Documentación de apoyo a la preparación de la oposición al Cuerpo General Administrativo de la Administración del Estado, especialidad Estadística

Módulo 5: Tecnologías de la información y de las comunicaciones

Segunda parte

ÍNDICE

Unidad 22: Sistemas operativos. Sistema Windows. Archivos ejecutables. Extensión de un archivo. Archivos ocultos. Gestión de archivos, carpetas y discos. Opciones de carpeta. Compresión de archivos y carpetas. Tipos de redes. Redes de área local. Usuarios y grupos. Permisos. Seguridad: los programas maliciosos; tipos; formas de entrada; contramedidas.

Unidad 22: Sistemas operativos. Sistema Windows. Archivos ejecutables. Extensión de un archivo. Archivos ocultos. Gestión de archivos, carpetas y discos. Opciones de carpeta. Compresión de archivos y carpetas. Tipos de redes. Redes de área local. Usuarios y grupos. Permisos. Seguridad: los programas maliciosos; tipos; formas de entrada; contramedidas.

Introducción y objetivos

La presente unidad se estructura en cinco partes:

Una primera parte de la descripción de lo que es un **sistema operativo**, de su definición y de sus características.

En una segunda parte se hablará del sistema operativo más difundido, **Windows**. Se comentarán aspectos generales relativos al sistema de ficheros donde se guarda la información.

En la tercera parte se dará una breve pincelada **a los tipos de redes** y en particular a las redes de área local.

En la cuarta parte se describirán los conceptos de **usuarios, grupos y permisos**.

La quinta y última parte se detallarán aspectos muy importantes de **seguridad de la información**. Aspectos que ayudarán a formar y concienciar al lector y que redunde en una reducción de los riesgos que hoy en día tenemos y a los que estamos expuestos.

El **objetivo** de esta unidad es proporcionar al lector unos conocimientos teóricos generales sobre los sistemas operativos, los sistemas operativos Windows en particular, las redes y los conceptos más importantes en seguridad de la información.

1 Sistemas Operativos

El Sistema Operativo (SO) lo podemos definir desde dos puntos de vista:

- Desde el punto de vista de los usuarios, visión externa, el sistema operativo actúa como un interfaz entre los programas de aplicación y la máquina pura.

- Desde el punto de vista interno el sistema operativo puede concebirse como un gestor de recursos

Un sistema informático puede describirse mediante un modelo de capas, cada capa representa subir un escalón en el nivel de abstracción con el que describimos el sistema y reducir la complejidad que percibe el usuario. Los sistemas operativos estrían entre la capa física y las aplicaciones:

Usuarios
Programas de aplicación
SISTEMAS OPERATIVOS
Dispositivos Físicos: hardware

Hay que tener en cuenta que los primeros ordenadores de la historia no tenían sistema operativo, no tenía esa capa entre hardware y aplicaciones. Por este motivo, cada aplicación necesitaba una detallada especificación del hardware sobre el que estaba, para ejecutarse correctamente y desarrollar sus propios drivers para cualquier dispositivo periférico como impresoras o discos. El incremento de la complejidad del hardware y los programas de aplicaciones hicieron del sistema operativo algo imprescindible.

Otro aspecto es determinar lo que realmente forma parte del sistema operativo y lo que realmente no, ya que en la actualidad los SO vienen con gran cantidad de aplicaciones que no forman parte del sistema. El Kernel o Núcleo es una pieza fundamental en cualquier sistema operativo. Ya tengas Windows, macOS o GNU/Linux, todos ellos tienen su propio núcleo que se encarga de que el software y el hardware de cualquier ordenador trabajen juntos. La visión más restrictiva considera Sistema Operativo exclusivamente el kernel, esto es, el Núcleo que corre constantemente en modo protegido o supervisor; tiene acceso a todas las operaciones de bajo nivel sobre los recursos hardware. El modo usuario sólo puede acceder a estos recursos a través de llamadas al sistema que se ejecutarán en modo supervisor. Por tanto, cualquier programa que requiriese usar los servicios del kernel no podría considerarse parte del sistema operativo. Otra visión considera el sistema operativo formado por el software que funciona en modo supervisor y por los programas del sistema.

Desde la visión de que los sistemas operativos son gestores de recursos, las áreas que gestionan son:

1. **Gestión de procesos**: gestionan los procesos que llegan a la CPU usando técnicas como la multiprogramación.
2. **Gestión de memoria principal**: también relacionada con la multiprogramación, ya que cada proceso necesita espacio en memoria para código y datos.
3. **Gestión de memoria secundaria (disco)**: Es necesaria en los procesos que no contienen espacio suficiente en memoria principal. La memoria secundaria también albergará los datos de los usuarios (no solo de los procesos) por lo que se necesitará un gestor de archivos.
4. **Gestión de Entrada/Salida**: para gestionar las interrupciones para reclamar la atención de la CPU.
5. **Llamadas al sistema y la API**: las llamadas al sistema constituyen la forma en que el sistema operativo pone sus servicios de gestión de procesos, memoria, ficheros o entrada/salida a disposición de los programas de aplicación. Están estrechamente relacionadas con las funciones de cada sistema operativo, ya que para cada una de estas existe su similar como llamada al sistema. Las funciones de la librería estándar constituyen la interfaz de programación de aplicaciones (API) de cada sistema operativo.

Existen múltiples formas de clasificar los sistemas operativos, aunque hay una serie de características básicas que los definen:

En función de cómo administran las aplicaciones

- **Monotarea**: solamente permite ejecutar un proceso en un momento dado. Una vez que empieza a ejecutar un proceso, continuará haciéndolo hasta su finalización o interrupción.
- **Multitarea**: es capaz de ejecutar varios procesos al mismo tiempo. Este tipo de sistemas operativos suelen asignar los recursos (CPU, memoria, periféricos) de forma alternada a los procesos que los solicitan, de manera que el usuario percibe que todos funcionan a la vez, de forma concurrente.

En función del número de usuarios:

- **Monousuario**: sólo atiende a un usuario al mismo tiempo.
- **Multiusuario**: es capaz de gestionar varios usuarios al mismo tiempo y estos pueden ejecutar simultáneamente sus programas, accediendo a la vez a los recursos del hardware. Esta capacidad requiere una mayor complejidad de los sistemas operativos para que el uso compartido de los recursos no genere bloqueos o incongruencia en los datos.

En función de cómo es capaz de manejar diferentes recursos hardware:

- **Centralizado**: solo es capaz de usar los recursos de una máquina.
- **Distribuido**: permite utilizar los recursos (memoria, CPU, disco, periféricos...) de más de una máquina al mismo tiempo.

Son muchas las familias de sistemas operativos y muchas las formas de clasificarlos (y no son mutuamente excluyentes estas clasificaciones). Se exponen a continuación las más relevantes y que nos ayudarán a diferenciarlos:

Sistemas operativos según su propósito:

- Sistemas operativos de Mainframe: para tareas que requieren un procesamiento masivo de trabajos. Ejemplo los IBM OS/390
- Sistemas operativos de servidor: para tener alta capacidad de atender múltiples peticiones de usuarios a través de la red. Ejemplos Unix, Linux o los Windows Server.
- Sistemas operativos de PC: Tienen mejores prestaciones en la interfaz gráfica de usuario para atender al usuario. Ejemplo: Linux, Mac y Windows
- Sistemas operativos de tiempo real, que controlan procesos industriales, robots, armas, etc..
- Sistemas operativos empotrados: básicamente para electrodomésticos, vehículos o pequeños equipos de comunicaciones: como el IOS de Cisco de los enrutadores.
- Sistemas operativos de dispositivos móviles: como son Android, Windows Mobile o Symbian OS

Sistemas operativos según el número de procesadores que controlan:

- Sistemas operativos monoprocesador: como son MS-DOS y los Mac OS
- Sistemas operativos multiprocesador: que controla varias CPUs (no confundirlo con los sistemas distribuidos, que son CPUs en entidades físicas separadas).

Sistema Operativo según su relación con el entorno:

- Sistemas operativos aislados: que están en desuso
- Sistemas operativos en red: que tienen capacidad para comunicarse con otros Sistemas operativos manteniéndose como sistemas autónomos independientes y comunicándose la red.
- Sistemas operativos distribuidos: integran recursos y el usuario los ve como una sola máquina virtual donde no tiene que saber la ubicación de los recursos.

Sistemas operativos según los servicios que ofrece:

- Por el nº de usuarios:
  - Monousuario: solo un usuario a la vez. Ejemplos: Windows 98 y Mac OS
  - Multiusuario: más de un usuarios a la vez. Unix, Windows 10, etc..
- Por el nº de tareas:
  - Monotarea: una sola tarea a la vez por usuario: Windows 3.x y 95
  - Multitarea: Unix y derivados, Windows 10, 7
- Por el nº de procesadores:
  - Sistemas operativos monoprocesador: como son MS-DOS y los Mac OS
  - Sistemas operativos multiprocesador: que controla varias CPUs (no confundirlo con los sistemas distribuidos, que son CPUs en entidades físicas separadas).

Ejemplos de familias más relevantes de Sistemas Operativos

- **Windows**: Sistema operativo creado por Microsoft, que se puede considerar el más difundo en el mundo de los PC personales. Hablaremos más adelante de este sistema operativo.
- **macOS**: (previamente se llamó Mac OS X, luego OS X) Creado por Apple para su línea de ordenadores Macintosh, es el segundo sistema operativo más usado en ordenadores de sobremesa después de Windows.
- **GNU/Linux** (también conocido informalmente como Linux): es la combinación de varios proyectos, entre los cuales destacan GNU (encabezado por Richard Stallman) y el núcleo Linux (encabezado por Linus Torvalds). Su desarrollo es uno de los ejemplos más importantes del software libre: todo su código fuente puede ser utilizado, modificado y redistribuido libremente, bajo los términos de la GPL (Licencia Pública General de GNU) y otras licencias libres. Partiendo del Kernel de Linus Torvalds, hay múltiples distribuciones diferentes (o sabores) de Linux, entre las más populares están: Debian, Ubuntu, Arch Linux o Red Hat
- **Android** es un sistema operativos desarrollado por Google para los dispositivos móviles, se puede considerar el más popular. Android usa gran parte del Kernel de Linux, por lo que en muchos ámbitos se puede considerar una distribución más de Linux adaptada a dispositivos móviles.
- **iOS** es un sistema operativo para dispositivos móviles creado por la multinacional Apple Inc. Originalmente fue desarrollado para el dispositivos móvil iPhone, pero después se ha usado en dispositivos como el iPod touch, el iPad y el Apple TV.

- **Windows Phone** (abreviado WP) fue el sistema operativo móvil desarrollado por Microsoft, como sucesor de Windows Mobile. Competía directamente contra Android de Google e iOS de Apple. Debido a la fragmentación de sus sistemas operativos, Microsoft dio de baja a Windows Phone, para enfocarse en un único sistema más versátil denominado Windows 10 Mobile.
- **Unix**: aunque la lista de sistemas operativos que estamos dando es muy breve, no podemos dejar de nombrar un histórico como es Unix, fue la base de sistemas operativos como Linux o macOS. Unix fue desarrollado en 1969 por un grupo de empleados de los laboratorios Bell de AT&T, entre los que figuran Dennis Ritchie, Ken Thompson y Douglas McIlroy. A lo largo de la historia de Unix han surgido una gran multitud de implementaciones comerciales de Unix, las más importantes son:
    - **Solaris** de Sun Microsystems. Uno de los sistemas operativos Unix más difundidos en el entorno empresarial y popular por su gran estabilidad, por lo que es muy apropiado en grandes servidores.
    - **AIX** de IBM, con cierta herencia del mainframe en campos como la virtualización.
    - **HP-UX** de Hewlett-Packard. Este sistema operativo nació ligado a las computadoras departamentales de HP y es un sistema operativo muy estable y apropiado para servidores.

2. Sistemas Windows

El sistema operativo Microsoft Windows, conocido popularmente como Windows, hace referencia a toda una familia de sistemas operativos desarrollados por la empresa Microsoft Corporation para equipos PC, smartphone, servidores y sistemas empotrados.

Los sistemas Windows pueden funcionar en diferentes arquitecturas hardware, donde son más usados es en las arquitecturas x86 de Intel y la x86-64 de AMD.

Aunque popularmente es conocido como sistema operativo Windows, en realidad no solo es un sistema operativo. Microsoft lleva muchos años comercializando su producto como un Kernel (antiguamente el de MS-DOS y actualmente el de Windows NT) con un montón de aplicaciones incluidas dentro del mismo paquete de Windows: calculadora, block de notas, navegador, el paint, etc. Es decir, que Windows es más una distribución que un sistema operativo.

Windows se comercializa principalmente en tres grande sectores: el de equipos de escritorio, dispositivos móviles y servidores. Aunque tiene una gran variedad de

versiones y distribuciones en cada uno de estos sectores, en los últimos años ha homogenizado sus productos en sus tres últimas versiones:

- **Windows 10** para equipos de escritorio
- **Windows Server 2016** para servidores
- **Windows 10 Mobile** para dispositivos móviles

Para equipos de escritorio, Windows ha tenido muchas distribuciones, pero actualmente solo están soportadas Windows 7 y Windows 8.1 (además de Windows 10). Cualquier versión antigua de Windows no soportada es un peligro para la seguridad de la información que maneja y, por tanto, no debería usarse.

2.1. Archivos ejecutables. Extensión de un archivo. Archivos ocultos.

Para organizar las unidades de disco, los sistemas operativos usan gestores de ficheros que tienen sus propios sistemas de ficheros. Un sistema de ficheros es la organización lógica de un dispositivo de almacenamiento que nos permite almacenar y recuperar información en forma de fichero.

En los ficheros se organiza toda la información, tanto datos como los programas de aplicaciones. El sistema operativo es el encargado de proporcionar que su gestor de ficheros pueda:

- Construir, eliminar archivos y directorios.
- Ofrecer funciones para manipular archivos y directorios.
- Establecer la correspondencia entre archivos y unidades de almacenamiento.
- Realizar copias de seguridad de archivos.

Cada sistema operativo suele organizar los sistemas de ficheros de una forma, por ejemplo:

NTFS, FAT 32, FAT 16 y FAT 12	Windows
ext2, ext3	Linux
NFS	SUN
RFS	ATT

HPFS	OS/2 de IBM
iso9660	CD

Para un usuario puede parecer insignificante pero la organización que tiene detrás cada sistema de archivos es muy diferente y conlleva limitaciones muy diferentes. Por ejemplo, si usamos un sistema de archivos FAT 32 tendremos una limitación en el tamaño de cada archivo de 4 Giga Bytes.

Hoy en día, para dar compatibilidad a los dispositivos removibles, los sistemas operativos son compatibles entre ellos en una gran variedad de sistemas de ficheros. Por ejemplo, la familia de sistemas operativos Windows declara ser compatible con sistemas de ficheros: NTFS, FAT exFAT ISO 9660, UDF, ext2, ext3, ReiserFS, HFS+, FATX y HFS.

Dentro de los sistemas de ficheros se encontrará la información de aplicaciones y datos ordenada en carpetas y archivos a disposición de los usuarios y del propio sistema operativo. Tanto las carpetas como los archivos tendrán una serie de propiedades, las más útiles en los archivos son: el nombre, la fecha de creación, el tipo de archivo y el tamaño que ocupa en la unidad de almacenamiento.

En Windows los archivos son nombrados por una cadena de caracteres seguida por un punto y tres caracteres adicionales. Estos tres últimos caracteres adiciones definen el tipo de archivo y es lo que se conoce como la **extensión de los archivos**.

Windows, que hereda las extensiones de MS-DOS, utiliza la extensión de los archivos para reconocer su formato, por ejemplo para saber si un archivo es ejecutable o solo de texto. Otros sistemas operativos utilizan las extensiones de los archivos por simple convención y, no las usan para determinar el tipo de archivo; este es el caso de los sistemas operativos basados en Unix.

En Windows, un archivo con la extensión ".exe", es un ejemplo de **archivo ejecutable**, esto hace que sea interpretado por el sistema operativo por un archivo que contiene el código de una aplicación ya compilado y preparado para solicitar recursos de la unidad central de proceso (CPU).

Windows, como todos los sistemas operativos, tiene una gran cantidad de extensiones posibles, las más relevantes y heredadas de MS-DOS son:

- Extensiones ejecutables: que continen una aplicación programada por algún tipo de lenguaje de programación, por ejemplo: EXE, COM, BAT, DLL

- Extensiones de datos: contienen información y necesitan una aplicación para poder ser tratados, por ejemplo: TXT, DOC, XLS, RTF

El número de extensiones que puede haber es muy grande, si el lector desea saber más, recomendamos las tablas de la página: https://es.wikipedia.org/wiki/Extensión_de_archivo.

La gran cantidad de tipos de archivos que tiene un sistema operativo puede llegar a ser abrumador para un usuario, mas cuando muchas de las extensiones de los archivos son del propio sistema o propias de aplicativos totalmente desconocidas para el usuario.

Una funcionalidad que permite simplificar la vista del sistema de archivos a los usuarios consiste en ocultar las extensiones que no necesita ver y que no es recomendable que edite o modifique. Esto se conoce como la **ocultación de archivos**.

Desde el Panel de Control de Windows podemos configurar las opciones de las carpetas y hacer que no molesten a los usuarios.

También es posible hacer lo contrario, un usuario avanzado puede necesitar modificar dichas carpetas o archivos.

2.2. Gestión de archivos, carpetas y discos. Opciones de carpeta

El sistema operativo Windows lleva integrada una aplicación que permite navegar por los sistemas de ficheros de todas las unidades de almacenamiento que sean reconocidas por el sistema.

Además, esta aplicación es una herramienta muy útil que permite crear, editar o eliminar carpetas y archivos. De esta forma el Explorador de Windows es la herramienta nativa del sistema operativo Windows para gestionar los archivos y carpetas de nuestros discos o dispositivos.

Las carpetas tambien tienen una serie de propiedades que nos permiten una mejor gestión de las mismas. Desde el propio Explorador de Windows, pulsando en la propiedades de una carpeta, podemos verlas.

También podemos hacer lo mismo con un archivo, pero las propiedades de un archivo son diferentes a las propiedades de las carpetas. Hay una pestaña común que es muy relevante, se trata de la pestaña “Seguridad”.

Mediante las opciones de la pestaña seguridad de las carpetas y los archivos se pueden gestionar los permisos que hay sobre ellos.

Podemos decidir para un usuario o grupo de usuarios que tipos de permisos le damos a una carpeta o archivo determinado. Veremos más adelante estos conceptos.

2.3. Compresión de archivos y carpetas

Las unidades de disco donde están nuestros archivos y carpetas suelen ser un recurso que podemos agotar con facilidad conforme aumentamos el volumen de nuestros datos.

Una forma muy eficaz de mejorar estos recursos de disco es el de comprimir las carpetas y los archivos que tenemos. ¿Qué entendemos por comprimir?

La compresión es una técnica de codificación diferente para hacer que los archivos y carpetas de nuestras unidades ocupen menor espacio, es decir, tengan un tamaño menor. La comprensión se basa en codificar de una forma especial los datos buscando repeticiones o patrones y generando un nuevo archivo que guarda la misma información pero anotando el número de veces que se repiten los patrones en lugar de repetir toda la información.

En algunos casos la información que tratamos de comprimir ya puede llevar algún tipo de comprensión por su naturaleza. Este es el caso de los formatos multimedia, que por su gran tamaño suelen gestionarse directamente con formatos que implican alguna técnica de compresión. Este tipo de archivos pueden ser comprimidos, pero para este caso se usan técnica de comprensión con pérdidas, lo que implica una cierta pérdida de la calidad y la imposibilidad de recuperar totalmente el original. Esto es factible por las características de la información multimedia.

Debemos recordar que la compresión la podemos hacer con técnicas que implican cierta pérdida de información (usada en archivos multimedia) o sin pérdida (cuando es importante volver a la información original al descomprimir).

Para hacer esta operación de compresión se requieren aplicaciones particulares y estas generarán archivos de compresión con extensiones particulares. Las extensiones más populares son ZIP, GZIP, RAR, 7z.

De estas extensiones destacaremos 7z, que es un formato libre y fue creado e implementado por los desarrolladores del programa 7-Zip.

7z que es un formato de compresión de datos sin pérdida, con tasas muy altas que superan a las de los populares formatos ZIP y RAR.

Recomendamos visitar la web https://www.7-zip.org/ para obtener información detallada de este sistema de compresión.

3. TIPOS DE REDES

En este contexto tecnológico, debemos entender por redes a los medios (protocolos, cables, conectores, antenas, etc.) que conectan múltiples ordenadores y que permite que se comuniquen.

Hoy en día no se concibe un equipo informático o un ordenador de sobremesa o un simple dispositivo móvil sin estar conectado a una red. Esta conexión a la red permite aumentar notablemente su funcionalidad y hace que se establezcan flujos de información que incrementa sus capacidades de acceso a múltiples servicios o datos en la nube.

Hay muchos tipos de redes y las podemos clasificar según la distancia de su enlace de la siguiente manera:

Tipo de red	**Distancia**	**Ejemplo**
PAN o WPAN (Redes de Área Personal)	menos de 10 metros	Bluetooth
LAN o WLAN: (Redes de Área local)	Unos 300 metros, menos de 1 km	Ethernet o Wifi
MAN o WMAN (Rede de Área metropolitana)	de unos 10 Km.	DQDB, FDDI, Wimax
WAN (Redes de Área extensa)	más de 100 Km	RDSI, ATM,...

3.1 Red de área local

Las redes de área local (o LAN por su nombre en inglés: Local Área Network) se caracterizan por ser de alta velocidad, para un área de cientos de metros, por realizarse en modo compartido, de bajo coste y alta fiabilidad.
Las dos grandes tecnologías que dominan este sector son Ethernet y Wifi (esta última de forma inalámbrica).

El IEEE (Institute of Electrical and Electronics Engineers) es un organismo que, a través del comité 802, ha estandarizado la mayor parte de las redes LAN existentes. Los

estándares desarrollados por el comité 802 están enfocados a las capas 1 y 2 del modelo de referencia OSI (Interconexión de Sistemas Abiertos). Este comité se divide en subcomités 802.X, cuyo nombre oficial es "Grupos de Trabajo", y se identifican por un número decimal. La mayor parte de estos grupos se dedican a un tipo de red en concreto y su ámbito de actuación cubre tanto la subcapa del nivel de enlace como el nivel físico.

Los grupos de trabajo más importantes en relación a las redes de área local del IEEE y que establece los estándares LAN más usados son:

- **IEEE 802.3** – CSMA / CD (ETHERNET) Define la conexión de redes sobre varios medios, coaxial, par trenzado, fibra óptica.
- **IEEE 802.11** – Redes inalámbricas WLAN. También conocido como WIFI.

Recomendamos la visita de la web http://www.ieee802.org/ para tener con todo detalle los protocolos y las normas de estos estándares que regulan las LAN.

4. USUARIOS Y GRUPOS

Para una correcta gestión o administración de un sistema de información es muy vital tener correctamente definidos los usuarios, los grupos y los permisos que poseen cada uno de estos.

- **Un usuario** suele ser un identificador que identifica a una persona física. Una persona física puede tener múltiples usuarios en un mismo sistema o en múltiples sistemas diferentes y con permisos diferentes. Por motivos de seguridad, para no perder la trazabilidad de las operaciones realizadas, un mismo usuario no debería corresponderse con más de una persona física. También es posible que un usuario no se corresponde con una persona física real, puede ser de una aplicación. De la misma forma (por motivos de seguridad) un mismo usuario no debería corresponderse con diferentes aplicaciones, cada aplicación debe tener su propio usuario en cada sistema.
- **Un grupo** es una agrupación lógica que se suele corresponder con la organización en la que trabaja el sistema de información. Los grupos permiten una gestión conjunta de los usuarios, ya que estos suelen pertenecer a uno o varios grupos. Mediante los grupos se establecen de forma más sencilla los permisos que tienen los usuarios que pertenecen a dicho grupo en un sistema de información dado.

Cada sistema de información o cada sistema operativo tendrán sus propias herramientas o aplicaciones que permite la gestión de los usuarios, los grupos y los permisos establecidos sobre ellos.

Windows, de forma nativa, tiene una aplicación para gestionar usuarios, grupos y permisos de forma local. Se suele acceder a ella desde el panel de control y buscando la administración de cuentas de usuario.

4.1 Permisos

Los permisos definen lo que un usuario o grupo puede hacer o no en un sistema, los privilegios que tiene.

De poco sirve tener muy bien definido los usuarios y los grupos si luego todos tienen permisos para hacer de todo.

Cada usuario debe estar en los grupos en los que por sus funciones en el sistema debería estar y al mismo tiempo cada grupo debe tener establecido los permisos mínimos necesarios para poder cumplir con las funciones del grupo. De esta forma, los usuarios adquirirán los permisos que tiene cada grupo al que pertenecen.

Cuando un usuario cambia de grupo, solo hay que cambiarlo en el administrador de usuarios y de forma automática perderá los permisos del grupo al que ha dejado de pertenecer y adquirirá los nuevos permisos del grupo al que ha sido añadido.

Cuando un grupo adquiere o pierde permisos, solo hay que cambiarlo en el grupo y afectará a todos los usuarios que pertenecen al mismo.

Este tipo de operaciones se suelen hacer de forma gráfica en los gestores de cuentas de usuario y es muy importante que las organizaciones tengas definidos flujos de información entre sistemas diferentes para que los cambios se propaguen de forma automática. Así, cuando un usuario se da de baja en una organización, automáticamente desaparecería de todos los sistemas al mismo tiempo, lo que redunda en una gestión más eficiente y en una mayor seguridad.

Una persona física puede requerir tener diferentes usuarios con un rol muy diferente en un mismo sistema. Por ejemplo: puede ser en algunos momentos un mero usuario del sistema y en otros momentos administrador del mismo. Es muy mala práctica, desde el punto de vista de la seguridad, que un usuario que tiene este doble rol en el sistema siempre trabaje como administrador, lo correcto es que trabaje con los permisos que necesita en cada momento, ya que esto limitará los riesgos ante incidentes.

5. SEGURIDAD

Un ataque informático aprovecha debilidades de los sistemas de información. Estas debilidades se suelen centran en obtener información buscando debilidades en: usuarios, software, hardware, etc.

Muchos ataques informáticos utilizan estrategias orientadas a explotar el eslabón más débil "el factor humano". Para ello utilizan técnicas de Ingeniería Social basadas en el engaño.

Así, en los últimos años, los ciberdelincuentes usan las técnicas de "phishing" (que en castellano lo podríamos traducir como pescar), basadas en lanzar señuelos contra los usuarios de forma que no puedan distinguir fácilmente lo fraudulento de lo legítimo. Una vez consumado el engaño se apropian de sus datos, o lo que es peor, suplantan su identidad para robar información más sensible como sus datos de la tarjeta de crédito.

La mejor medida contra la ingeniería social es la formación y concienciación del usuario de los sistemas de información.

El propósito de los próximos apartados es el de exponer las principales debilidades y buscar un conjunto de posibles contramedidas que ayuden a prevenir o mitigar en lo posible las ciberamenazas.

5.1 Los programas maliciosos y sus tipos

También llamado código malicioso, software malicioso, software malintencionado o malware (MALicious softWARE): Son programas que se instalan en un ordenador sin el consentimiento del usuario y realizan una serie de acciones:

¿QUÉ ACCIONES PUEDEN REALIZAR?

Una o varias de las siguiente acciones:

- El equipo queda fuera de servicio (Denegación de Servicio DoS). Pueden llegar a paralizan servicios industriales.
- Robo de información confidencial.
- Robo de identidad (mediante el robo de credenciales)
- Violación de intimidad mediante la activación de la cámara de videoconferencia de equipos y grabación del usuario
- Violación de intimidad mediante la grabación y posterior envío por mp3 de conversaciones telefónicas realizadas a través de internet (skype,..).
- Secuestro de información con rescate (ransomware que se basan en el cifrado de la información con una clave que se puede conseguir pagando al atacante).
- Alteración y borrado de información (son ataques contra la integridad).

- Espionaje de hábitos de navegación (spyware). Son usados para recabar información de los usuarios.
- Espionaje de datos de ubicación de teléfonos móviles.
- Apertura de ventanas de publicidad no deseada (adware).
- Bloqueo de programas de seguridad (antivirus, cortafuegos...).
- Inclusión en **una "botnet"**. Toma de control del equipo para cometer desde éste acciones ilegales incluyéndolo en redes de zombies/botnets con las implicaciones legales que puede llegar a acarrear. El equipo recibe órdenes desde el centro de control de la botnet.

  Los equipos dentro de una botnet, además de cometer acciones ilegales, pueden convertirse en almacenadores de todo tipo de información, normalmente ilegal.
- Utilización del equipo para lanzar spam de correo.
- Utilización del equipo para dar "clicks" automáticos en páginas diversas y así subir el ranking de páginas y aparecer bien posicionado en redes sociales, buscadores (clicking).
- Simulación de infección del equipo (abriendo alertas de falsos virus) para que el usuario adquiera un falso antivirus para desinfectar (rogueware o scareware).
- Llamada a números de tarificación adicional, suscripciones premium.
- Cambio del servidor de nombres de dominio y alteraciones del fichero etc/hosts.

  Para el ordenador los nombres que escribimos en un navegador "www.ine.es", no significan nada. Necesitan relacionarlos con una dirección de internet (dirección IP). Es necesario relacionar lo que los humanos son capaces de recordar (nombres) y lo que el ordenador es capaz de dirigir (IPs).

  Para realizar esta transformación se utiliza un servicio llamado DNS (Servicio de Nombres de Dominio). El fichero "etc/hosts" también juega un papel en esta función ya que normalmente prevalece a la hora de transformar nombres en IPs, por lo que es objeto de ataques.

  Si un software malicioso es capaz de envenenar nuestras consultas al DNS o modificar nuestro fichero "etc/hosts", puede redirigir nuestra consultas a otra dirección. Un ejemplo típico es el de suplantar las webs de banca electrónica (pharming).
- Cambio de las rutas para enviar las comunicaciones, haciéndolas pasar por servidores intermedios del atacante (Routing Table Scam.)

¿CÓMO SE CLASIFICA EL MALWARE SEGÚN SU CAPACIDAD DE PROPAGARSE?

1.- VIRUS:

Muchas personas llaman virus a cualquier software que infecta un ordenador, pero los virus son solo un tipo específico de malware.

Su nombre se originó por analogía con los virus reales ya que infectan los archivos. Su objetivo principal es alterar el funcionamiento del equipo y propagarse por los ficheros del sistema. Su característica principal es que necesita de la intervención del usuario para ser ejecutado.

Los ficheros infectados generalmente son con extensiones ejecutables: .exe, .src,.com, .bat. También pueden infectar otros archivos, por ejemplo, un virus de Macro infectará programas que utilicen macros, como los que hay en los productos de Microsoft Office.

Los virus se ejecutan cuando se ejecuta el fichero infectado.

Algunos se activan en una fecha concreta.

Cuando están en ejecución, suelen infectar otros ficheros con las mismas características que el fichero anfitrión original.

Si el fichero que infectan se encuentra dentro de un dispositivo extraíble o una unidad de red, cada vez que un nuevo usuario acceda al fichero infectado, su equipo también se verá comprometido.

Si bien los virus fueron los primeros ejemplares de software maliciosos en surgir, actualmente se encuentran en desuso y casi no se encuentran nuevos virus. Es más frecuente otro tipo de código malicioso, como gusanos y troyanos.

2.- GUSANOS:

Son programas cuya característica principal es realizar el máximo número de copias de sí mismos posible para facilitar su propagación. Es lo que se denomina replicación. A diferencia de los virus no infectan otros ficheros ni necesitan la intervención directa del usuario para ejecutarse.

Eliminar un gusano de un ordenador suele ser más fácil que eliminar un virus. Al no infectar ficheros la limpieza del código malicioso es más sencilla, aunque no basta con eliminar el archivo origen del gusano en cuestión.

Como los gusanos no infectan ficheros, para garantizar su auto-ejecución suelen modificar ciertos parámetros del sistema. Por ejemplo, pueden cambiar la carpeta de inicio para incluir una copia de sí mismos en el listado de programas que deben activarse al arrancar el ordenador. También pueden modificar alguna clave del registro que sirva para ejecutar programas en determinado momento: al arrancar el ordenador o cuando se llama a otro programa.

3.- TROYANOS:

Es código malicioso que se oculta dentro de programas que aparentemente son legítimos o inofensivos. El término troyano proviene de la historia del caballo de Troya mencionado en la Odisea de Homero, por su similitud en la forma de actuar.

Su principal vía de propagación es ocultándose dentro de código que se descarga de Internet, que lleva además de la función principal, una función oculta: el troyano.

También se pueden propagar por otro malware (virus), que después accede a Internet y se descarga el troyano.
Tienen cierta similitud con los virus (al infectar ficheros) pero se diferencia en que suelen ser más sofisticados y procuran no presentar síntomas para no ser detectados.
Un troyano bancario falseará el balance de las cuentas robadas para evitar ser detectado, incluso estudiará en función del saldo cuánto puede ir descontando en cada operación para que no salten los mecanismos de alerta de la banca en-línea.
Existe una amplia gama de troyanos bancarios pero también suelen utilizarse en ataques dedicados. Un ataque dedicado es un código malicioso específicamente creado para atacar a una persona, empresa o gobierno.
Para evitar ser detectados no suelen llevar rutinas de auto propagación o la replicación está limitada en el número de saltos (sólo hasta llegar al sistema objetivo). Su código suele mutar y puede ir cifrado para dificultar el estudio de su comportamiento.
Suelen abrir una puerta trasera (bakdoor) para control remoto del equipo. Con una puerta trasera el atacante puede entrar en los equipos saltándose los sistemas de seguridad de acceso.
Puede llegar hasta ordenadores no conectados a internet en casos de espionaje.
Suelen acompañarse de otro software que, sin ser en sí mismo malware, contribuye a conseguir los objetivos, como puede ser:

- **RECOLECTOR DE PULSACIONES DE TECLADO Keylogger**: Captura todo lo que se teclea y lo envía al centro de mando y control del atacante.
- **RECOLECTOR DE VIDEO DE PANTALLA (SCREEN LOGGER):** Graban todo lo que aparece en pantalla y lo envían al atacante. Pueden capturar lo que se pulsa en un teclado virtual. (Un teclado virtual es la imagen del teclado en pantalla para escribir sin usar un teclado físico, muchas veces usado por la banca por Internet para intentar evitar los "keylogger").
- **ROOTKIT**: Modifica programas del sistema operativo para que actúe de forma diferente. El Rootkit altera el flujo de ejecución del sistema operativo. No es un software maligno en sí mismo, pero permite ocultar las acciones de troyanos. Para evitar ser detectado, manipula un conjunto de comandos del sistema ocultando procesos, conexiones, utilización de recursos como memoria, disco, modificaciones en el registro de Windows. Este caso es de los más difíciles de detectar y eliminar.

5.2 Formas de entrada

Hay distintas vías o estrategias de propagación del malware. Antiguamente los programas maliciosos se propagaban mediante los discos extraíbles. Hoy en día existen muchas vías de propagación, también llamados **vectores de ataque**.

1. VECTORES DE ATAQUE: VULNERABILIDADES Y EXPLOITS DE SISTEMAS OPERATIVOS Y HERRAMIENTAS INFORMÁTICAS

Todo software tiene errores de desarrollo: Sistema operativos, Navegadores, Java, procesadores de Texto, Clientes de correo, Lectores de PDF, Lectores de video, flash,....

Una vulnerabilidad de software es un error de desarrollo que puede comprometer la seguridad de un ordenador.

Una vulnerabilidad será más o menos crítica en función de lo fácilmente que se pueda explotar y de las consecuencias que tenga sobre el equipo.

Cuando las vulnerabilidades son conocidas, los fabricantes liberan parches para solucionar el problema. Unos lo hacen siguiendo un ciclo programado y otros sin una política concreta. Muchos tienen formas de automatizar estas actualizaciones y son las propias aplicaciones las que averiguan si hay parches disponibles y los instalen en tal caso.

Un exploit es un programa o código que explota una vulnerabilidad para lograr cualquiera de las acciones maliciosas de las que hemos hablado.

Una vez que una vulnerabilidad es pública, es prácticamente segura la aparición de un exploit que la aproveche. Una vez el exploit es conocido, todo sistema sin parchear corre un serio peligro de ser comprometido.

Tanto una vulnerabilidad como un exploit decimos que son públicos, si son conocidos (han sido publicados); si son desconocidos se denominan de "día-cero" (o también día-0, 0-day))

Un ataque de día-0 es un ataque contra un equipo utilizando una vulnerabilidad desconocida o que está sin corrección por el fabricante.

Cada vez es más floreciente el negocio de compra y venta de vulnerabilidades día-0. Gobiernos, empresas de seguridad y redes de delincuentes están interesados en ellas. Existen exploits día cero cuyos precios pueden superar el millón de euros.

2. VECTORES DE ATAQUE: FALSIFICACIÓN DE CERTIFICADOS SSL DE SERVIDOR

Existen unos "notarios digitales" llamados autoridades de certificación. Éstos deben certificar ante las aplicaciones (el navegador por ejemplo) que una entidad es quién dice ser. Las aplicaciones confían en determinadas autoridades de certificación.

Estos certificados digitales son los que sirven para autenticar un servidor cuando usamos el protocolo seguro httpS.
Existen entidades de certificación que expiden certificados sin demasiadas comprobaciones (formulario web).
Autoridades de certificación de alto prestigio han sufrido ataques en los que se han logrado comprometer sus sistemas de expedición de certificados de servidor y los atacantes han llegado a expedir certificados falsos de compañías informáticas.
De esta forma, software o páginas ilegítimas serán vistas como legítimas y reputadas por las aplicaciones

3. VECTORES DE ATAQUE: DISPOSITIVOS DE MEMORIA EXTRAÍBLE Y PERIFÉRICOS.

Ataques usando memorias flash y discos USB, aunque también se dan casos con CDs y DVD. El ordenador se infecta por utilizar un dispositivo extraíble que hemos usado en otra ubicación como cibercafé, máquina de revelar, puesto de un amigo, etc.
Llegó a ser una de las 10 formas más comunes (el Top 10) de infección a nivel mundial.
En marzo de 2011 Microsoft publicó un parche que deshabilitaba el autoplay en dispositivos USB en todos sus sistemas Windows. Esta medida fue decisiva para mitigar este vector.

4. VECTORES DE ATAQUE: CORREO ELECTRÓNICO:

Aunque algo antiguo, sigue siendo un vector de ataque importante, bien directamente, o como paso previo redirigiendo al usuario a una página web desde la que se descarga el malware, o a un supuesto soporte telefónico.
Los clientes (programas de lectura) de correo electrónico no comprueban el remitente porque usan protocolos que fueron desarrollados hace muchos años. Es fácil manipular al cliente de correo para que pretenda proceder de un conocido o usuario del INE, de la Agencia Tributaria, de la policía, de Correos, de Tráfico, etc.
Muchos correos fraudulentos, se reconocen por estar escritos en inglés o por sus faltas de sintaxis y ortografía ya que proceden de traducciones automáticas. Pero no siempre es así. Algunos están escritos en perfecto castellano. Pretenden engañar al usuario con señuelos seductores o bien asustándole con multas, con perder sus credenciales de banca,... (y otras tácticas de ingeniería social). Se conocen como técnicas de phishing (ya comentadas) y son utilizadas con otros vectores.
La infección se consigue

- Directamente a través de un adjunto con el malware. El adjunto puede llevar una doble extensión para ocultar su condición de ejecutable o aprovechará alguna vulnerabilidad del aplicativo que lo abre para actuar. Una vez abierto el adjunto, se produce la infección.
- Redirigiendo (mediante un enlace) a una página en la que se materializarán la infección mediante vulnerabilidades del navegador o simularán ser del banco de la víctima, simulan ser un servicio legítimo y solicitan el cambio de contraseña, de esta forma roban las credenciales.
- Combinando el correo con un falso soporte telefónico (vishing). Se solicita a la víctima que llame a un número de teléfono desde el que intentarán averiguar sus credenciales.

5. VECTORES DE ATAQUE: ENLACES EN REDES SOCIALES:

Actualmente es uno de los principales vectores de ataque.

Se usan las mismas técnicas que para el correo electrónico y algunas que le son propias.

El atacante envía (postea) enlaces maliciosos, invitaciones... entre sus "amigos".

Utiliza también técnicas de clickhacking (Engaños para pinchar en el botón "Me gusta").

Existen botnets que utilizan twiter para que el centro de control de la botnet envíe sus órdenes de ejecución a sus zombies.

6. VECTOR DE ATAQUE: REDES DE INTERCAMBIO DE FICHEROS P2P

Introducir entre los ficheros que se comparten un fichero "goloso" (como un fichero con el título de una película de estreno) con el malware.

También es muy frecuente engañar con las dobles extensiones, por ejemplo: un fichero con el título de una canción y su extensión es ejecutable (exe, bat..) y no de multimedia (mp3, avi…). Normalmente son gusanos que se reproducen a sí mismos.

Muchos de los programas utilizados para el P2P instalan spyware.

7. VECTORES DE ATAQUE: ALMACENES DE APLICACIONES PARA MÓVILES (APP STORE)

Se calcula que casi el 75% del planeta tiene un teléfono móvil y hay más tarjetas SIM que personas en el mundo, según datos de Mobile World Congress (MWC).

Además, se pueden realizar pagos por esta vía y muchos bancos y organizaciones envían credenciales a los usuarios a través del teléfono móvil.

Los puntos de venta electrónicos de pequeñas aplicaciones para teléfonos móviles (Apple Store, Android Market de Google, Ovi de Nokia y el Windows Phone Marketplace de Microsoft...), son uno de los mercados más florecientes. El usuario puede descargar cómodamente aplicaciones en un solo click a un precio económico y en muchos casos gratis.

Este éxito no ha pasado desapercibido a los ciberdelicuentes que hace mucho tiempo que tienen su punto de mira en este mercado.

Muchas de esta aplicaciones tiene derechos excesivos sobre los recursos del móvil y los usuarios no suelen verificar dichos derechos. Se calcula que un 30% de las aplicaciones para móviles detecta la ubicación del usuario y un 10% accede a la agenda de contactos.

8. VECTOR DE ATAQUE: COMUNICACIONES MÓVILES, INALÁMBRICAS: 3G, WI-FI, BLUETOOTH, INFRARROJOS

Cuando usamos redes inalámbricas la comunicación está en el aire y por tanto es muy fácil de fisgar. Cualquiera puede "escuchar" ya que existen herramientas de "pirateo" gratuitas que permiten que usuarios con apenas conocimientos técnicos realicen este tipo de intrusión. Las escuchas pueden hacerse desde bastante distancia ya que se comercializan antenas que permiten hacerlo desde kilómetros. Si la comunicación no está cifrada no hay más que tomarla. Si se usan contraseñas o protocolos poco robustos seremos vulnerables.

WiFi Pública:

Si usamos un punto de acceso público hay que tener en cuenta que la mayoría de ellos no cifra la información que se envía a través de internet o pueden usar protocolos inseguros. Muchos de ellos sólo cifran la página de inicio pero no así el resto de la comunicación. Cualquier otro usuario de la red puede ver todo lo que circula por este medio e incluso modificar la información en tránsito sin necesidad de hardware adicional.

La mayor parte de las WiFis públicas implanta medidas de seguridad débiles, sin bastionar, protegiendo la comunicación con claves poco robustas o que no se cambian con frecuencia. En estos casos es también relativamente fácil interceptar o inyectar información.

Compartir una WiFi pública con otros usuarios desconocidos permite que éstos puedan aprovechar cualquier vulnerabilidad del equipo utilizado por el usuario, para entrar en el sistema y obtener cualquier dato que resida en éste.

Ataques con punto de acceso falso (Rogue PA):

Cada vez ha proliferado más el despliegue por parte de atacantes de falsos puntos de acceso (PA) de interconexión WiFi. Estos Puntos de Acceso WiFi ("Rogue PA"), se despliegan principalmente en aeropuertos, cafeterías, hoteles, universidades, bibliotecas, etc. aunque también se realizan contra instituciones. Suelen tener una potencia mayor que la de la WiFi original, adaptando su aspecto completamente a la legítima; la víctima se conecta al punto de acceso del atacante que queda en el medio de toda comunicación interceptando toda la transferencia de información entre el usuario y cualquier otro servidor. En este momento el atacante puede escuchar y manipular todo lo que viaje a través de la conexión inalámbrica; desde una escucha pasiva a una interceptación activa como secuestro de la sesión legítima (aunque sea https), utilizando las credenciales del usuario o inyectando información en su propio beneficio.

9. VECTOR DE ATAQUE: ERRORES DE PROTOCOLO

Este es el más difícil de mitigar ya que el fallo o vulnerabilidad no está en una implementación concreta en un programa sino en el propio diseño inseguro del protocolo. Protocolos como DNS, SSL,... han tenido errores de protocolo que pueden tardar meses o años en corregirse.

10. VECTOR DE ATAQUE: HARDWARE

Existen interfaces de programación para el hardware de última generación que pueden ser usadas para introducir código malicioso en la BIOS.

Se dieron casos de este tipo, como un troyano para la BIOS de Award, que infectó el sector maestro de arranque.

Otra posibilidad es la de pequeños adaptadores que se interponen entre la terminación del cable del teclado y el ordenador y permite la grabación de todo lo tecleado por hardware.

11. VECTOR DE ATAQUE: DEBILIDAD Y REUTILIZACIÓN DE CONTRASEÑAS O UTILIZACIÓN DE ÉSTAS DESDE MEDIOS INSEGUROS

La debilidad de las contraseñas facilita la penetración en sistemas sin necesidad de recurrir a mecanismos sofisticados.

Un estudio sobre las contraseñas de los usuarios revela que el 90% de las contraseñas que circulan por internet están entre una lista de las 1.000 más usadas. La utilización de contraseñas débiles permite su adivinación con un pequeño esfuerzo (ataques de diccionario).

Muchas aplicaciones, teléfonos móviles, routers... tienen contraseñas por defecto 1234, 0000... Si no se cambian estas contraseñas por defecto, ni siquiera será necesario un ataque para tomar control del equipo.

La reutilización de la misma contraseña en varias cuentas para acceso a servicios de perfiles de seguridad diferentes, tiene como consecuencia que la seguridad sea equivalente a la del servicio más débil. Puede aprovecharse el compromiso de credenciales en una cuenta para comprometer el resto. Por ejemplo, en el acceso a servicios que necesitan autenticación desde equipos públicos (cibercafés, hoteles...) en los que desconocemos el estado de seguridad de los mismos. Los atacantes pueden haber implantado programas o dispositivos físicos para captura de pulsaciones de teclado, captura de pantalla para grabar nuestras credenciales. En función de la configuración de los navegadores, las páginas cifradas se guardan en cachés (archivos temporales) y permanecen por un tiempo indefinido.

Otra debilidad que afecta a las contraseñas es la utilización de protocolos de comunicación en claro para la distribución de las mismas (el correo electrónico, navegación web, chat...) que pueden observarse si transcurren por un medio inalámbrico. También es frecuente cometer el error de enviar al mismo tiempo y/o por el mismo medio los datos cifrados con la contraseña que los descifra.

12. VECTORES DE ATAQUE: INGENIERÍA SOCIAL:

BAITIN: La infección proviene de un dispositivo extraíble "olvidado" a propósito por el atacante cerca de su víctima (persona o institución); contiene un caballo de Troya que después le permitirá acceso al sistema El dispositivo llevará etiquetas que inciten mucha curiosidad, en nuestro caso podría ser por ejemplo el logo del INE y "copia de las nóminas 2019".

SHOULDER SURFING: Es una técnica muy empleada y consiste en espiar por encima del hombro a los usuarios cuando teclean su nombre y contraseña en algún sistema.

LLAMADA TELEFÓNICA (PHISHING TELEFÓNICO): Una llamada de un falso soporte técnico (imaginemos que el atacante se identifica como del CSU) a usuarios pidiendo que ceda sus credenciales para hacer mantenimiento mientras desayuna. Kevin Mitnick, uno de los piratas informáticos arrepentidos más famosos del mundo, reveló los secretos que le ayudaron a cometer sus fechorías y, el phishing telefónico era el primero, el más fácil y el más útil.

PHISHING CON PROMESAS GOLOSAS: Pueden prometer: trabajo con beneficios desorbitados, vales descuento, viajes...

ESCARBAR EN PAPELERAS Y CUBOS DE BASURA "DUMPSTER DIVING": El Dumpster-diving consiste en rebuscar entre la basura, para intentar buscar información utilizable para un posterior ataque.

Conclusiones

Vectores de ataque: No terminarán de aparecer nuevos vectores de ataque ya que el delito informático es barato y está al alcance de cualquiera, saca copiosos beneficios, traspasa fronteras y es difícil de perseguir.

5.3 Contramedidas

1. CONTRAMEDIDAS: FORMACIÓN CONTINUA EN SEGURIDAD

Incibe (Instituto Nacional de Ciberseguridad) tiene oferta de cursos de seguridad https://www.incibe.es/protege-tu-empresa/formacion

El eslabón más débil es el humano y la formación y la concienciación de los usuarios es vital para cualquier organización.

2. CONTRAMEDIDAS: HÁBITOS DE SEGURIDAD

- Configurar el bloqueo automático de dispositivos. Bloquear la pantalla cuando se deja abandonado el puesto, aunque sea por pocos minutos (En Windows, simultáneamente tecla de Windows_L)
- No tener pegatinas a la vista con las contraseñas o pegadas en el portátil.
- No guardar las contraseñas en un archivo de texto o en un correo sin cifrar.
- No almacenar contraseñas en el móvil.
- Tapar el teclado antes de teclear las contraseñas si creemos que podemos estar siendo observados (no hay por qué avergonzarse).
- Al introducir la contraseña, equivocarse a propósito en algunas pulsaciones para después eliminar la parte errónea marcando con el ratón y pulsando suprimir (esto complica el shouder sourfing o la captura de teclado pero no la captura de pantalla si el teclado es virtual)
- Desconfiar de llamadas telefónicas, mensajes de correo, cartas,... que piden datos confidenciales o sospechosos.
- No tirar documentos con información confidencial a la papelera/basura, sin haber utilizado previamente un mecanismo que la haga ilegible.
- Guardar documentos confidenciales bajo llave.
- No tirar dispositivos extraíbles como CD, DVD con información confidencial. Borrar previamente la información y, si es de solo lectura, destruirlos.

- Borrar todos los datos (formateando el equipo, teléfono...) antes de deshacernos del equipo en un punto limpio. Si la información tiene un nivel de confidencialidad alto, debe reescribirse varias veces con datos aleatorios para que sea verdaderamente irrecuperable. En casos extremos es mejor recurrir a una empresa certificada.
- Desconfiar de lo encontrado en las cercanías al lugar de trabajo o domicilio, puede ser un ataque dirigido.
- Desconectar la localización geográfica de un dispositivo si no se está usando. Ahorraremos batería y ganaremos privacidad.
- La información de portátiles, teléfonos inteligentes debe ser la mínima necesaria y, si es confidencial, debe estar cifrada. Descargar los datos confidenciales en cuanto haya ocasión en un punto más estable o seguro (PC, red).
- Los portátiles deben mantenerse actualizados; conviene, si se utilizan poco, encenderlos para que vayan actualizándose poco a poco.
- No perder de la vista equipos portátiles, teléfonos inteligentes. Una posible solución es utilizar cadenas de seguridad al portátil.
- Revisar siempre las facturas telefónicas por si hubiera cambios sospechosos. Avisar cuanto antes a la compañía telefónica si hay algún cargo extraño.
- Si sospechamos que nuestro ordenador está comprometido tener en cuenta que los troyanos pueden darnos un saldo falso, revisar el extracto de banca online desde un PC limpio.
- Apuntar el número IMEI para poder desactivar el terminal en caso de pérdida o robo a través de la compañía telefónica (se muestra en la pantalla del teléfono pulsando *#06#).
- Apagar el equipo incluyendo el router cuando no se utiliza.
- En caso de que el incidente se materialice, avisar al área de seguridad de las organizaciones o realizar una denuncia formal si es a nivel personal.

3. CONTRAMEDIDAS: NAVEGAR CON CABEZA.

- Nunca navegar en internet como usuario administrador. Siempre es recomendable trabajar con los mínimos privilegios necesarios.
- Elegir siempre sitios de reputación para navegar y muy especialmente para comprar.
- Descargar las aplicaciones desde sitios oficiales y, muy especialmente, para programas de seguridad y parches.
- Tener precaución con los resultados servidos por los buscadores, especialmente ante noticias de impacto y primicias. Buscar las noticias de actualidad siempre de

sitios de confianza. Hay que fijarse en el dominio antes de enlazar. Desconfiar si el enlace es directamente una IP sin nombre de dominio.

- Leer cuidadosamente cualquier mensaje antes de hacer clic en el botón "Aceptar" o "Siguiente". La falta de atención cuando aceptamos advertencias de seguridad puede ser fatal.
- Evitar enlaces sospechosos, especialmente aquellos que ofrecen descuentos imposibles, servicios gratuitos...
- Antes de instalar algún programa gratuito hay que leer las condiciones de la licencia, puede que estemos aceptando anuncios que cargarán la red y el ordenador.
- Para cerrar una ventana emergente sospechosa no usar los botones aceptar/cerrar que ésta ofrezca ya que no sabemos qué acciones encubiertas puede ocasionar. Cerrar la ventana con el aspa de la esquina superior derecha (o teclear Alt_F4 si no la trae).
- Impedir la ejecución de archivos desde sitios web sin verificar previamente el archivo descargado. Es importante NO hacer "clic" sobre el botón "ejecutar" para pode verificar su integridad. Analizar con un antivirus cada archivo que se descarga antes de ejecutarlo.
- Es especialmente delicado aceptar la ejecución de programas que ni siquiera se han solicitado.
- Recordar que no hace falta descargar software para ser objeto de una infección ya que sólo con navegar con una vulnerabilidad de Java o del navegador, incluso por un sitio legítimo y conocido al que hayan inyectado software malicioso, seremos objeto de infección.
- Las direcciones de la banca teclearlas siempre directamente en la barra de navegación; no usar enlaces obtenidos de buscadores, redes sociales, mensajes de correos electrónicos...
- No equivocarse al teclear ya que a veces los atacantes compran dominios primos, dominios de escritura similar y parecidos al ojo humano (cambiando la "b" por una "h" o la O por el cero "0" ...).
- Si se navega desde sitios públicos, es recomendable eliminar los archivos temporales, caché, cookies, direcciones URL, contraseñas y formularios donde se hayan ingresado datos. Si el navegador tiene opción de navegación privada, usarla.
- Si nos hemos conectado a un sitio (log-in), a la hora de desconectarnos, utilizar el botón "salir" o "desconectar" en lugar de cerrar directamente la ventana del navegador. De esta forma la conexión no podrá reutilizarse.

- Acceder siempre que sea posible a sitios seguros con protocolo httpS.

4. CONTRAMEDIDAS: CIFRAR TODA LA INFORMACIÓN CONFIDENCIAL

- Toda la información confidencial debe almacenarse cifrada: la que se almacena en los puestos, portátiles o dispositivos extraíbles como llaves USB , CD, DVD...
- Toda la información confidencial debe transferirse cifrada: la que intercambiamos con otros organismos o personas, incluyendo la que circula por el correo electrónico.

  Si tanto nosotros como nuestro interlocutor tenemos certificados digitales y el cliente de correo lo permite, utilizar S/MIME para enviar correos cifrados

  Para ello basta intercambiar nuestras claves públicas firmando ambos un primer correo (que sólo llevará la firma).

  A partir de ahí podremos cifrar el correo con este destinatario, y al contrario de lo que sucede con https (que solo cifra en el tránsito), este permanecerá cifrado en el ordenador de destino. Además nos permitirá verificar la autenticidad del origen y la integridad.
- Cifrar la información previamente, antes del envío.

  Si usamos un algoritmo con clave común compartida (cifrado simétrico), nunca enviaremos por el mismo mecanismo la clave de cifrado y la información cifrada (sería como colocar una pegatina con la clave). Por ejemplo si enviamos un documento previamente cifrado por el correo electrónico, telefonearemos para dar la clave a nuestro interlocutor o la enviaremos por correo ordinario.
- No utilizar unidades temporales de red para intercambiar información confidencial sin cifrar.

5. CONTRAMEDIDAS: PROTEGER NUESTRA DIRECCIÓN DE CORREO ELECTRÓNICO Y LA DE LOS DEMÁS

- Hay que pensar siempre antes de ingresar datos personales en cualquier formulario web, foros... en los que se nos solicite el correo electrónico para acceder a una determinada página. Conviene crear una cuenta de correo (cuenta de paja) dedicada a este fin con unos identificadores inventados. Los recolectores automáticos de correo electrónico cosechan las cuentas de correo electrónico que se publican en internet. Esta medida evitará que recojan tus datos personales y protegerá de spam la cuenta privada lo que se traducirá en ahorro de tiempo a la hora de leer el correo. Si la cuenta de paja se llena se puede cerrar y abrir otra nueva.

- Nunca contestar a un mensaje sospechoso con el botón "Responder a" de correo ya que podemos estar respondiendo al atacante. Averiguar por otro medio la veracidad del mensaje:
    - Teléfono (nunca el que se incluya en la carta).
    - Utilizar la vía de contacto desde la página web oficial tecleada directamente sin seguir enlaces.
    - Correo electrónico nuevo al "Contacte con Nosotros" de la página web oficial.
- Desconfiar de todo lo que pide que distribuyas al mayor grupo de conocidos posible. Estará cosechando tu dirección de correo y la de tus contactos e invadiendo la red de spam. Hay que romper cadenas. Es una mala idea distribuir mensajes a muchos contactos utilizando el campo "Para" (To) si no es necesario que todos los destinatarios estén advertidos de a quiénes más va dirigido el correo. Cuando alguien realiza un "Redirigir" (Forward), el mensaje acumula las trazas de los "Para" del mensaje original.
- Así un mensaje con muchos destinatarios, redirigido a su vez a otros muchos destinatarios... acaba cosechando un montón de direcciones válidas de correo electrónico.
    - Piensa si es necesario un "redirigir". Si no lo es, protege la intimidad de tu fuente creando un mensaje nuevo o eliminando los restos con direcciones de contactos.
    - Al escribir un mensaje para varios conocidos mándatelo a ti mismo en el campo "para" y en copia oculta (bcc o blind copy) al resto. Evitarás que si alguien lo reenvía a otros tantos, sus direcciones sean cosechadas.
- Nunca redirigir el correo del corporativo (por ejemplo el del INE) a correos personales en la nube, ya que no suelen existir acuerdos de confidencialidad y estarás almacenando información confidencial en sitios inseguros y poniendo en peligro la reputación de tu organismo.

6. CONTRAMEDIDAS: UTILIZAR CONTRASEÑAS FUERTES Y CAMBIARLAS CON REGULARIDAD

Daremos cuatro recomendaciones básicas:

1. **Una contraseña diferente para cada servicio o web**: si no podemos recordar muchas usar gestores de contraseña.
2. **Que sean lo más robustas posibles** (largas, con letras, números y símbolos) pero fáciles de recordar.
3. **Cambiarlas cada cierto tiempo:** al menos cada 6 meses.

4. **Si existe la posibilidad de un segundo factor de autenticación, usarlo siempre.**

7. CONTRAMEDIDAS: UTILIZAR SIEMPRE SOFTWARE CON SOPORTE DEL FABRICANTE

Utilizar software con soporte del fabricante. No utilizar productos descontinuados (Windows XP, Vista, 95, 2K, Internet Explorer 6...) . Un sistema o aplicación al que un fabricante ya no da soporte está expuesto a un sin número de exploits.

8. CONTRAMEDIDAS: MANTENER EL SISTEMA OPERATIVO ACTUALIZADO

Activar la actualización automática del sistema para lo cual se debe configurar en el Centro de Seguridad de Windows la descarga automática.

Descargar siempre los parches desde sitios oficiales. No descargar actualizaciones desde sitios de dudosa reputación.

Los teléfonos móviles también tienen sistema operativo y también conviene buscar actualizaciones, especialmente si se usan para navegar por Internet o para leer correo.

9. CONTRAMEDIDAS: MANTENER LAS APLICACIONES ACTUALIZADAS

Muchas de las aplicaciones que utilizamos tienen la opción de actualizar automáticamente, si es así conviene activar esta opción y la propia aplicación nos alertará cuando haya un cambio de versión, o incluso se actualizará automáticamente.

De no ser así, debe comprobarse periódicamente de forma manual que la versión usada es la última disponible. La mayor parte de las aplicaciones tienen en el menú la opción "acerca de" que nos informa de la versión que estamos usando.

Es importante mantener actualizados todos los programas y, especialmente, los que se utilizan en conexiones con internet: navegador, correo electrónico, versión de Java, lector de pdf, visualizadores de animaciones flash o video, herramientas de ofimática.

Los teléfonos móviles también tienen aplicaciones y también deben parchearse.

NAVEGADOR:

Se debe prestar especial atención a los parches del navegador ya que es la aplicación con el que nos conectamos a Internet. Visitar una web maliciosa con un navegador o versión de Java vulnerable es suficiente para infectarnos con malware.

No solo es importante tener actualizado el navegador sino también todos los complementos del navegador ("plugins") de otros fabricantes que sirven para interactuar con aplicaciones externas. Estos complementos son los que nos permiten visualizar pdf, animaciones flash, recreaciones 3D, video... con el navegador.

No debe olvidarse que los teléfonos inteligentes, también tienen navegadores y por tanto son vulnerables. Deben estar siempre actualizados a la última versión.

10. CONTRAMEDIDAS: CONFIGURACIÓN DE SEGURIDAD DEL NAVEGADOR

- Configure el navegador para que bloquee todas las ventanas emergentes.
- Utilizar flitro antiphishing
- Limpiar datos privados, cachés,... por omisión
- No almacenar https en caché ("No almacenar información cifrada en disco")
- Los teléfonos móviles también tienen navegador, cookies...
- Buscar un buen manual para más indicaciones

11. CONTRAMEDIDAS: TENER SIEMPRE ACTIVADOS LOS PROGRAMAS DE SEGURIDAD

Los programas de seguridad tienen que estar activados antes de la primera conexión a internet. Después ya puede ser tarde.

- El cortafuegos (firewall) debe estar siempre activado.
  Las reglas del cortafuegos deben ser lo más restrictivas posibles no solo para las conexiones de entrada desde internet hacia nuestro equipo, sino también para las conexiones desde nuestro equipo hacia internet. Hay troyanos que se ponen en contacto con su centro de control a través de un puerto determinado. Si el cortafuegos cierra ese puerto ya no podrá realizar esta conexión.
- El programa antivirus debe realizar actualizaciones diarias y estar configurado de modo proactivo (para detectar en tiempo real).
- No olvidar pasar el antivirus a los periféricos de entrada (discos, usbs...).
- Conviene comprobar de forma rutinaria que estos programas están activados y actualizados.
- Utilizar programas de seguridad en teléfonos inteligentes.

Estas medidas, siendo completamente necesarias, ¡no son suficientes!, no deben darnos una falsa sensación de seguridad. Existe un periodo de tiempo entre la aparición del malware y su detección por las casas antivirus. Un estudio de la compañía Cyveillance concluyó que los porcentajes de detección de los antivirus son bajos. En el caso de malware reciente (fresco) la detección apenas llegaba al 20% de los programas antivirus, y después de un mes de su aparición a un 60%.

12. CONTRAMEDIDAS: EVITAR COMPARTIR PERIFÉRICOS

- Utilizar un dispositivo de solo lectura para llevar fotos a revelar, impartir curso en un ordenador ajeno...

- Vacunar la memoria USB con un programa que evite que puedan incluir en ésta un autoejecutable dañino.
- Analizar con un antivirus todo periférico después de haber visitado otro ordenador.

13. CONTRAMEDIDAS: CONFIGURACIÓN SEGURA DE LOS CERTIFICADOS ELECTRÓNICOS

CUIDADOS CON EL CERTIFICADO PERSONAL:

- Proteger los certificados personales en software (C2CA FNMT, CatCERT...) con una contraseña que pedirá antes de usarlo.
- Hacer una copia del certificado en un CD y volverlo a importar al ordenador esta vez como "no exportable", evitaremos que nos lo sustraigan.
- Si creemos que nuestro certificado ha podido ser comprometido, revocarlo (la autoridad lo incluirá en la lista de certificados que ya no reconoce como válidos).

CUIDADOS CON CERTIFICADOS DE TERCEROS:

- Comprobar siempre la validez del certificado así como quién lo expide.
- Si el navegador advierte que el sitio es inseguro no conviene aceptar sin más la conexión. Algunas veces el mensaje aparece porque es necesario decirle al navegador que confíe en una autoridad de certificación concreta. Por defecto los navegadores no siempre confían en un grupo de autoridades de certificación. Para comunicar al navegador que confiamos en ella, hay que importar su certificado raíz y decir para qué propósitos confiamos en ella.

Los certificados raíz (y subordinados en el caso de que haya una jerarquía de autoridades, como en el caso de la autoridad de certificación para empleados públicos, APE, por ejemplo), se descargan de las páginas oficiales de las autoridades en las que queremos confiar. Una vez descargados, se importan en el navegador y se detalla para qué actividades vamos a confiar en estas autoridades (autenticar servidores, firmar software,...).

14. CONTRAMEDIDAS: CONFIGURACIÓN DE SEGURIDAD DEL SISTEMA OPERATIVO

- Nunca deshabilitar la autenticación para entrar a un equipo. Es incómodo pero fundamental.
- Habilitar el bloqueo automático de la pantalla tras un tiempo de inactividad.
- Todos los usuarios deben usar contraseña y ser robustas. Deben cambiarse con regularidad. Si es posible, forzar estas políticas con el sistema operativo.
- Crear un perfil de usuario con privilegios restringidos (usuario no administrador). Incluso distintos usuarios con la autorización mínima necesaria para desarrollar

cada actividad. Utilizar para el día a día un usuario no administrador. Reservar el usuario administrador para instalar software de confianza.

- Por defecto, el usuario Windows creado en la instalación posee privilegios administrativos. Esto es un factor que aumenta la probabilidad de infección ya que un exploit, de materializarse estando con privilegios de administrador, tendrá lugar con privilegios totales sobre el ordenador.
- Deshabilitar usuarios no necesarios (invitado de windows...).
- Cambiar todas las contraseñas por defecto en todos los equipos (puestos, routers, teléfonos inteligentes, tablets...).
- Si existe la opción, utilizar como sistema de ficheros NTFS evitando FAT, FAT32, o FAT32x.
- Deshabilitar el uso de carpetas e impresoras compartidas.
- Deshabilitar la ejecución automática de dispositivos USB. Plantearse la desactivación de arranque automático de CD/DVD.
- Configurar la visualización de las extensiones de archivos para evitar ser víctimas de técnicas como la doble extensión.
- Configurar la visualización de archivos ocultos.
- Crear carpetas cifradas para almacenar la información confidencial.
- Crear puntos de restauración del sistema operativo limpios antes de instalar nuevo software, esto nos permitirá volver a una situación estable anterior. (Solo incluye el sistema, no los datos).
- Considerar crear una partición para el sistema operativo y otra diferente para los datos.
- Mantener el archivo etc/hosts en modo solo lectura.

15. CONTRAMEDIDAS: EVITAR EL USO DE TECNOLOGÍAS INALÁMBRICAS INSEGURAS.

- Plantearse si es realmente necesario acceder a una red WiFi externa.
- Nunca utilizar una WIFI pública para acceder a organismo con información sensible (como es el INE) o a la banca electrónica.
- Evitar puntos de acceso como aeropuertos, transporte público... especialmente si utilizan un protocolo de cifrado débil como Wep.
- Apagar el router del domicilio cuando no se esté utilizando, especialmente en vacaciones.
- Si el punto de acceso en domicilio es WiFi considerar si pasar a cable. Cambiar la contraseña con frecuencia y elegir siempre una robusta.

- El uso de bluetooth, WiFi, infrarrojos debe restringirse al momento necesario, desactivándose cuando cesa la necesidad.

16. CONTRAMEDIDA: TENER COPIA DE SEGURIDAD REGULAR DE LA INFORMACIÓN EN DISPOSITIVO EXTERNO

- Decidir qué directorios es necesario salvaguardar. Si la información es confidencial, debe cifrarse. Diseñar un calendario de copias de seguridad en función de cada actividad: cada día, semana, cada vez que...
- No olvidar sacar una copia de los certificados electrónicos en un medio de solo lectura como un CD, etiquetarlo.
- Las copias deben almacenarse fuera del ordenador con seguridad física y etiquetarse.
- Conviene realizar copias de seguridad de puntos de restauración del sistema, así, si hay que volver a un estado seguro de un sistema, se evitará tener que volver a cargar el sistema y todos los parches.
- Conviene comprobar que las copias han funcionado con un par de ficheros. No sería la primera vez que al intentar utilizar una copia se descubre que está vacía o incompleta.

6. RESUMEN

Las ideas más relevantes en este capítulo son:

- Desde el punto de vista de los usuarios, visión externa, el sistema operativo actúa como un interfaz entre los programas de aplicación y la máquina pura.
- Desde el punto de vista interno el sistema operativo puede concebirse como un gestor de recursos.
- Desde la visión de que los sistemas operativos son gestores de recursos, básicamente gestionan los recursos que tiene: Gestión de procesos, gestión de la memoria principal, gestión de memoria secundaria (disco), gestión de entradas y salidas y llamadas al sistema.
- En los ficheros se organiza toda la información, tanto datos como los programas de aplicaciones. El sistema operativo es el encargado de proporcionar que su gestor de ficheros pueda: Construir, eliminar archivos y directorios.
- En Windows los archivos son nombrados por una cadena de caracteres seguida por un punto y tres caracteres adicionales. Estos tres últimos caracteres adiciones definen el tipo de archivo y es lo que se conoce como la extensión de los archivos.

- La compresión es una técnica de codificación diferente para hacer que los archivos y carpetas de nuestras unidades ocupen menor espacio, es decir, tengan un tamaño menor.
- Las redes de área local (o LAN por su nombre en inglés: Local Área Network) se caracterizan por ser de alta velocidad, para un área de cientos de metros, por ser en broadcast (de medio compartido y no punto a punto), de bajo coste y alta fiabilidad.
- Los permisos definen lo que un usuario o grupo puede hacer o no en un sistema, los privilegios que tiene. De poco sirve tener muy bien definido los usuarios y los grupos si luego todos tienen permisos para hacer de todo.
- Muchos ataques informáticos utilizan estrategias orientadas a explotar el eslabón más débil "el factor humano". Para ello utilizan técnicas de Ingeniería Social basadas en el engaño.
- El malware no siempre da la cara. Los antivirus no son suficiente protección.
- Vectores de ataque: No terminarán de aparecer nuevos vectores de ataque ya que el delito informático es barato y está al alcance de cualquiera, saca copiosos beneficios, traspasa fronteras y es difícil de perseguir.