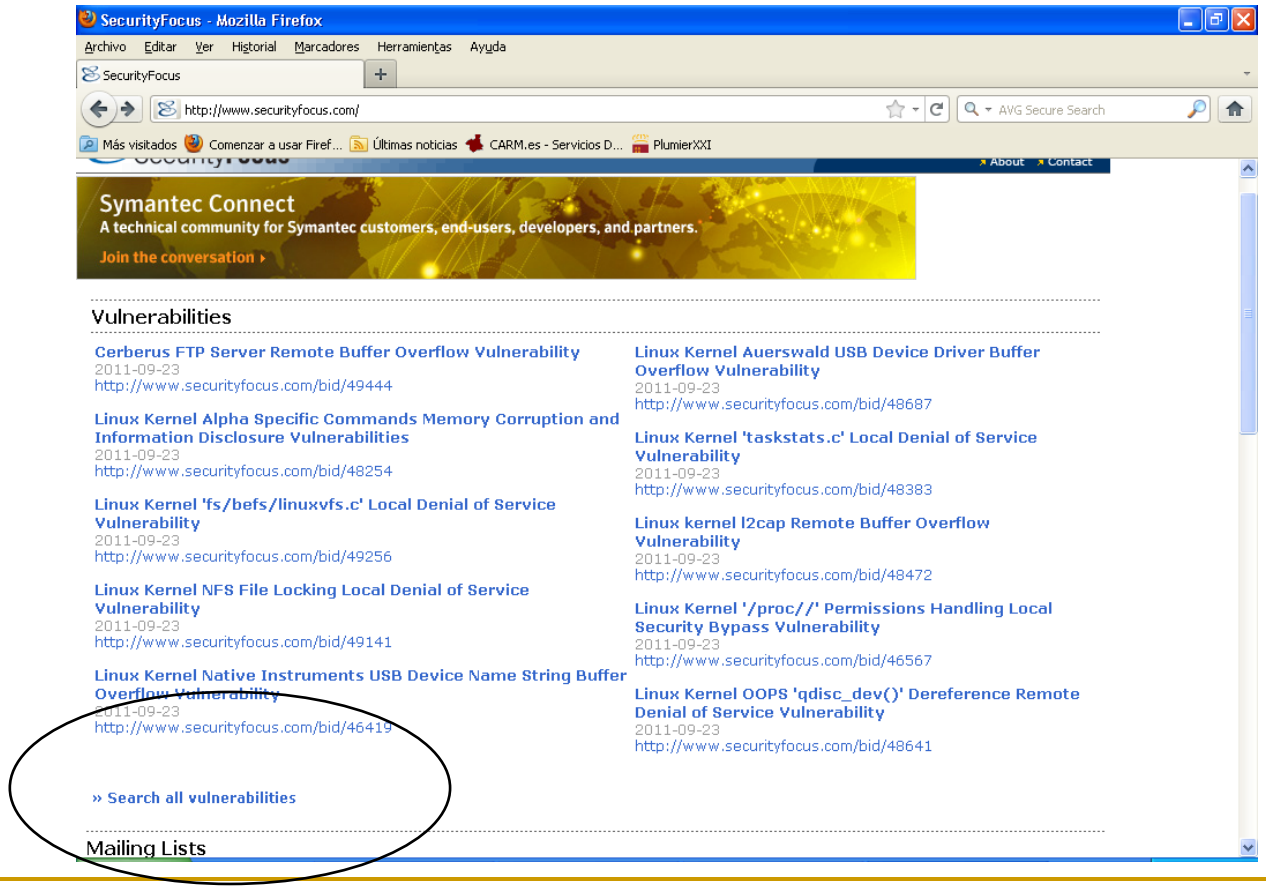
Para las versiones de software de servidores y de los sistemas operativos es posible **buscar posibles vulnerabilidades existentes:**

- *www.securityfocus.com. Informes sobre vulnerabilidades en aplicaciones y sistemas operativos, se puede buscar información sobre las versiones de los productos de distintos fabricantes e incluso descargar **exploits** de verificación.*

Exploit (del inglés *to exploit*, *explotar* o *aprovechar*) es una pieza de software, un fragmento de datos, o una secuencia de comandos con el fin de automatizar el aprovechamiento de un error, fallo o vulnerabilidad, a fin de causar un comportamiento no deseado o imprevisto en los programas informáticos, hardware, o componente electrónico (por lo general computarizado).

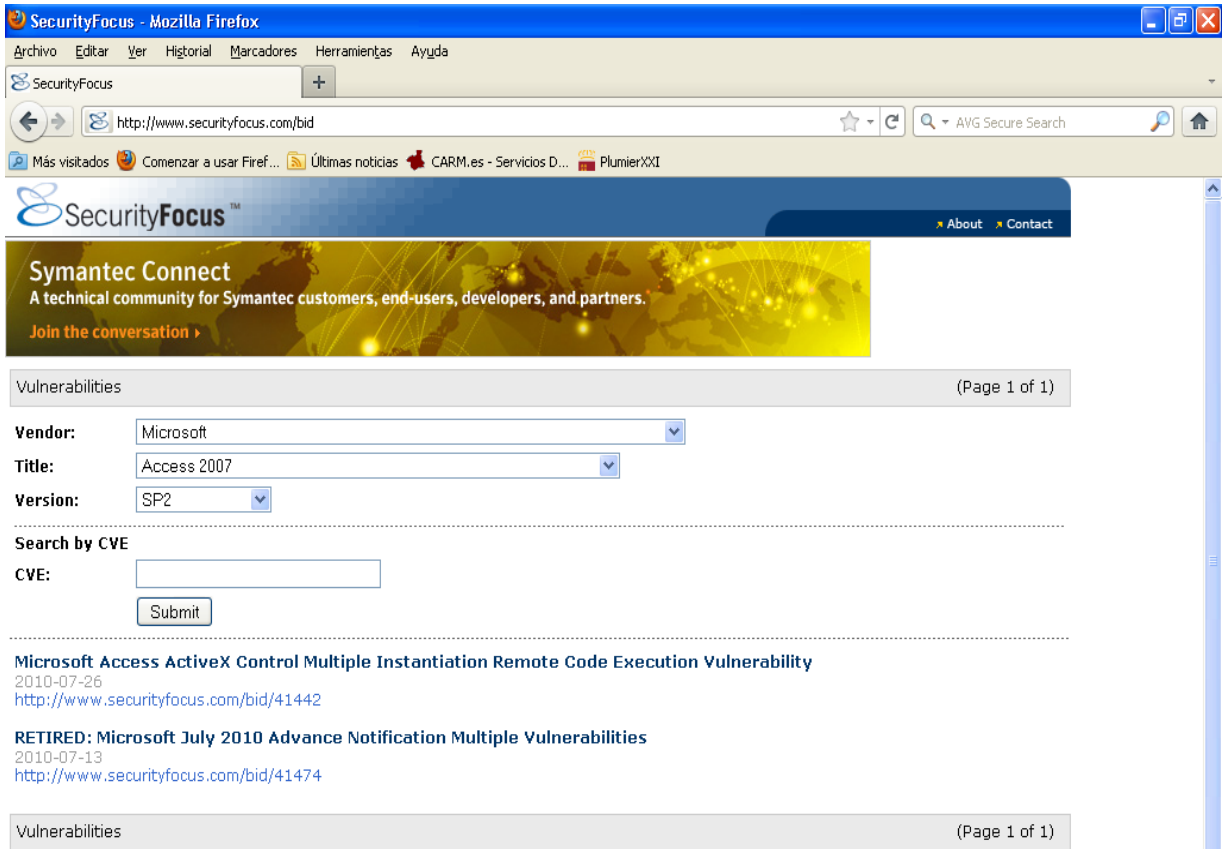
Fiabilidad, Confidencialidad, Integridad y disponibilidad

Práctica/cuestión sobre Disponibilidad



Fiabilidad, Confidencialidad, Integridad y disponibilidad

Práctica/cuestión sobre Disponibilidad



Fiabilidad, Confidencialidad, Integridad y disponibilidad

Práctica/cuestión sobre Disponibilidad

Amenaza o vulnerabilidad

- *www.nessus.org.* Es un programa de escaneo de vulnerabilidades en diversos sistemas operativos. Consiste en nessusd, el daemon Nessus, que realiza el escaneo en el sistema objetivo, y nessus, el cliente (basado en consola o gráfico) que muestra el avance y resultado de los escaneos .

Fiabilidad, Confidencialidad, Integridad y disponibilidad

Práctica/cuestión sobre Disponibilidad

Amenaza o vulnerabilidad

Microsoft Baseline Security Analyzer 2.2

Microsoft Baseline Security Analyzer (MBSA) es una herramienta fácil de usar diseñada para los profesionales de TI que ayuda a las pequeñas y medianas empresas a determinar su estado de seguridad según las recomendaciones de seguridad de Microsoft y ofrece orientación de soluciones específicas. Sirve para detectar los errores más comunes de configuración de seguridad y actualizaciones de seguridad que falten en sus sistemas informáticos.

http://technet.microsoft.com/es-es/security/cc184923

Microsoft Baseline Security Analyzer
(disponible en alemán, francés, inglés y japonés)

Fiabilidad, Confidencialidad, Integridad y disponibilidad

Práctica/cuestión sobre Disponibilidad

Fiabilidad, Confidencialidad, Integridad y disponibilidad

Práctica/cuestión sobre Disponibilidad

Amenaza o vulnerabilidad

Del análisis y estudio de las vulnerabilidades se aprovechan los desarrolladores de exploits.

Para explorar un sistema existen aplicaciones como los **metasploits**, herramientas con interfaz modo comando y web, que posee un conjunto de exploits para aprovechar las vulnerabilidades más conocidas de puertos, sistemas y aplicaciones.

Metasploit Es un proyecto open source de seguridad informática que proporciona información acerca de vulnerabilidades de seguridad y ayuda en tests de penetración y en el desarrollo de firmas para Sistemas de Detección de Intrusos.

http://www.metasploit.com/framework/download/

Fiabilidad, Confidencialidad, Integridad y disponibilidad

Práctica/cuestión sobre Disponibilidad

Verificación

***N*map** es un programa de código abierto que sirve para efectuar rastreo de puertos, escrito originalmente por Gordon Lyon (más conocido por su alias *Fyodor Vaskovich*). Se usa para evaluar la seguridad de sistemas informáticos, así como para descubrir servicios o servidores en una red informática.

http://nmap.org/man/es/index.html#man-description

Fiabilidad, Confidencialidad, Integridad y disponibilidad

ALTA DISPONIBILIDAD

La alta disponibilidad (High Availability) se refiere a la capacidad de que aplicaciones y datos se encuentren operativos para los usuarios autorizados en todo momento y sin interrupciones, debido principalmente a su carácter crítico.

El objetivo de la misma es mantener nuestros sistemas funcionando las 24 horas del día, 7 días a la semana, 365 días al año, manteniéndolos a salvo de interrupciones, ***teniendo en cuenta que se diferencian dos tipos de interrupciones:***

- Las interrupciones previstas, que se realizan cuando paralizamos el sistema para realizar cambios o mejoras en nuestro hardware o software.
- Las interrupciones imprevistas, 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).

Fiabilidad, Confidencialidad, Integridad y disponibilidad

ALTA DISPONIBILIDAD

- Las métricas comúnmente utilizadas para medir la disponibilidad y fiabilidad de un sistema son el tiempo medio entre fallos o MTTF (Mean Time To Failure) que mide el tiempo medio transcurrido hasta que un dispositivo falla, y el tiempo medio de recuperación o MTTR (Mean Time To Recover) mide el tiempo medio tomado en restablecerse la situación normal una vez que se ha producido el fallo.

- El tiempo en el que un sistema está fuera de servicio se mide a menudo como el cociente MTTR / MTTF.

- Lógicamente, nuestro principal objetivo es aumentar el MTTF y reducir el MTTR de forma que minimicemos el tiempo de no disponibilidad del servicio.

Fiabilidad, Confidencialidad, Integridad y disponibilidad

ALTA DISPONIBILIDAD

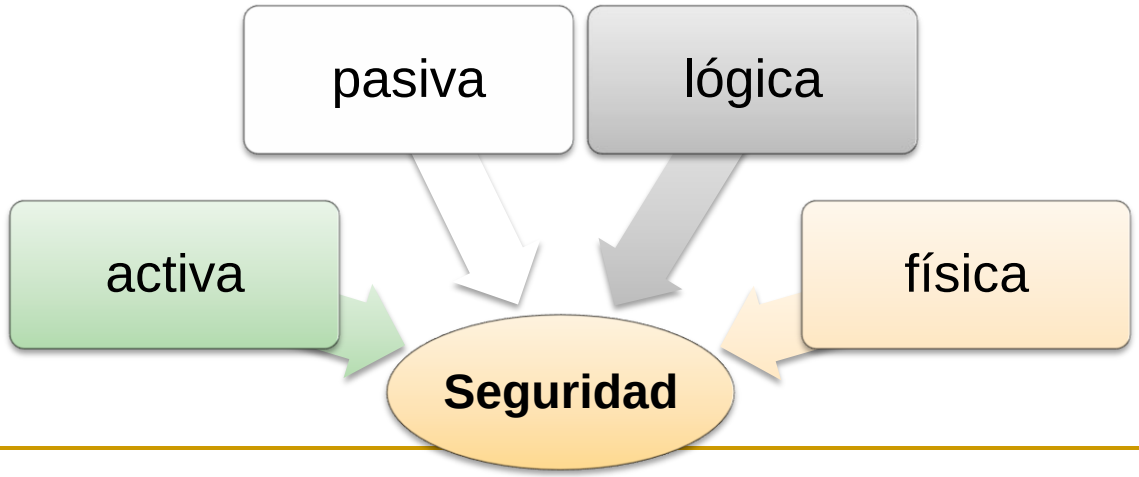
Existen distintos niveles de disponibilidad del sistema, según el tiempo aproximado de tiempo en inactividad por año se determina el porcentaje de disponibilidad. El mayor nivel de exigencia de alta disponibilidad acepta 5 minutos de inactividad al año, con lo que se obtiene una disponibilidad de 5 nueves: 99,999%.

Como ejemplos de sistemas y servicios de alta disponibilidad podemos mencionar sistemas sanitarios, control aéreo, de comercio electrónico, bancarios, transporte marítimo, militares, etc., donde la pérdida o interrupción de conectividad pueden suponer graves consecuencias personales y económicas.

Clasificación de la seguridad

Se pueden hacer diversas clasificaciones de la seguridad informática en función de distintos criterios.

Según el activo a proteger, es decir, *todos los recursos del sistema de información necesarios para el correcto funcionamiento de la actividad de la empresa*, distinguiremos entre **seguridad física y lógica** (con independencia del momento preciso de actuación), entre **seguridad pasiva y activa** , según se actúe antes de producirse el percance, de tal manera que se eviten los daños en el sistema, o después del percance, minimizando los efectos ocasionados por el mismo.



Clasificación de la seguridad

Seguridad física y lógica

En este apartado distinguiremos los distintos tipos de seguridad en función del recurso del sistema de información que a de protegerse.

Seguridad Física

Habitualmente nos centramos en protegernos de posibles hackers, virus… y nos olvidamos de un aspecto muy importante en la seguridad informática, la **seguridad física**.

La seguridad física es aquella que trata de proteger el hardware (los equipos informáticos, el cableado…) de los posibles desastres naturales (terremotos, tifones…), de incendios, inundaciones, sobrecargas eléctricas, de robos y un sinfín de amenazas más.

*A continuación vamos a enumerar las principales **amenazas** y los **mecanismos** para salvaguardarnos de las mismas:*

Clasificación de la seguridad

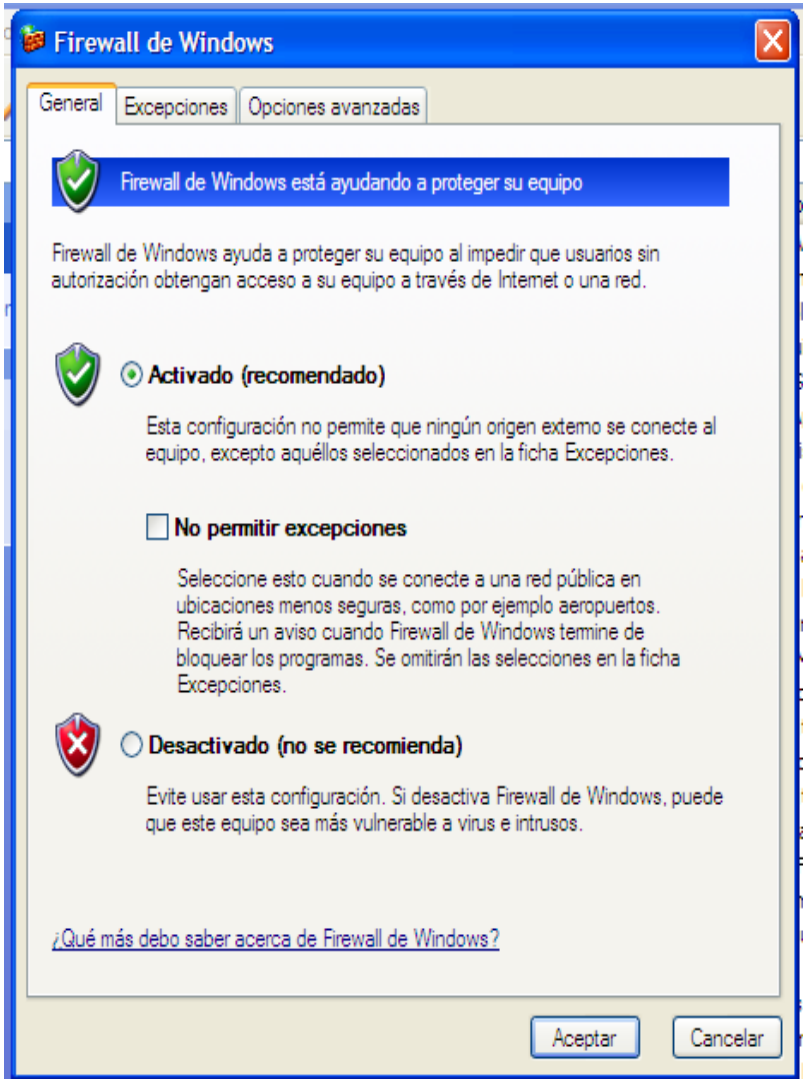
Amenazas	Mecanismos de defensa
Incendios	• El mobiliario de los centros de cálculo debe ser ignífugo. • Evitar la localización del centro de procesamiento de datos cerca de zonas donde se manejen o almacenen sustancias inflamables o explosivos. • Deben existir sistemas antiincendios, detectores de humo, rociadores de gas, extintores… para sofocar el incendio en el menor tiempo posible y así evitar que se propague ocasionando numerosas pérdidas materiales.
Inundaciones	• Evitar la ubicación de los centros de cálculo en las plantas bajas de los edificios para protegerse de la entrada de aguas superficiales. • Impermeabilizar las paredes y techos del Centro de Cálculo. Sellar las puertas para evitar la entrada de agua proveniente de las plantas superiores.
Robos	• Proteger los centros de cálculo mediante puertas con medidas biométricas, cámaras de seguridad, vigilantes jurados…, con todas estas medidas pretendemos evitar la entrada de personal no autorizado.
Señales Electromagnéticas	• Evitar la ubicación de los centros de cálculo próximos a lugares con gran radiación de señales electromagnéticas, pues pueden interferir en el correcto funcionamiento de los equipos informáticos del cableado de red. • En caso de no poder evitar la ubicación en zonas con grandes emisiones de este tipo de señales deberemos proteger el centro frente de dichas emisiones mediante el uso de filtros o de cableado especial, o si es posible, utilizar fibra óptica, que no es sensible a este tipo de interferencias.
Apagones	• Para evitar los apagones colocaremos Sistemas de Alimentación Ininterrumpida (SAI), que proporcionan corriente eléctrica durante un periodo de tiempo suficiente.
Sobrecargas Eléctricas	• Además de proporcionar alimentación, los SAI profesionales incorporan filtros para evitar picos de tensión, es decir, estabilizan la señal eléctrica.
Desastres Naturales	• Estando en continuo contacto con el Instituto Geográfico Nacional y de Meteorología, organismos que informan sobre los movimientos sísmicos y meteorológicos en España.

Clasificación de la seguridad

Seguridad Lógica

La seguridad lógica complementa a la seguridad física, protegiendo el software de los equipos informáticos, es decir, las aplicaciones y los datos de usuario, de robos, de pérdidas de datos, entrada de virus informáticos, modificaciones no autorizadas de los datos, ataques desde la red, etc.

A continuación vamos a enumerar las principales ***amenazas*** y ***mecanismos*** para salvaguardarnos de los mismos:



Clasificación de la seguridad

Amenazas	Mecanismos de defensa
Robos	• Cifrar la información almacenada en los soportes para que en caso de robo no sea legible. • Utilizar contraseñas para evitar el acceso a la información. • Sistemas biométricos (uso de huella dactilar, tarjetas identificadoras, caligrafía…).
Pérdida de Información	• Realizar copias de seguridad para poder restaurar la información perdida. • Uso de sistemas tolerantes a fallos, elección del sistema de ficheros del sistema operativo adecuado. • Uso de conjunto de discos redundantes, protege contra la pérdida de datos y proporciona la recuperación de los datos en tiempo real.
Pérdida de integridad en la información	• Uso de programas de chequeo del equipo, SiSoft Sandra 2000, TuneUp… • Mediante la firma digital en el envío de información a través de mensajes enviados por la red. • Uso de la instrucción del SO Windows, sfc (System file checker).
Entrada de Virus	• Uso de antivirus, que evite que se infecten los equipos con programas malintencionados.
Ataques desde la red	• Firewall, autorizando y auditando las conexiones permitidas. • Programas de monitorización. • Servidores Proxys, autorizando y auditando las conexiones permitidas.
Modificaciones no autorizadas	• Uso de contraseñas que no permitan el acceso a la información. • Uso de listas de control de acceso. • Cifrar documentos.

Clasificación de la seguridad

Seguridad activa y pasiva

Aquí el criterio de clasificación es el momento en el que se ponen en marcha las medidas oportunas de actuación.

Seguridad Activa.-

La **seguridad activa** la podemos definir como el conjunto de medidas que previenen e ***intentan evitar los daños*** en los sistemas informáticos.

A continuación, vamos a enumerar las principales técnicas de seguridad activa:

Clasificación de la seguridad

Técnicas	¿Qué previene?
Uso de Contraseñas	Previene el acceso a recursos por parte de personas no autorizadas.
Listas de control de acceso	Previene el acceso a los ficheros por parte de personas no autorizadas.
Encriptación	Evitan que personas sin autorización pueden interpretar la información.
Uso de software de seguridad informática	Previene de virus informáticos y de entradas indeseadas al sistema informático.
Firmas y certificados digitales	Permite comprobar la procedencia, autenticidad e integridad de los mensajes.
Sistemas de ficheros con tolerancia a fallos	Previene fallos de integridad en caso de apagones de sincronización o comunicación.
Cuotas de disco	Previene que ciertos usuarios hagan un uso indebido de la capacidad de disco.

Las tarjetas inteligentes, es un ejemplo de seguridad activa, impiden el acceso a personas no autorizadas a los recursos.

Clasificación de la seguridad

Seguridad Pasiva.-

La seguridad pasiva complementa a la seguridad activa y se encarga de minimizar los efectos que haya ocasionado algún percance.

A continuación enumeraros las técnicas más importantes de seguridad pasiva:

Técnicas	¿Cómo minimiza?
Conjunto de discos redundantes	Podemos restaurar información que no es válida ni consistente.
SAI	Una vez que la corriente se pierde las baterías del SAI (sistemas de alimentación ininterrumpida) se ponen en funcionamiento proporcionando la corriente necesaria para mantener los equipos encendidos el tiempo necesario para guardar la información una vez que se ha producido el desastre (el apagón de la luz).
Realización de copias de seguridad	A partir de las copias realizadas, podemos recuperar información en caso de pérdida de datos.

Amenazas

Las amenazas a un sistema informático puede provenir desde un hacker remoto que entra en nuestro sistema con un troyano, pasando por un programa descargado gratuitamente que nos ayuda a gestionar nuestras fotos, pero que supone una puerta trasera a nuestro sistema permitiendo la entrada a espías, hasta la entrada no deseada al sistema mediante contraseñas de bajo nivel de seguridad.

El objetivo final de la seguridad es proteger lo que la empresa posee. Todo aquello que es propiedad de la empresa se denomina activo. Un activo es tanto el mobiliario de la oficina (sillas, mesas, estanterías), como los equipos informáticos (servidores, ordenadores, impresoras), como los datos que se manejan (datos de clientes, facturas, personal).

Cualquier daño que se produzca sobre estos activos tendrá un impacto en la empresa y supone una amenaza.

Amenazas

La seguridad de un sistema real nunca será completa, pero el uso de buenas políticas de seguridad es imprescindible para evitar y minimizar los daños.

> *Una **vulnerabilidad** es cualquier fallo que compromete la seguridad del sistema.*
>
> *Un **riesgo** es la posibilidad de que se produzca un impacto negativo para la empresa aprovechando alguna de sus vulnerabilidades.*

Actuaciones para mejorar la seguridad

Los pasos a seguir para mejorar la seguridad son los siguientes:

- ***Identificar los activos***, es decir, los elementos que la empresa quiere proteger.

Amenazas

- ***Evitar los riesgos***, considerando el impacto que pueden tener la perdida de los datos sobre los activos del sistema.

- ***Diseñar el plan de actuación***, que debe incluir:

*Las medidas que traten de minimizar el impacto de los daños ya producidos. Es lo que hemos estudiado referido a la **seguridad pasiva**.*

*Las medidas que traten de prevenir los daños minimizando la existencia de vulnerabilidades. Se trata de la **seguridad activa**.*

- ***Revisar periódicamente*** las medidas de seguridad adoptadas.

Amenazas

Vulnerabilidades

Las vulnerabilidades de un sistema ***son una puerta abierta para posibles ataques***, de ahí que sea tan importante tenerlas en cuenta-en cualquier momento podrían ser aprovechadas-.

Podemos diferenciar tres tipos de vulnerabilidades según *cómo afectan a nuestro sistema*:

Vulnerabilidades ya conocidas sobre aplicaciones o sistemas instalados. Son vulnerabilidades de las que ya tienen conocimiento las empresas que desarrollan el programa o sistema al que afecta, y para las cuales, ya existe una solución, que se publica en forma de parche y actuación explítica.

Existen mecanismos de información, por ejemplo, listas de correo relacionadas con las noticias oficiales de seguridad, que informan de la detección de esas vulnerabilidades y las publicaciones de los parcheas a las que podemos suscribirnos.

Amenazas

Vulnerabilidades

Vulnerabilidades conocidas sobre aplicaciones no instaladas. Estas vulnerabilidades también son conocidas por las empresas desarrolladoras de la aplicación, pero puesto que nosotros no tenemos dicha aplicación instalada no tendremos que actuar.

Vulnerabilidades aún no conocidas. *Estas vulnerabilidades aún no han sido detectadas por la empresa que ha desarrollado en programa, sistema ..etc, que podemos tener instalado, por lo que, si otra persona ajena a dicha empresa detectara alguna, podría utilizarla contra todos los equipos que tienen instalado este sw.*

Amenazas

Vulnerabilidades

Lograr que los sistemas y redes operen con seguridad resulta primordial para cualquier empresa y organismo. Esto ha llevado a que empresas como Microsoft dispongan de departamentos dedicados exclusivamente a la seguridad, como es **Microsoft Security Response Center (MSRC).**

Sus funciones son, entre otras, *evaluar los informes que los clientes proporcionan sobre posibles vulnerabilidades en sus productos, y preparar y divulgar revisiones y boletines de seguridad que respondan a estos informes*.

Amenazas

Vulnerabilidades

Para ello clasifica las vulnerabilidades en función de su gravedad, lo que nos da una idea de los efectos que pueden tener en los sistemas.

En la siguiente tabla puedes ver dicha clasificación:

Codificación	Definición
Crítica	Vulnerabilidad que puede permitir la propagación de un gusano de Internet sin la acción del usuario.
Importante	Vulnerabilidad que puede poner en peligro la confidencialidad, integridad o disponibilidad de los datos de los usuarios, o bien, la integridad o disponibilidad de los recursos de procesamiento.
Moderada	El impacto se puede reducir en gran medida a partir de factores como configuraciones predeterminadas, auditorías o la dificultad intrínseca en sacar partido a la vulnerabilidad.
Baja	Vulnerabilidad muy difícil de aprovechar o cuyo impacto es mínimo.

Amenazas

Tipos de amenazas

Un sistema informático se ve expuesto a un gran número de amenazas y ataques. En este apartado veremos una pequeña introducción a las clasificaciones más importantes.

Para identificar las amenazas a las que está expuesto un sistema informático realizaremos tres clasificaciones.

- ***Según los tipos de atacantes****: recoge, en la primera columna, los nombres con los que se han denominado a las personas que llevan a acabo los ataques, y en la segunda columna, una pequeña definición que los caracteriza*.

Amenazas

Tipos de amenazas

Codificación	Definición
Hackers	Expertos informáticos con una gran curiosidad por descubrir las vulnerabilidades de los sistemas pero sin motivación económica o dañina.
Crackers	Un hackers que, cuando rompe la seguridad de un sistema, lo hace con intención maliciosa, bien para dañarlo o para obtener un beneficio económico.
Phreakers	Crackers telefónicos, que sabotean las redes de telefonía para conseguir llamadas gratuitas.
Sniffers	Expertos en redes que analizan el tráfico para obtener información extrayéndola de los paquetes que se transmiten por la red.
Lammers	Chicos jóvenes sin grandes conocimientos en informática pero que se consideran a sí mismos hackers y se vanaglorian de ellos.
Newbie	Hacker novato.
Ciber terrorista	Expertos en informática e intrusiones en la red que trabajan para países y organizaciones como espías y saboteadores informáticos.
Programadores de virus	Expertos en programación, redes y sistemas que crean programas dañinos que producen efectos no deseados en los sistemas o aplicaciones.
Carders	Personas que se dedican al ataque de los sistemas de tarjetas, como los cajeros automáticos.

Amenazas

Tipos de amenazas

- ***Según los tipos de ataque:*** *se recogen los principales ataques que puede sufrir un sistema, si se aprovechan sus vulnerabilidades.*

Codificación	Definición
Interrupción	Un recurso del sistema o la red deja de estar disponible debido a un ataque.
Intercepción	Un intruso accede a la información de nuestro equipo o a la que enviamos por la red.
Modificación	La información ha sido modificada sin autorización, por lo que ya no es válida.
Fabricación	Se crea un producto (por ejemplo una página Web) difícil de distinguir del auténtico y que puede utilizarse para hacerse, por ejemplo, con información confidencial del usuario.

Amenazas

Tipos de amenazas

❑ ***Según cómo actúan estos atacantes***:

Codificación	Definición
Spoofing	Suplanta la identidad de un PC o algún dato del mismo (como su dirección MAC).
Sniffing	Monitoriza y analiza el tráfico de la red para hacerse con información.
Conexión no autorizada	Se buscan agujeros de la seguridad de un equipo o un servidor, y cuando se descubren, se realiza una conexión no autorizada a los mismos.
Malware	Se introducen programas malintencionados (virus, troyanos o gusanos) en nuestro equipo, dañando el sistema de múltiples formas.
Keyloggers	Se utiliza una herramienta que permite conocer todo lo que el usuario escribe a través del teclado, e incluso pueden realizar capturas de pantallas.
Denegación de Servicio	Interrumpen el servicio que se está ofreciendo en servidores o redes de ordenadores. También denominado DoS (denial of Service).
Ingeniería social	Se obtiene información confidencial de una persona u organismo para utilizarla con fines maliciosos. Los ejemplos más llamativos son el phishing y el spam.
Phishing	Se engaña al usuario para obtener su información confidencial suplantando la identidad de un organismo o páginas Web de Internet.
Spam	Correo o mensaje basura, no solicitado, no deseados o de remitente no conocido.
Pharming	Redirigir un nombre de dominio a otra máquina distinta falsificada y fraudulenta.
Password cracking	Descifrar contraseñas de sistemas y comunicaciones. Los métodos más comunes son mediante sniffing, observando directamente la introdución de credenciales (shoulder surfing), ataque por fuerza bruta.
Botnet	Conjunto de robots informáticos o bots, que se ejecutan de manera autónoma en multitud de host, para controlarlos de forma remota.

Auditoria Informática

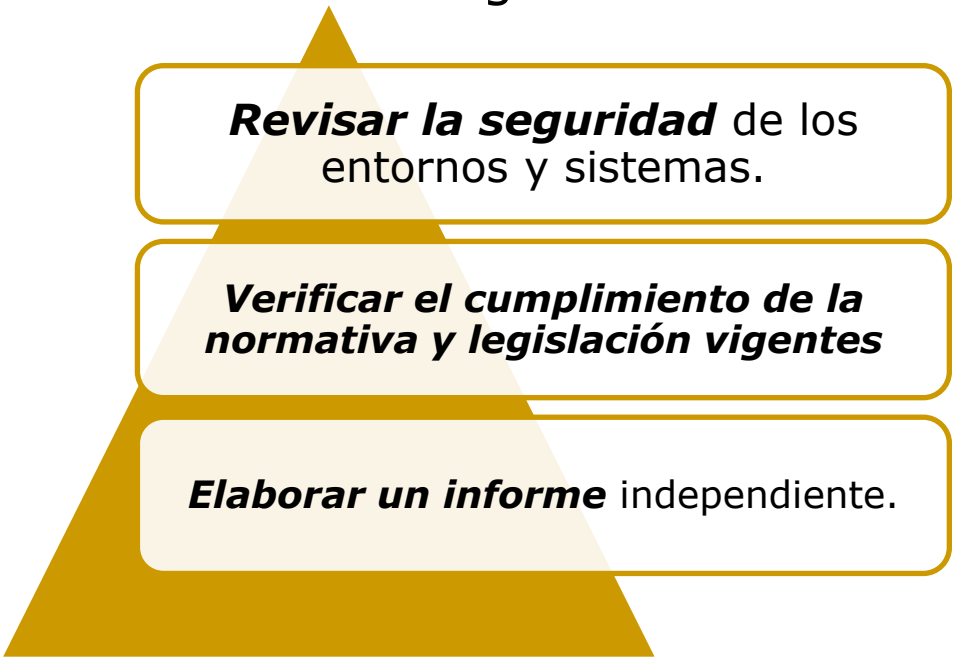
Una auditoría de seguridad informática o auditoría de seguridad de sistemas de información (SI) es el estudio que comprende el ***análisis y gestión de sistemas para identificar y posteriormente corregir las diversas vulnerabilidades*** que pudieran presentarse en una revisión exhaustiva de las estaciones de trabajo, redes de comunicaciones o servidores.

Una vez obtenidos ***los resultados, se detallan, archivan y reportan a los responsables quienes deberán establecer medidas preventivas de refuerzo***, siguiendo siempre un proceso secuencial que permita a los administradores mejorar la seguridad de sus sistemas aprendiendo de los errores cometidos con anterioridad.

Auditoria Informática

Las auditorías de seguridad de SI permiten conocer, en el momento de su realización, cuál es ***la situación exacta de sus activos de información*** en cuanto a ***protección, .control y medidas de seguridad***.

Los objetivos de una auditoría de seguridad de los sistemas de información son:



Auditoria Informática

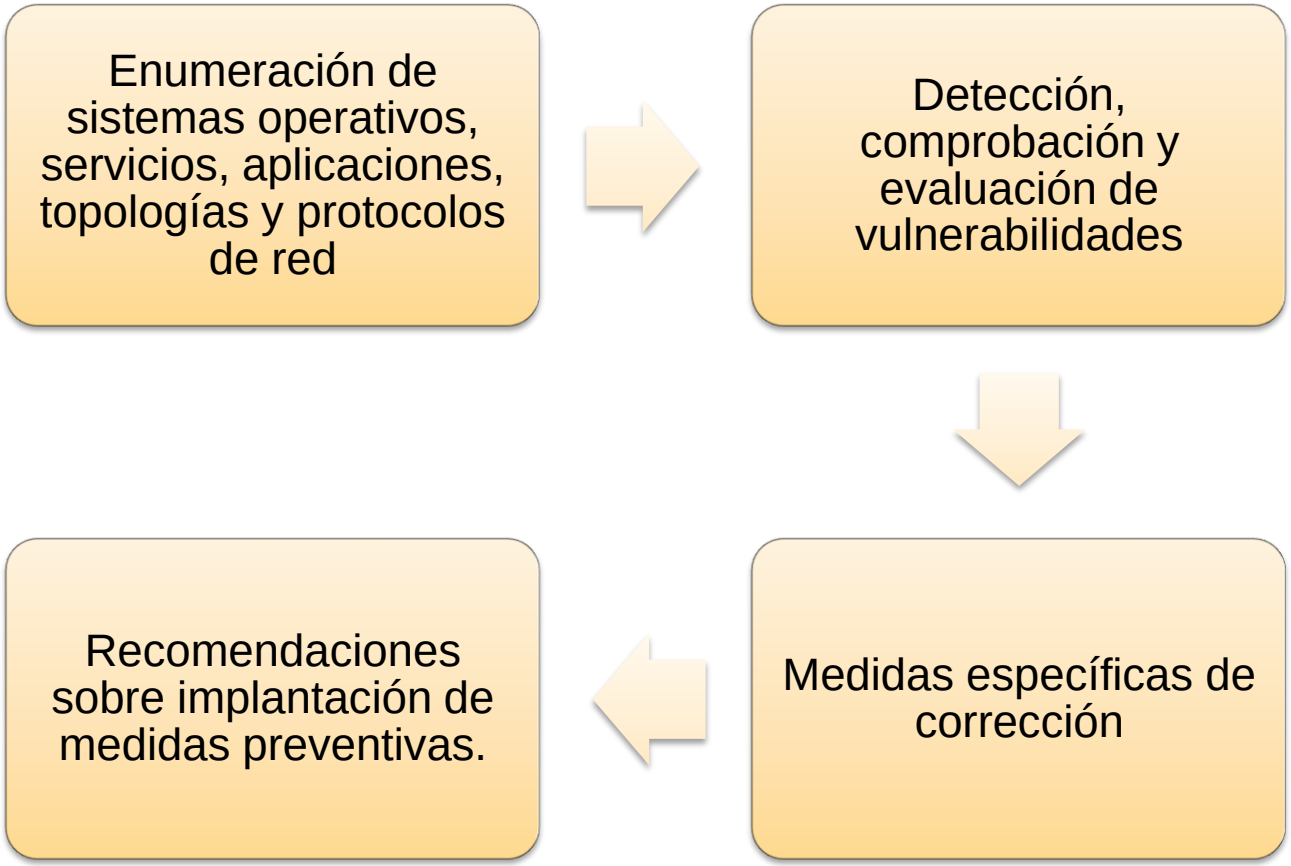
- *Una auditoría se realiza con base a un patrón o conjunto de directrices o buenas prácticas sugeridas*.

- Existen estándares orientados a servir como base para auditorías de informática:

  - ***COBIT (Objetivos de Control de las Tecnologías de la Información).***
  - ***estándar ISO 27002***, el cual se conforma como un código internacional de buenas prácticas de seguridad de la información, éste puede constituirse como una directriz de auditoría apoyándose de otros estándares de seguridad de la información que definen los requisitos de auditoría y sistemas de gestión de seguridad, como lo es el estándar ***ISO 27001***.

Auditoria Informática

Los servicios de auditoría constan de las siguientes fases:



Auditoria Informática

Tipos de auditoría

- ***Auditoría de seguridad interna:*** se contrasta el nivel de seguridad de las redes locales y corporativas de carácter interno.

- ***Auditoría de seguridad perimetral:*** se estudia el perímetro de la red local o corporativa, conectado a redes públicas.

- ***Test de intrusión:*** se intenta acceder a los sistemas, para comprobar el nivel de resistencia a la intrusión no deseada.

Auditoria Informática

Tipos de auditoría

- ***Análisis forense:*** análisis posterior de incidentes *(recogida de evidencias del sistema de información)*, mediante el cual se trata de reconstruir cómo se ha penetrado en el sistema, a la par que se valoran los daños ocasionados. Si los daños han provocado la inoperatividad del sistema, se denomina análisis post mórtem.

- ***Auditoría de código de aplicaciones:*** análisis del código independientemente del lenguaje empleado, un ejemplo concreto y frecuente se realiza con los sitios web, mediante el análisis externo de la web, comprobando vulnerabilidades *como la inyección de código SQL*, *Cross Site Scripting,* etc.

Resumen

Hablar hoy en día de un sistema informático totalmente seguro es imposible, la conectividad global permite extender el campo de posibles amenazas. Aunque éstas provienen de distintos ámbitos: *personas (personal de una organización, hackers y crackers en red), amenazas lógicas (malware y exploits sobre vulnerabilidades de las aplicaciones), así como todo tipo de amenazas físicas como robos o catástrofes (naturales o artificiales como incendios).*

En esta unidad de trabajo se han ***analizado los fundamentos y conceptos para conseguir sistemas y configuraciones fiables, partiendo del principio de garantizar disponibilidad***.

Resumen

Hoy en día se realizan un importante y gran número de operaciones a través de las redes de comunicaciones y la disponibilidad de sus servicios ofrecidos se convierten en ocasiones en algo crítico, pasamos a hablar de alta disponibilidad cuando son necesarias medidas específicas que garanticen la operatividad 24 horas al día, 7 días a la semana, los 365 días al año.

Sobre la disponibilidad de los sistemas se sustentan otros aspectos que se deben perseguir para mejorar la seguridad informática como la confidencialidad, integridad, autenticación y el no repudio.

Resumen

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

Dichas medidas se diferencian en función de qué elemento protegen seguridad física y seguridad lógica, y según sean preventivas (activas) o correctivas después de un incidente (pasivas).

Proyecto: Unidad de trabajo 2.-

Búsqueda de un vector de ataque – Exploración e identificación de las vulnerabilidades de un sistema

Búsqueda de un vector de ataque – Exploración e identificación de las vulnerabilidades de un sistema

Actividad 1.- Análisis de Herramientas

Búsqueda de información con el fin de elaborar un diccionario de herramientas mencionadas en este tema, en el que se describan los siguientes elementos:

- *Descripción,*
- *http de descarga y*
- *http de tutorial/manual de uso,*
- *http de ejemplo de aplicación/uso,*
- *Herramientas relacionadas.*
- *Otras cuestiones*

Búsqueda de un vector de ataque – Exploración e identificación de las vulnerabilidades de un sistema

Actividad 2.- Análisis de la distribución KALI

Describe someramente la distribución Kali:

Kali Linux es una distribución basada en Debian GNU/Linux diseñada principalmente para la auditoría y seguridad informática en general. Fue fundada y es mantenida por Offensive Security Ltd. Mati Aharoni and Devon Kearns, ambos pertenecientes al equipo de Offensive Security, desarrollaron la distribución a partir de la reescritura de BackTrack,que se podría denominar como la antecesora de Kali Linux.

Kali Linux trae preinstalados numerosos programas incluyendo Nmap (un escáner de puertos), Wireshark (un sniffer), John the Ripper (Un crackeador de passwords) y la suite Aircrack-ng (Software para pruebas de seguridad en redes inalámbricas). Kali puede ser usada desde un Live CD, live-usb y también puede ser instalada como sistema operativo principal.

Búsqueda de un vector de ataque – Exploración e identificación de las vulnerabilidades de un sistema

Actividad 3.- Preparación de las máquinas virtuales

Objetivo: El objetivo de la práctica es que el alumno prepare las máquinas virtuales necesarias para esta práctica.

1.- Las maquinas virtuales que vamos a utilizar son –instalación básica-:

- Windows Server
- KALI-Linux (distribución LiveCD de seguridad y auditoría informática)

2.- Una vez que tenemos en marcha nuestras máquinas virtuales, el siguiente paso es configurar sus adaptadores de red para que puedan salir a Internet y comunicarse entre sí.

3.- Comprueba que los equipos tienen conexión a Internet y que tienen comunicación entre sí. Para ver si dos equipos tienen comunicación entre sí ejecuta el comando ping <IP>.

Búsqueda de un vector de ataque – Exploración e identificación de las vulnerabilidades de un sistema

Actividad 4.- Metodología de un atacante

Objetivo: El objetivo de la práctica es que el alumno conozca las herramientas y la metodología que utiliza un atacante para entrar en un equipo

Búsqueda de un vector de ataque – Exploración e identificación de las vulnerabilidades de un sistema

Actividad 4.1.- Metodología de un atacante "Explorar e identificar las vulnerabilidades de un sistema"

Para ello el alumnos deberá realizar las siguientes tareas:

Windows Server:

- 4.1.1.- Instalar el programa *MBSA* y obtener las vulnerabilidades del propio sistema.
- 4.1.2.- Instalar el programa *GFI Languard* y obtener las vulnerabilidades del propio sistema.
- 4.1.3.- *Utilizar al menos otra herramienta de análisis de obtención de vulnerabilidades*

Búsqueda de un vector de ataque – Exploración e identificación de las vulnerabilidades de un sistema

Actividad 4.2.- Metodología de un atacante "Obtener información del sistema vulnerable"

Utilizando KALI-Linux se ejecutará un "*Escaneo de puertos, detección de servicios, sistemas operativos..*" *al Windows Server mediante los siguientes comandos/utilidades Sw:*

- 4.2.1.- nmap [opciones] ip_equipo "Windows server"
- 4.2.2.- xprobe2 [opciones] ip_equipo "Windows server"

Nota: *4.2.2.- Se realizará un manual de ambas utilidades Sw*

Búsqueda de un vector de ataque – Exploración e identificación de las vulnerabilidades de un sistema

Actividad 4.3.- Metodología de un atacante "Ataque a un Sistema de Información"

Utilizando KALI-Linux se realizará un ataque *al Windows Server o similar:*

- El FrameWork de **Metasploit** es una herramienta de penetración de código libre, desarrollado para ejecutar exploits a un objetivo remoto. Metasploit cuenta con la mayor base de datos de exploits públicos y probados y puede ser usado para detectar las vulnerabilidades de nuestros sistemas para protegerlos o usar esas vulnerabilidades para obtener acceso a sistemas remotos.

Los pasos básicos a seguir para explotar las vulnerabilidades usando Metasploit son:

- ✓ Elegir y configurar el Exploit (Codigo que permite aprovechar la vulnerabilidad de un sistema)
- ✓ Opcionalmente confirmar si el objetivo es susceptible al exploit elegido
- ✓ Elegir y configurar el Payload (Codigo que se ejecutara una vez explotemos la vulnerabilidad)
- ✓ Ejectutar el Exploit

Para poder elegir un exploit es necesario que contemos con alguna información del sistema remoto, tal como el Sistema operativo y servicios de red instalados. Esto lo podemos obtener con una herramienta de escaneo de puertos y **Fingerprinting** -proceso de recopilación de información que permite identificar el sistema operativo en el ordenador- como Nmap.

Búsqueda de un vector de ataque – Exploración e identificación de las vulnerabilidades de un sistema

- 4.3.1.-Herramienta **MetaSploit** por línea de comando **msfconsole**.

"The **msfconsole** is probably the most popular interface to the Metasploit Framework (MSF)"

Se accederá al servidor/equipo mediante el exploit más adecuado (un exploit posible para su uso Microsoft RPC DCOM MS03-026)

Kali Metasploit Guide
https://www.hackthis.co.uk/articles/a-beginners-guide-to-metasploit
http://www.offensive-security.com/metasploit-unleashed/Using_Exploits
http://www.offensive-security.com/metasploit-unleashed/Msfconsole_Commands

- 4.3.2.-Herramienta **MetaSploit por** frontend o entorno gráfico **Armitage**.

"makes penetration testing easy by adding a GUI to the Metasploit framework"

https://www.dragonjar.org/manual-de-armitage-en-espanol.xhtml

Entre otras acciones -extraer SAM (hashdump), subir/bajar ficheros … , crear un nuevo usuario … , activar la webcam- en definitiva utilizar la potencialidad de estos sw.

Búsqueda de un vector de ataque – Exploración e identificación de las vulnerabilidades de un sistema

Formato de entrega:

Documento en formato xhtml 1.0, por grupos, ***con enlaces a elementos multimedia elaborados por el alumno****, que resuelvan las cuestiones planteadas, detallen el proceso de la actividad 1,2,3 y que el resultado sea base para cualquier usuario que quiera introducirse en el mundo de la vulnerabilidad de sistemas.*

Posibles aplicaciones, programas y herramientas: MBSA, GFI Languard, nmap, xprobe2, MetaSploit, Armitage … y los que consideres aunque den el mismo resultado.