Guía de Seguridad de la Información para Ciudadanos

Región de Murcia
Consejería de Industria y Medio Ambiente
Dirección General de Innovación Tecnológica y Sociedad de la Información

Región de Murcia
Consejería de Industria y Medio Ambiente
Dirección General de Innovación Tecnológica y Sociedad de la Información

regiónde murciaSI
PLAN PARA EL DESARROLLO DE LA SOCIEDAD DE LA INFORMACIÓN EN LA REGIÓN DE MURCIA

Crecemos con Europa

Unión Europea
Fondo Europeo de Desarrollo Regional

Índice de contenido

LAS NUEVAS TECNOLOGÍAS. Una apuesta necesaria

El impulso de las nuevas tecnologías es un hecho innegable e imparable. Cada día es más frecuente encontrar ordenadores en los hogares que funcionan a pleno rendimiento y dedicados a múltiples tareas: hacer la compra, consultar los horarios de los cines, planificar las vacaciones, presentar las declaraciones de renta, buscar información, música, cine, etc. El ordenador y las nuevas tecnologías han cambiado la forma de medir la evolución de un país, actualmente algunos de los indicadores que miden la madurez y futuro de una sociedad pasan por evaluar el acceso y uso de las nuevas tecnologías por parte de los integrantes de esa sociedad.

La incorporación de los ciudadanos a la Sociedad de la Información y del Conocimiento ha requerido un importante esfuerzo cultural y tecnológico por parte de la Administración Pública, empresas de tecnología, organizaciones, asociaciones y por supuesto de los propios ciudadanos.

Esta guía de seguridad se presenta con el objetivo de sensibilizar a los ciudadanos sobre la importancia de la seguridad en el uso de las nuevas tecnologías, recomendando soluciones sencillas que permitan su incorporación a la Sociedad del Conocimiento de forma segura y controlada, evitando riesgos innecesarios y problemas por desconocimiento de ese nuevo mundo que es Internet.

LA SEGURIDAD DE LA INFORMACIÓN. La asignatura pendiente

Un usuario que adquiere un ordenador y se conecta a Internet está accediendo a un mundo de servicios, pero al mismo tiempo está asumiendo riesgos que, en la mayoría de los casos, le son desconocidos. Los incidentes de seguridad, además de ocasionar un problema para el usuario que los sufre, suponen una importante responsabilidad; infecciones producidas por virus hacen que el usuario infectado, la mayoría de las veces, sea participe directa o indirectamente de la infección de otros usuarios, colaborando así a la propagación del virus o generando el envío de mensajes no deseados o Spam.

Las ultimas evoluciones detectadas en los virus muestran una nueva tendencia, ya no intentan producir daños en los equipos de los usuarios infectados, sino que intentan robar la información de los usuarios que utilizan Internet para entrar en las cuentas bancarias, generar grandes listas de envío de Spam e incluso, en los casos más extremos, secuestrar la información del ordenador para pedir un rescate o realizar actos delictivos con el equipo infectado.

Como se puede ver, no solo está en juego nuestra seguridad, sino también la de nuestros conocidos, por tanto, guiar a los usuarios en sus primeras experiencias con el ordenador y en su acceso a Internet ayuda a prevenir riesgos.

A lo largo de los capítulos de la guía se presentarán comportamientos que pueden comprometer la seguridad de su información y aportar ideas y soluciones que permitan protegerla.

1. Elegir el equipo

Elegir un equipo es el primer paso sobre el que construir la seguridad para proteger nuestra información. Si el equipo no se adapta a nuestras necesidades, los componentes no son los adecuados o no disponemos de garantía de funcionamiento no dispondremos de una base sólida sobre la que aplicar las medidas de seguridad.

Consideramos que, por su aceptación, el equipo seleccionado será un PC, (Personal Computer). En este caso la oferta es desconcertante, equipos de multitud de marcas comerciales y modelos que están compuestos por multitud de componentes que, a veces, ni siquiera indican a qué corresponden. Así podemos entrar en una tienda y pedir: "quiero un Pentium IV con 1 giga de RAM y 180 gigas de disco, regrabadora de DVD y pantalla plana". La mayoría de las características porque tenemos un amigo que nos ha aconsejado eso o por los conocimientos que hemos adquirido en conversaciones con amigos o compañeros de trabajo, y el dependiente, que lo ha entendido todo nos pregunta, ¿de marca o clónico?, ¿Gigahertzios?, ¿tarjeta grafica de 256Mb?, ¿tarjeta de sonido?, ¿tarjeta de red?, ¿modem?, ¿lector de tarjetas?... en fin, toda una lección de lenguaje por símbolos en la que hay que avanzar paso a paso. Identifiquemos algunos de los componentes que debemos especificar para comprar un ordenador:

Si no dispone de la publicación Diccionario para internautas publicado por www.regmurcia.com, hágase con uno, le servirá para identificar la mayoría de los conceptos técnicos que se utilizarán a lo largo de la guía.

El Procesador: La CPU (Central Processor Unit), aunque ya nadie la llama así, de hecho ahora únicamente se menciona el modelo (Pentium, AMD, etc.), es el "motor" del ordenador, ya que su trabajo es ejecutar el software que el usuario utiliza (sistema operativo, aplicaciones, etc.). Su velocidad se mide en Gigahertzios (GHz), que determina la información que es capaz de manejar a la vez.

La oferta actual se compone de marcas de procesadores: Intel, AMD, Cirix, etc, y multitud de modelos dentro de estas marcas. Dual Core, Doble o Doble Núcleo significa que el equipo dispone de un doble procesador.

Los programas de tratamiento de fotografías, videos digitales o gráficos complejos, tales como diseño gráfico o juegos, son los que necesitan una mayor capacidad de proceso.

Memoria RAM: El procesador necesita para trabajar una memoria muy rápida que permita leer y ejecutar las distintas instrucciones, de esto se encarga la memoria RAM. Esta memoria es volátil, es decir, la información escrita en ella desaparece cuando se apaga el equipo. Su capacidad de mide en Megabites MB o Gigabites GB.

Es casi tan importante un procesador rápido como una adecuada capacidad de memoria RAM. Uno de los indicios de que el equipo necesita más memoria RAM puede ser la lentitud al ejecutar aplicaciones.

Memoria Cache: La memoria cache es un tipo de memoria que se sitúa entre el procesador y la memoria RAM para acelerar los intercambios de datos, este tipo de memoria es mucho más rápida que la memoria RAM. Su capacidad de mide en Megabites MB.

La memoria Caché viene predeterminada con el tipo de procesador que se instala en el equipo, más memoria implica más rapidez en la realización de las operaciones entre la memoria RAM y el procesador.

Disco Duro: El disco duro es la unidad para el almacenamiento permanente de información. A diferencia de la Memoria RAM o Cache, este dispositivo guarda la información incluso cuando apagamos el equipo. En el se guarda toda la información del equipo, sistema operativo, programas instalados, configuraciones, documentos de texto, etc. Su capacidad de almacenamiento se mide en Gigabites (GB).

La capacidad del Disco Duro debe ser suficiente para almacenar la información del equipo. Vídeos e imágenes suelen ser los tipos de archivos que más memoria ocupan (una película de video suele ocupar de 600Mb a 4Gb y una imagen, dependiendo del formato y la calidad, entre 56Kb y varios Mb).

Tarjeta gráfica: La tarjeta gráfica es el dispositivo que permite al ordenador mostrar imágenes en pantalla. Las prestaciones de una tarjeta gráfica suelen depender de la cantidad de puntos y de colores que es capaz de mostrar (resolución), y de la cantidad de memoria de que dispone. La tarjeta gráfica debe ir en consonancia con la pantalla o monitor.

Las tarjetas gráficas también incluyen una memoria que permite almacenar las imágenes que después se muestran en el monitor, de una forma más rápida que si se almacenaran en la memoria RAM, facilitando así el tratamiento de imágenes y videos.

Dispositivos de almacenamiento externo: Existen muchos periféricos que permiten leer y grabar datos en soportes externos, así se pueden adquirir disqueteras, unidades de CD, DVD, grabadoras de CD, grabadoras de DVD, discos duros externos, lápices de memoria, etc.

Estos dispositivos permiten el almacenamiento de la información de forma temporal o definitiva.

Componentes para personas discapacitadas: Existen muchos periféricos adaptables dependiendo de tipo de discapacidad, si es motórica, auditiva, visual, psíquica, etc, se deben escoger aquellos que mejor se adapten a la persona que vaya a manejar el equipo. Algunos ejemplos de dispositivos son joysticks, trackballs, teclados silábicos, teclados braille, terminales de lectura braille, micrófonos, pantallas táctiles, sistemas de soplido y absorción, etc, facilitando a las personas con alguna discapacidad el control del equipo por otros medios diferentes a los estándar.

Periféricos: Existen multitud de periféricos que pueden ser utilizados para sacar el máximo partido al equipo, impresoras, escáneres, cámaras, tarjetas de sonido, tarjetas de televisión, etc.

Con esta información debemos ser capaces de solicitar la oferta de un equipo adaptado a nuestras necesidades.

2. Elegir las aplicaciones

La elección de las aplicaciones que van a permitir realizar trabajos en el equipo debe realizarse de forma cuidadosa y planificada.

Una licencia de utilización software permite al propietario que la recibe la utilización de dicho software. En el caso del **software libre** se conceden derechos de uso y en caso del **software comercial** se adquieren derechos de uso. Se debe tener en cuenta que determinado software cuenta con la renuncia de los derechos de autor de los creadores del software, es el caso del **software de dominio público**.

Una vez introducido el término "licencia de uso", se pueden establecer similitudes entre la forma de distribución de las licencias de software que permiten distinguir entre: Software comercial, shareware, de demostración, software libre, de dominio público y freeware.

Software comercial o propietario

En el software comercial, el propietario distribuye licencias de uso mediante la compra de tales derechos. Es el que producen las grandes y pequeñas empresas, los casos más conocidos son Microsoft, Oracle, Adobe, Apple, Panda, Norton, etc., la licencia que se adquiere permite, de forma habitual, su uso en uno o varios equipos y disponer de copias de respaldo. La redistribución o copia no está autorizada en este tipo de licencia.

Software shareware o de evaluación

Es un software que permite su libre distribución o copia durante un periodo limitado de tiempo, transcurrido el cual hay que adquirir la licencia de uso. No está protegido contra copia ya que el autor busca la mayor difusión para el software. Este tipo de software es distribuido por autores y empresas que quieren dar a conocer sus productos.

Software de demostración

Es una formula que se utiliza frecuentemente para la difusión del software comercial ya que es software propietario limitado en funcionalidad y/o tiempo de uso, que se distribuye con fines netamente comerciales. Si el software está limitado en tiempo, se dispone de autorización para su uso, no obstante, al expirar el periodo de demostración, se debe adquirir la licencia comercial o acceder a una nueva versión del software de demostración.

Código abierto u Open Source

La denominación de código abierto se debe a la Free Software Foundation (FSF), entidad que promueve el uso y desarrollo de software de este tipo, en el acuerdo de licencia se autoriza a su uso, copia, distribución, modificación. Uno de los principales exponentes del software libre es el sistema operativo LINUX.

Software de dominio público

Es software libre sin derechos de autor. En este caso los autores renuncian a todos los derechos que les puedan corresponder, por lo tanto es software gratuito de libre uso.

Software libre o freeware

Es un software que se puede usar, copiar y distribuir libremente pero no modificar. No tiene coste alguno para el usuario.

Existe multitud de software comercial, y también gratuito, para casi cualquier función del equipo. Sin embargo, debemos evitar infringir las leyes del copyright y propiedad intelectual utilizando software comercial distribuido de forma fraudulenta (habitualmente conocido como software “pirata”), ya que en la mayoría de los casos no dispone de todas las funcionalidades y no podemos comprobar si realiza acciones no previstas.

A continuación se propone un resumen del software que puede responder a las necesidades básicas de un equipo familiar:

Sistema Operativo (SO)

Es un conjunto de programas (software) destinados a permitir la comunicación del usuario con el ordenador y gestionar sus recursos de manera eficiente. Comienza a trabajar cuando se enciende el ordenador y gestiona el hardware desde los niveles más básicos. El Sistema Operativo es imprescindible para que el ordenador funcione.

Se adoptará una solución comercial que permita la instalación con unos conocimientos mínimos y recibir de forma periódica actualizaciones de seguridad.

Actualmente el mas utilizado es Windows, aunque poco a poco las distribuciones de Linux van ganando terreno al hacer su uso mas intuitivo. También se puede encontrar Macintosh, aunque es más utilizado en entornos profesionales.

Navegador web

Es una aplicación software que permite al usuario acceder y visualizar documentos hipertexto (páginas web) desde servidores web de todo el mundo. Esta red denominada World Wide Web (WWW) está creada sobre internet. Los navegadores permiten acceder y visualizar: gráficos, vídeo, sonido y programas diversos además de texto. Las páginas web, poseen hipervínculos que enlazan una porción de texto o una imagen a otro documento, normalmente relacionado con el texto o la imagen, que son enlaces a otras páginas web. El seguimiento de enlaces de una página a otra, se denomina navegación, origen del nombre “navegador”.

Se utilizará de forma habitual el navegador que proporciona el Sistema Operativo adquirido, sin embargo, para algunas funcionalidades especiales se buscarán otros navegadores freeware.

Los navegadores mas comunes son Internet Explorer, Mozilla Firefox, Netscape y Opera.

Correo Electrónico (e-mail):

Es un servicio que permite el envío y recepción de mensajes. Los mensajes pueden contener texto y todo tipo de ficheros. Para que una persona pueda enviar un correo a otra ambas han de tener una dirección de correo electrónico. La mayoría de los proveedores de correo proporcionan el denominado correo web, que permite el envío y recepción de mensajes desde el navegador.

Existe diverso software para la gestión del correo electrónico en el equipo, aunque es necesario que el proveedor de correo permita esta opción de comunicación entre el programa y el servidor de correo.

Si utilizamos correo web no necesitaremos un software especial para enviar y recibir mensajes vía correo electrónico, ya que podremos hacerlo desde el navegador.

www.regmurcia.es proporciona entre otros muchos servicios una cuenta de correo de forma gratuita.

Mensajería instantánea:

Es una aplicación software que permite la mensajería y que se diferencia del correo electrónico en que el intercambio de información se realiza en tiempo real. Ofrece habitualmente un "aviso de presencia", indicando cuando una persona, de nuestra lista

de contactos, se conecta o el estado en que se encuentra. El usuario se identifica de forma habitual con un "Nickname" o sobrenombre. Algunas de las aplicaciones de mensajería instantánea más utilizadas son ICQ, Yahoo! Messenger, MSN Messenger, AIM (AOL Instant Messenger), Google Talk, etc.

Software de accesibilidad:

Al igual que existe hardware para el equipo que facilita el uso del mismo a personas con algún tipo de discapacidad, también existe software para el mismo cometido. El software existente abarca desde teclados virtuales, lectores de pantalla, reconocedores de voz, magnificadores de pantalla, programas de reconocimiento de textos, visualizadores fonéticos, emuladores de ratón, etc., incluso los sistemas operativos tales como Windows, Linux o Mac, ya tienen funciones para facilitar su manejo.

La mayoría del software de accesibilidad suele ser gratuito, por lo que podemos conseguirlo a través de nuestro distribuidor o por Internet sin coste.

Una vez identificado el equipo y el software necesario estamos en disposición de adquirirlo en la tienda especializada de nuestra elección. Para la financiación del equipo podremos utilizar las líneas de subvención equivalente a los intereses de préstamos para la adquisición de ordenadores con capacidad de conexión a Internet, esta subvención está incluida en el "Programa Internet en casa III" promovido por la Consejería de Industria y Medio Ambiente en el marco del II PlanRegióndeMurciaSI.

3. Configurando el equipo

Una vez recibido y desembalado el equipo en casa, el primer paso será **instalar las aplicaciones y configurar el equipo,** la mayoría de los equipos tienen preinstalado el Sistema Operativo con lo que solamente tendremos que instalar las aplicaciones adicionales que vayamos a utilizar.

Instrucciones para la configuración del equipo:

1. En primer lugar es conveniente **guardar toda la documentación** que acompaña al equipo y a sus periféricos, (manuales, CD de instalación, controladores, etc.), ya que pueden ser de mucha ayuda si se presenta algún problema que obligue a reinstalar el software del equipo.
2. Nos aseguraremos de disponer de todas las **licencias del software que vamos a instalar**. Utilizar software sin licencia genera un riesgo para nuestra información, ya que no dispone de actualizaciones periódicas que solucionen posibles defectos de programación o agujeros de seguridad. Pueden efectuar acciones no solicitadas o no controladas por los usuarios y/o provocar fallos en el sistema incluyendo la pérdida de la información.
3. A continuación instalaremos el **sistema operativo**, en algunos casos el equipo llega con él preinstalado, con lo que solo tendremos que completar la configuración del mismo. En su configuración es recomendable activar el máximo nivel de protección posible, incluyendo las actualizaciones automáticas (si están

disponibles), ya que en cualquier sistema operativo, en mayor o menor medida, se descubren regularmente vulnerabilidades de seguridad, éstas son aprovechadas por malware y hackers para acceder a los equipos con los más diversos fines.

4. También es recomendable activar, si el sistema operativo lo permite, la **instalación automática de actualizaciones** de seguridad; los responsables del software resuelven los "agujeros de seguridad" a través de actualizaciones periódicas del mismo, para evitar que las vulnerabilidades puedan ser utilizadas.
5. Antes de iniciar la instalación de las aplicaciones identificaremos los **usuarios** que van a utilizar el equipo. Es importante crear una cuenta de acceso para cada uno de ellos, reservando la cuenta de administrador solamente para las tareas de mantenimiento. En nuestro caso iniciaremos como usuario administrador, asignaremos una contraseña a este usuario y después crearemos una cuenta personal y una contraseña para cada usuario obligando a todos ellos a iniciar sesión con su cuenta.
6. Debemos intentar que la elección de la **contraseña** de usuario cumpla con unas mínimas características de seguridad, evitando que la contraseña sea igual al nombre de usuario (ejemplo: usuario "angel", contraseña "angel"), seleccionando algo que podamos recordar fácilmente, como, por ejemplo, una frase, (ejemplo: usuario "angel", contraseña "megustalainformatica"), de esta forma crearemos una contraseña mas segura y más fácil de recordar.
7. Las cuentas de acceso que creamos para los distintos usuarios del equipo no deben disponer de **privilegios** de administrador, en especial de permisos para instalar y configurar nuevo software. La restricción de permisos permite evitar que se instale en el equipo software externo, fruto de la navegación por Internet, que pueda dar lugar a problemas de seguridad.
8. Se debe procurar no **compartir unidades**, documentos, etc., a través de la red sin incluir una contraseña que solo conozcan los usuarios que deban acceder. En algunos sistemas operativos aparecen por defecto unidades compartidas (C$, D$, etc.), se debe suprimir esta práctica para evitar el acceso no deseado a las mismas.
9. A continuación seleccionaremos las **aplicaciones** que vamos a utilizar en el futuro, tratando de evitar la instalación de software que no necesitemos, extremando las precauciones si dicho software no proviene de una fuente de confianza.

De momento tras la instalación del sistema operativo y las aplicaciones que hemos seleccionado quedará configurado el equipo para poder utilizarlo, a falta de implantar medidas de seguridad que protejan de las distintas amenazas que puedan producirse.

4. Mantenimiento del equipo

Una de las actividades claves para que el equipo funcione correctamente es su correcto mantenimiento. Mantener el equipo limpio y bien configurado conseguirá prolongar su tiempo de vida y el de la información que almacenamos.

El mantenimiento del equipo se divide en dos tipos de tareas: **mantenimiento físico,** que consiste en la limpieza del equipo y sus componentes y el **mantenimiento lógico,** que incluye la limpieza de datos innecesarios y la reparación de los datos almacenados.

Mantenimiento Físico

Limpieza física:

Es una actividad que merece atención y a la que, de forma habitual, no se le dedica ningún esfuerzo. Los equipos deben limpiarse en su parte exterior e interior, eliminando el polvo depositado y la suciedad en general de ventiladores, placa base, tarjetas incorporadas al equipo, fuente de alimentación, etc. La acumulación de suciedad somete al equipo a mayores temperaturas y esfuerzo para realizar sus funciones, produciendo de esta forma: reducción de su vida útil, incremento del nivel de ruido, roturas y fallos de componentes, lentitud en la ejecución de las aplicaciones, etc.

Es imprescindible desconectar el cableado y la alimentación para realizar una limpieza física del interior del equipo.

Para la limpieza exterior se puede utilizar un paño con productos no abrasivos y para la interior una aspiradora.

Mantenimiento Lógico

Archivos Temporales:

Los archivos temporales son ficheros que crean las aplicaciones utilizadas en el equipo para su propia gestión, por ejemplo, en la instalación del software se suelen crear archivos de configuración de la instalación en carpetas temporales, o al crear un documento de texto, primero se almacena en el directorio temporal, guardando todos los cambios, para después guardarse cuando el usuario así lo requiera en la ubicación elegida. Estos archivos, una vez terminada la actividad con la aplicación ya no son necesarios y algunos no se eliminan automáticamente, quedando almacenados y ocupando espacio en nuestro disco duro, por lo que es conveniente eliminarlos y liberar el espacio ocupado.

Los archivos temporales se almacenan habitualmente en una carpeta llamada Temp del sistema o en las unidades donde se almacenan los ficheros de trabajo

y suelen tener el mismo nombre que el fichero original pero una extensión diferente. Eliminarlos es sencillo y recomendable.

Archivos temporales de Internet:

Otros archivos temporales son los generados por la navegación en Internet. Todas las páginas Web a las que accedemos se almacenan en una carpeta temporal del disco duro del equipo, para agilizar la visualización de la misma. Estos archivos, al igual que los anteriormente mencionados, ocupan espacio en el disco duro y también es conveniente eliminarlos cada cierto tiempo.

- La eliminación de estos archivos se puede hacer desde el mismo navegador.

Desfragmentar el disco duro:

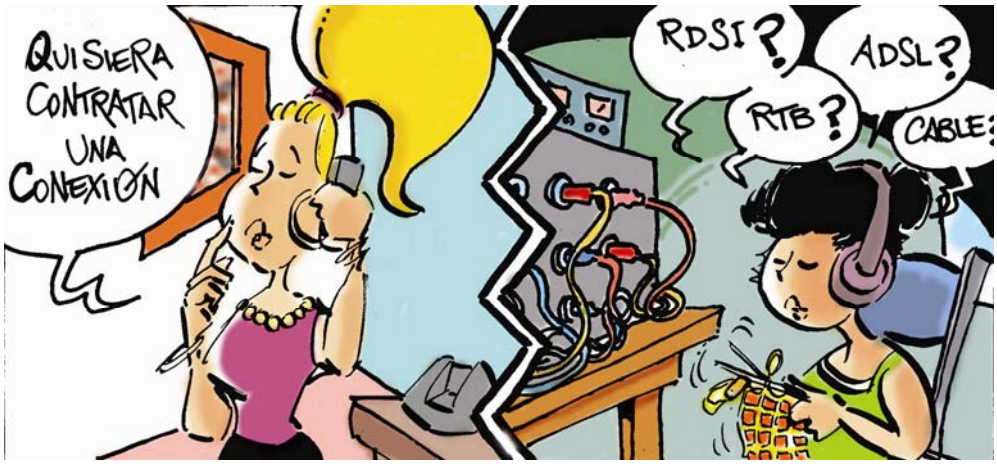
Físicamente los archivos de nuestro ordenador se almacenan en diferentes clústeres (un clúster es la unidad mas pequeña de almacenamiento en un disco duro), con el paso del tiempo los archivos se van fragmentando ocupando clústeres no continuos lo que requiere más tiempo para recuperarlos. Es conveniente usar herramientas de desfragmentación, proporcionadas por el Sistema Operativo o programas especializados, de forma regular, para ordenar la información en el disco duro y agilizar su lectura.

Escaneo del Disco:

Existen aplicaciones para revisar la integridad de los discos duros, sometiéndolos a una revisión minuciosa, buscando posibles errores físicos y reparando o bloqueando los errores detectados para que no dañen los sectores adyacentes. Es conveniente utilizar esta herramienta de mantenimiento de forma planificada para no abusar de ella ya que escanear los discos con demasiada frecuencia hará que estos se sometan a un trabajo excesivo y podría dañarlos.

5. Eligiendo la conexión a Internet apropiada

Ha llegado el momento de conectar el equipo a Internet para disfrutar de los servicios que están esperando en la red.



Existen varios tipos de conexiones, RTB, RDSI, ADSL y Cable y cada una de ellas tiene un ancho de banda distinto (velocidad a la que se transmiten los datos).

RTB

Red Telefónica Básica, permite la navegación a través de la conexión de un módem que fija la velocidad máxima de transmisión de datos en 56.6 Kb/s. Este tipo de acceso a Internet no puede competir con el acceso de Banda Ancha y solamente es recomendable cuando las características técnicas de las comunicaciones impiden otro tipo de acceso.

RDSI

Red Digital de Servicios Integrados (RDSI o ISDN en inglés) facilita conexiones digitales extremo a extremo para proporcionar una amplia gama de servicios, tanto de voz como de datos, y a la que los usuarios acceden a través de un conjunto de interfaces normalizados. Utiliza canales de conexión de 64 Kb/s, permitiendo la unión de 2 canales para un ancho de banda total de 128 Kb/s.

ADSL

Son las siglas de Asymmetric Digital Subscriber Line ("Línea de Abonado Digital Asimétrica"). Es una línea digital de alta velocidad, apoyada en el par simétrico de cobre de la línea telefónica convencional o línea de abonado. En una línea ADSL se establecen tres canales de comunicación: envío de datos, recepción de datos y servicio telefónico normal. Existen versiones mejoradas de ADSL que permiten suministrar televisión y video de alta calidad por el par telefónico. El ADSL permite en su concepción original hasta 8 Mb/s, siendo aumentada esta velocidad por mejoras como ADSL2, ADSL2+, etc., llegando a mas de 20 Mb/s.

CABLE

Este tipo de conexión consiste en la conexión directa desde un “cable modem” instalado en nuestro domicilio con un servidor, este cable es de fibra óptica o coaxial, permitiendo conexiones de hasta 30MB/s, pero siendo necesaria la instalación por un técnico especializado, ya que no basta con la línea telefónica, sino que es necesaria una conexión especial para poder conectarnos.

En todas las modalidades existe la posibilidad de contratar una tarifa plana, en la que se paga una cantidad fija y se puede navegar todo el tiempo que se necesite.

Para cada tipo de conexión existe un equipo que conecta el ordenador a la línea de comunicaciones, existen módems, routers y cable módems, estos equipos deben estar bajo una especial atención y, si es posible, debe ser un profesional el que los configure, ya que a través de ellos se pueden recibir intentos de conexión desde Internet.

6. Conexiones inalámbricas (Wifi)

Cada día es más común en los hogares la instalación de una conexión a Internet inalámbrica, ya que es mucho más cómoda que la convencional, evitando tener que instalar cableado y permitiendo la conexión desde cualquier punto de la casa.

Este tipo de conexiones no suelen tener activa la protección adicional para evitar conexiones externas por parte de otros usuarios, por lo que es recomendable limitar el acceso para permitir la conexión a Internet únicamente a los equipos autorizados y así evitar que nuestra conexión sea utilizada por terceros no autorizados.

La mejor opción para configurar la seguridad en una red inalámbrica es contar con la ayuda de un profesional especializado.

A continuación se relacionarán una serie de medidas para aumentar la seguridad de una red inalámbrica:

Se deben cambiar los valores configurados por defecto en concreto las contraseñas de acceso y el nombre de la red inalámbrica (SSID es el nombre o identificador de nuestra red inalámbrica que utilizan todos los equipos para conectarse a ella y disponer de conexión entre si y a Internet).

Otra opción es ocultar el nombre de la red para evitar su identificación cuando se realice una búsqueda de las redes disponibles.

También se debería configurar la red para utilizar un cifrado mínimo, como puede ser mediante cifrado WEP, WPA o WPA2. El cifrado hace que los datos que transmitimos únicamente puedan ser legibles por los equipos configurados en nuestra red.

También resulta recomendable limitar los equipos que se conectan identificando, de forma concreta, aquellos equipos que tienen autorización para la conexión (Filtrado MAC).

Estas medidas ayudan a disponer de una red inalámbrica más segura.

7. ¿Qué vamos a proteger?

¿Qué contiene el equipo? Información, pero ¿Qué valor tiene la información que queremos almacenar? ¿tiene toda la información el mismo valor? No se puede establecer una adecuada estrategia para proteger la información si no se valora previamente, pensemos un momento en los datos que vamos a almacenar en el equipo:

- Nuestra correspondencia electrónica (e-mails)
- Las fotos de los viajes
- Los videos que hemos grabado en las excursiones
- La cuenta bancaria y la contraseña de acceso a la misma
- El acceso remoto a la oficina y la contraseña para acceder a los sistemas
- Nuestro certificado digital y las ultimas rentas presentadas por internet
- ...

Identificar la información que vamos a almacenar es el primer paso para buscar los mecanismos adecuados para su protección: No se debe invertir en proteger algo más de lo que vale.

En primer lugar podemos intentar valorar la información que se almacenará en el equipo, para ello, debemos pensar en el valor de una perdida parcial o total de la misma (perder un documento o todos los documentos), esta valoración está relacionada con la disponibilidad de la información pero también es importante valorar la

confidencialidad (que no la conozcan otros) y la integridad (que lo que consideramos ultima versión lo sea de verdad). Puede haber información cuya pérdida no ocasione un perjuicio importante pero nadie debe verla o conocer su contenido y viceversa, clasificar la información puede resultar muy útil para saber qué usuarios pueden acceder al equipo y de qué forma.

Se puede establecer una clasificación fácil de la información en: Muy importante, Importante y Prescindible. Será información “Muy importante” aquella que requiera una protección especial, para evitar su pérdida o para restringir su acceso, será información “Importante” aquella cuya recuperación sería necesaria pero no ocasionaría un gran perjuicio su pérdida y será información “Prescindible” aquella que no es preciso mantener.

De esta forma podríamos obtener una tabla similar a la siguiente:

	Muy importante	Importante	Prescindible
E-mails		XX	
Fotografías personales		XX	
Videos grabados de los viajes		XX	
Documentos creados para el trabajo, estudios…	XX		
Datos de la cuenta bancaria y descargas de información del banco	XX		
Certificado Digital y rentas de años anteriores	XX		
Ficheros temporales, información capturada de internet			XX
Aplicaciones descargadas de internet			XX

8. Copias de Seguridad

La copia de seguridad es una de las principales medidas de seguridad para evitar la pérdida de la información almacenada en el equipo. Las copias de seguridad pueden realizarse sobre aplicaciones, ficheros de trabajo o ambas.

El objetivo de una copia de seguridad (también conocida como backup o copia de respaldo) es disponer de una copia de los datos que permita recuperar el sistema o los datos después de un incidente, al estado anterior al mismo. Las copias de seguridad se pueden realizar sobre diferentes soportes, incluso sobre diferentes ubicaciones físicas, así se pueden realizar sobre disco duro, CD-ROM, DVD, memorias flash, etc.

Cada uno de los soportes tiene unas características específicas de velocidad, capacidad y precio acorde a las mismas.

DISCO DURO

Se llama disco duro (en inglés Hard Disk, abreviado como HD) a un dispositivo magnético capaz de almacenar información de forma permanente. Hay distintos estándares para la conexión de un disco duro con el equipo, los más utilizados son IDE/ATA, SCSI, y SATA. La capacidad habitual está comprendida entre los 80 y los 300 GB.

Cuando se instala un disco duro aún no puede ser utilizado por el equipo, debe recibir un formato que permita almacenar información, es lo que se denomina “formatear” el disco.

CD-ROM

CD-ROM (Compact Disk - Read Only Memory, "Disco Compacto de Memoria de Sólo Lectura"), también denominado cederrón (en el Diccionario de la Real Academia Española), es un disco compacto óptico utilizado para almacenar información no volátil, el mismo medio utilizado por los CD de audio. Un CD-ROM estándar puede albergar entre 650 y 700 MB de datos.

Los discos CD-ROM pueden ser de una sola grabación CD-R o de múltiples grabaciones (se pueden sobrescribir y formatear) CD-RW.

Existen equipos lectores de CD-ROM y equipos que son a su vez lectores y grabadores.

DVD

El DVD ("Digital Versatile Disk" o "Disco Versátil Digital") es un disco compacto para almacenar información no volátil, puede ser utilizado para almacenar datos, audio y películas con alta calidad de vídeo.

Al igual que el CD-ROM también existen DVD-R y DVD-RW. Los grabadores pueden ser de una sola capa con lo que se pueden grabar DVD’s con una

capacidad máxima de 9’4GB, o de doble capa, que pueden almacenar hasta 17Gb.

Existen lectores de DVD y grabadores, que a su vez, son lectores.

DISQUETE

También conocido por Floppy o disco, es un dispositivo de almacenamiento de datos de baja capacidad y prácticamente en desuso. Permite almacenar hasta 1.44 Mb de información. Existen lectores y grabadores de disquetes denominados disqueteras.

DISPOSITIVOS DE MEMORIA NO VOLÁTIL

También conocidos como memorias flash, llaves USB, compact flash, smart media, sticks de memoria, tarjetas Secure Digital, etc., estos dispositivos son relativamente costosos por su baja capacidad, pero ofrecen una manejabilidad excelente en su uso.

SERVICIOS REMOTOS DE COPIA DE SEGURIDAD

Aunque este servicio inicialmente fue diseñado para empresas, en la actualidad gracias al incremento del ancho de banda de Internet y de la capacidad que los distintos proveedores ponen a nuestra disposición de forma gratuita, es posible realizar una copia de seguridad de varios GB en cuentas de usuario de Internet.

Una vez conocidos los diferentes tipos de soportes, se puede identificar la información a conservar en copias de seguridad para evitar su pérdida. Se debe tener en cuenta en primer lugar la importancia de la información, solamente se realizarán copias de seguridad de la información “Muy importante” y en algunos casos “Importante”, en segundo lugar se debe tener en cuenta la frecuencia con que cambia la información, pensar en información estática (no cambia frecuentemente, por ejemplos las películas de video, las fotografías…) e información dinámica (cambios frecuentes, por ejemplo los ficheros de trabajo).

Se debe tener en cuenta que el equipo ya dispone de un disco duro en el que se almacena el Sistema Operativo y datos, una opción fácil para mantener una copia de seguridad sería disponer de otro disco duro (interno o externo) en el que realizar de forma periódica (por ejemplo cada semana aproximadamente) una copia de la información “Muy importante” e “Importante”, de esta forma solo se puede perder, como máximo, una semana de trabajo, en el caso de perdida del disco duro principal. La información que no va a cambiar en el futuro puede pasar a un soporte físico más barato que los discos duros pero que garantice una vida a largo plazo, este podría ser el caso de los CD’s y DVD’s. La información que cambia con más facilidad y que requiere una garantía de disponibilidad puede almacenarse de forma diaria en una Llave de memoria.

Sobre este esquema se puede catalogar la información como:

	Muy importante	Importante
Estática	Datos cuenta bancaria. Descargas información del banco. Certificado Digital. Rentas años anteriores.	
Dinámica	Ficheros de trabajo.	E-mails Videos grabados de viajes.

		Fotografías

Por el volumen de información a incluir en la copia de seguridad se pueden utilizar los siguientes soportes:

	Muy importante	Importante
Estática	DVD-RW DVD-R	
Dinámica	DISCO DURO LLAVES USB	CD-RW DVD-RW LLAVES USB

Una vez seleccionado el formato adecuado para cada tipo de información es importante realizar una planificación de copias de seguridad y ponerla en práctica, un modelo que puede servir de referencia podría ser el siguiente:

Realizar copias de seguridad, en el mismo disco duro, en otro directorio denominado CS, BACKUP, COPIASEGURIDAD, o de cualquier otro modo que permita distinguir la copia de los demás datos. Este sistema protege frente a errores en los ficheros, pero no frente a la pérdida del disco.

Adquirir e instalar un segundo disco duro que se conecta al equipo mediante puerto usb (externo) o que se instala internamente. En este disco se puede hacer una copia completa del primer disco duro cada mes (si el disco es externo, se recomienda desconectarlo y guardarlo en un cajón bajo llave).

Para almacenar el material más estático, como por ejemplo las fotografías que hacemos con la cámara, se pueden adquirir y grabar CD's (cada CD tiene una capacidad de 640Mb y puede almacenar unas 1000 fotografías de 640 Kb cada una), es importante etiquetar y almacenar los CD's con cuidado. Si se requiere una capacidad mayor se pueden utilizar DVD'S (con capacidad desde 4,7Gb a 17Gb).

Para la información "Muy Importante" cada usuario puede disponer de su propia copia de seguridad en una llave de memoria usb, con capacidad de 1 o 2Gb y un precio muy asequible, esta puede ser una opción para la información más personal.

Es importante cuidar el almacenamiento de los soportes identificando y guardando en un cajón bajo llave todos los CD's con software, manuales, garantías, etc., que recibimos al comprar el equipo, la impresora, los equipos, periféricos y software adicionales, de esta forma estarán disponibles si se presenta algún problema en el futuro.

9. Amenazas en Internet

Las ventajas de Internet son indudables y hoy día la mayoría del ocio y servicios tiene una versión en esta red. Internet ha facilitado el acceso a trabajo, ocio y conocimiento a millones de personas con un acceso fácil e inmediato a una cantidad extensa y diversa de información.

La mayor parte de los usuarios creen que navegar por Internet es una actividad anónima y en realidad no lo es. Los usuarios al navegar por Internet utilizan una seña de identidad o identificador, es la dirección IP que asigna a su equipo el proveedor de acceso a internet. Esta IP queda reflejada en todo lo que se realiza, (visitas a páginas Web, mensajes en foros, descargas de información…), además, en los últimos años, los servidores de conexión a Internet y los de servicios como el correo electrónico o ISPs en España están obligados por ley a guardar dichos registros por seguridad, de esta forma, se podría saber quien ha modificado una determinada pagina Web en cierto momento uniendo los registros del servidor de webs y del servidor de Internet.

Prácticamente todo lo que se transmite por Internet puede archivarse, incluso los mensajes en foros, chats, programas de mensajería, páginas visitadas, etc., los proveedores de Internet y los operadores de sitios web tienen la capacidad de recopilar dicha información.

La información en Internet fluye a gran velocidad y puede alcanzar a un gran numero de personas, tanto la que se encuentra como la que se emite a través de esta gran red tiene los mismos derechos y obligaciones de copyright, por lo que si el usuario publica información, deberá enfrentarse a las posibles infracciones, demandas, juicios, etc., a las que puedan dar lugar sus publicaciones.

Internet ofrece muchas ventajas, pero también conlleva riesgos que todo usuario debe conocer e intentar evitar, algunos destacables son:.

- Recopilación de información poco fiable.
- Acceso a información no solicitada en muchos casos, (inapropiada, inmoral o peligrosa).
- Estafas
- Compras inducidas por publicidad abusiva
- Robos de información, códigos secretos, números de tarjetas de crédito
- Páginas webs falsificadas
- Virus insertados en páginas webs o pop-ups
- Avisos de seguridad fraudulentos que intentan que nos instalemos un software o accedamos a una pagina para solucionarlos
- Solicitudes de información personal abusiva para el alta paginas, en foros, etc.

Las herramientas imprescindibles para la navegación son:

NAVEGADORES

Para acceder al contenido de las páginas Web que existen en Internet, utilizamos los "**navegadores**" o "exploradores". Un navegador se puede obtener de varias formas, descargándolo desde internet (en este caso, siempre es recomendable hacerlo desde la página del fabricante), algunos como "Internet Explorer" se distribuyen con Sistemas Operativos y también se pueden obtener en revistas y publicaciones especializadas. Los navegadores más conocidos son Internet Explorer, Mozilla Firefox y Netscape, y permiten una navegación con prestaciones similares.

BUSCADORES

El primer servicio y uno de los más utilizados es el de búsqueda de contenidos web, para ello se utilizan los programas denominados "**buscadores"** que son realmente bases de datos que almacenan información de las páginas web que permiten su búsqueda (titulo, contenido, palabras clave, etc.). Los navegadores permiten buscar y encontrar otras páginas web relacionadas con los conceptos introducidos en la búsqueda. Existen diferentes buscadores entre los que destacamos por su velocidad y sencillez de manejo google o yahoo, y por su tradición altavista, lycos, msn, etc.

Una vez ejecutado el navegador y accesible su página Web, ya estamos conectados a Internet, la **información** que viaja entre nuestro ordenador y las páginas web que visitamos fluye como se denomina habitualmente "**en claro**", este concepto sirve para identificar que la información no está cifrada, es decir, si otro usuario intercepta la comunicación podría ver lo mismo que vemos nosotros. La probabilidad de que esto ocurra no es muy alta, pero conviene conocer que existe.

Cuando tratamos información "muy importante", como la información bancaria o el acceso a servicios de la Administración Pública, se utilizan técnicas para el cifrado de las comunicaciones. Una de las más comunes, es el protocolo https, este tipo de conexión establece una comunicación cifrada entre el servidor y nuestro navegador, para evitar que un tercero pueda interceptar y leer el contenido de dicha comunicación.

AMENAZAS

En prácticamente cualquier servicio, acceso, fichero, etc., puede encubrirse código que dañe o recoja información confidencial en el equipo, para detectar y evitar este tipo de amenazas se deben adoptar medidas de protección específicas.

VIRUS

Un virus informático es un programa que se copia automáticamente y que tiene por objeto alterar el normal funcionamiento del equipo, sin el permiso o conocimiento del usuario. Los virus, habitualmente, reemplazan archivos ejecutables por otros infectados, pueden destruir, de manera intencionada, los datos almacenados en un ordenador, aunque también existen otros menos malignos pero igualmente molestos.

El Virus informático se ejecuta cuando el usuario accede o ejecuta un programa que está infectado, el código del virus queda residente (alojado) en la memoria RAM del ordenador y toma entonces el control de los servicios básicos del sistema operativo, infectando, de manera posterior, archivos ejecutables.

Se pueden destacar como los virus más populares los Worms o gusanos que se multiplican ocupando la memoria y volviendo lento al ordenador y los Troyanos que suelen ser los más peligrosos y funcionan igual que el caballo de troya atacando al ser activados.

SPAM

Spam (o correo basura) son mensajes no solicitados, normalmente con publicidad y enviados de forma masiva. El medio habitual de enviar spam es el correo electrónico. En España el spam está prohibido por la Ley de Servicios de la Sociedad de la Información y de Comercio Electrónico (LSSICE), publicada en el BOE del 12 de julio de 2002 y por la Ley Orgánica de Protección de Datos (LOPD).

PHISHING

Es un término utilizado para denominar al intento de acceder a información confidencial de forma fraudulenta, como puede ser una contraseña o información detallada sobre tarjetas de crédito u otra información bancaria.

El estafador se hace pasar por una persona o empresa de confianza en una aparente comunicación oficial electrónica, por lo común un correo electrónico, algún sistema de mensajería instantánea o incluso utilizando también llamadas telefónicas.

SPYWARE

Se denomina spyware a los programas creados para recopilar información sobre personas u organizaciones sin su conocimiento. Los programas pueden capturar correo electrónico, password, dirección IP y DNS, teléfono, país, páginas que se visitan, tiempos y frecuencia de visita, software instalado, compras, tarjetas cuentas bancarias, etc.

Los programas espía pueden ser instalados en un ordenador mediante un virus, un troyano que se distribuye por correo electrónico, o bien puede estar oculto en la instalación de un programa aparentemente inocuo.

Los programas de recolección de datos, instalados con el conocimiento del usuario no son realmente programas espías si el usuario comprende plenamente qué datos están siendo recopilados y a quién se distribuyen.

COOKIES

Son un conocido mecanismo que almacena información sobre un usuario de internet en su propio ordenador, y permite identificar las páginas web que visita, mediante la asignación de una identificación individual.

VENTANAS EMERGENTES O POP-UPS

Es un elemento más de la navegación, los pop-ups son ventanas que aparecen sin autorización al entrar en alguna Web, también se les denomina ventanas emergentes. Existe la posibilidad de bloquear en los navegadores la aparición de este tipo de ventanas. En ocasiones, los pop-up que aparecen en una simple ventana pueden acarrear un riesgo de seguridad importante para el equipo, ya que a través de ese pop-up se puede instalar o cargar algún tipo de malware que infecte el equipo o robe nuestra información.

Hoy día existen pop-ups que utilizan la ingeniería social para hacer que el usuario acceda al enlace o hacer que instale algún programa por propia voluntad, por ejemplo, indicándole que su equipo está infectado.

MALWARE

En los últimos años han aparecido tantos tipos de virus (virus, gusanos, troyanos, dialers, jokes, exploits, blackdoors, etc.) que se ha utilizado Malware (Malicius Software o Software Malicioso) como denominación común para todo este tipo de software. La abundancia de este software lo ha convertido en un elemento común en la informática y la navegación por Internet, hoy día un equipo desprotegido es un equipo candidato a ser infectado.

MEDIDAS DE SEGURIDAD

Para evitar las amenazas que se pueden presentar en la navegación se deben seleccionar medidas específicas de apoyo para proteger el equipo, a continuación se relacionan algunas de las más importantes:

ANTIVIRUS

Son programas que tratan de descubrir las trazas que ha dejado un software malicioso para detectarlo y eliminarlo y, en algunos casos, contener o parar la contaminación. Tratan de tener controlado el sistema mientras funciona parando las vías conocidas de infección y notificando al usuario de posibles incidencias de seguridad.

CORTAFUEGOS

La instalación de un Cortafuegos (firewall) en el equipo es una medida que permitirá controlar las conexiones que se realizan a través de Internet desde nuestro equipo o dirigidas al mismo.

Los Cortafuegos controlan la información que llega o se envía desde nuestro ordenador, permitiendo o denegando la comunicación de las aplicaciones que utilizamos con el exterior; el usuario tendrá la responsabilidad de decidir los programas que permite que se comuniquen con el exterior y los que no.

Con un Cortafuegos instalado y configurado en el equipo se pueden evitar muchos problemas de seguridad, aplicando el principio de solamente autorizar las comunicaciones que se hayan ordenado.

ANTISPAM

Aplicaciones que se encargan de detectar y bloquear el correo basura.

ANTISPYWARE

Los antivirus más recientes son capaces de monitorizar y bloquear los archivos espías. Se recomienda no usar un solo programa antiespía sino una combinación de varios dado que, en muchas ocasiones, uno de ellos detecta algunas cosas que no encuentran los otros, y viceversa, por lo que el uso combinado, de varios de ellos, ofrece una protección más completa.

ACTUACIONES PARA PROTEGER EL EQUIPO

El primer paso para la protección del equipo y nuestros datos es la correcta actualización del software utilizado (sistema operativo, navegador, gestor de descargas, etc.).

Los sistemas operativos son aplicaciones muy complejas que cada día tienen que interactuar con un mayor número de hardware y software, este hecho motiva que regularmente aparezcan fallos o “bugs” que pueden representar agujeros de seguridad. Los fabricantes publican regularmente actualizaciones que corrigen dichos fallos, por eso es importante activar la opción de descargar actualizaciones para proteger el equipo de dichos errores en seguridad.

El segundo paso para la protección de malware es la instalación de un software específico en el equipo que evite su instalación y lo elimine en caso de detectarlo. Estas

son las principales características que se deben evaluar al elegir el software de seguridad para instalar en el equipo:

- El tipo de Malware que detecta (virus, gusanos, troyanos, spywares, etc.).
- La velocidad con que aparecen actualizaciones para detectar nuevos virus (al menos una vez al día) y si estas se realizan de forma automática.
- Los recursos que utiliza cuando está en ejecución (que no ralentice el equipo cuando se usa normalmente).
- El tipo de archivos que examina (ejecutables, paginas Web, correos electrónicos, etc.).
- El tiempo que tarda en hacer un análisis completo del disco duro.
- Si permite el análisis de recursos de red compartidos.
- Su facilidad de instalación y configuración.
- Si permite programar actuaciones con antelación (analizar el disco duro a una hora y día predeterminados).
- El idioma del programa, la ayuda y el soporte técnico.

Después de todo lo visto anteriormente, se puede decir que un programa anti-malware, un Cortafuegos configurado, la descarga e instalación de las actualizaciones del software y la responsabilidad de los usuarios, constituyen una gran defensa para nuestro equipo y la información que almacena.

10. Como reconocer una infección

Los razonamientos del tipo “tengo antivirus y estoy protegido”, “tengo firewall y nadie puede entrar en mi equipo”, “yo solo uso Internet para leer el correo” o “mi sistema no es importante para un hacker” impulsan a los usuarios a despreocuparse de la seguridad de sus equipos.

La mayoría de las veces la infección se realiza por desconocimiento o confianza en los nuevos sistemas de comunicación como Internet y en los equipos informáticos.

Los equipos pueden ser infectados de varias maneras:

- Por unidades de disco extraíbles (Disquetes, CD’s, DVD’s, etc.).
- Redes de ordenadores.
- Por correo electrónico.
- Desde páginas Webs.
- Desde programas de intercambio P2P.
- Desde programas de mensajería instantánea.

Hay ciertos indicios que delatan la posible presencia de Malware u otras amenazas en el equipo (aunque también pueden deberse a otros problemas ajenos a los virus). Algunos son:

- Lentitud repentina del equipo, sin causa aparente.
- Imposibilidad de abrir ciertos ficheros o determinadas aplicaciones.
- Desaparición de ficheros y carpetas.
- Aparición en la pantalla de avisos o mensajes de texto inesperados.
- Disminución repentina del espacio en el disco o de la capacidad de memoria.
- Alteración inesperada en las propiedades de un fichero.
- Aparición de errores en el sistema operativo o bloqueo del equipo al ejecutar tareas sencillas.
- El ordenador se apaga o reinicia repentinamente sin motivo aparente.
- El teclado y el ratón no funcionan correctamente o lo hacen de modo aleatorio.
- Aparición o desaparición de iconos en el escritorio.
- Cambios en la página de inicio de nuestro navegador.

Indicios de infección por spyware:

- Cambio en las páginas de inicio, error y búsqueda del navegador.
- Aparición de ventanas "pop-ups", incluso sin estar conectados y sin tener el navegador abierto.
- Barras de búsquedas de sitios web que no se pueden eliminar.
- Botones que aparecen en la barra de herramientas del navegador y no se pueden quitar.
- La navegación por la red se hace cada vez más lenta, y con más problemas.
- Bloqueo del panel de control y de determinados iconos de programas.
- Aparición de un mensaje de infección, así como un enlace web para descargar un supuesto antispyware.
- Denegación de servicios de correo y mensajería instantánea.
- Creación de carpetas tanto en el directorio raíz, como en otros.
- Modificación de valores de registro.

Es importante que todo usuario que utilice Internet tenga un conocimiento mínimo de las amenazas que existen y que el funcionamiento anormal del equipo que puede hacer sospechar de la existencia de virus o malware.

11. Utilizando el correo electrónico

El correo electrónico o e-mail (Electronic mail), es uno de los servicios de Internet más populares de Internet, permite a los usuarios intercambiar (enviar y recibir), mensajes escritos con otros usuarios de Internet, sin coste alguno.

Por medio de mensajes de correo electrónico se puede enviar, no solamente texto, sino todo tipo de documentos; su eficiencia, conveniencia y bajo costo están logrando que el correo electrónico desplace al correo normal para muchos usos habituales.

Las características mas conocidas del correo electrónico son su inmediatez, (un mensaje puede llegar a su destinatario en unos segundos), su coste (permite enviar mensajes a cualquier parte del mundo con el único coste del acceso a Internet) y ser asíncrono, es decir, no es necesario que el destinatario de un mensaje esté frente a la pantalla en el momento en el que se le envía, ni que su ordenador esté conectado a Internet.

Conseguir una cuenta de correo electrónico es muy sencillo, existen proveedores de acceso a Internet, operadores de comunicaciones e incluso organizaciones públicas que permiten disponer de una de forma totalmente gratuita. Tal es el caso de www.regmurcia.com, a través de esta página web se puede obtener una dirección de mail totalmente gratuita en el dominio regmurcia.com

Dada la popularidad de este servicio y su difusión, ha sido uno de los medios más utilizado por atacantes para el envío de Malware, ataques de Phishing, envío de Spam, etc.

La protección del correo electrónico forma parte de la protección de nuestra información y debe ser uno de los aspectos a proteger. Para ello, a continuación se relacionan unas pautas a seguir:

Recomendaciones al navegante:

Precauciones para evitar el correo basura

- No incluir la dirección como texto, mejor mostrarla como una imagen.
- Utilizar redirecciones que se pueden borrar cuando se reciba excesivo spam.
- Modificar la dirección para evitar el rastreo automático. Por ejemplo, cambiar @ por ARROBA, las oes por ceros.
- Utilizar cuentas temporales.
- Rechazar correos de orígenes no conocidos.
- Utilizar CCO (copia oculta), en lugar de Para o CC, cuando el mensaje vaya dirigido a más de un destinatario.
- Al rellenar una inscripción a un sitio que no sea de confianza no introducir el correo y si es imprescindible utilizar una dirección temporal.
- Leer los correos como texto, y no como HTML.
- No solicitar el cese de envío de spam, además de inútil confirmamos la existencia y vigencia de la cuenta.
- Tener siempre al día las actualizaciones de seguridad del sistema operativo.
- Instalar un cortafuegos (firewall) que evite los intentos de acceso externos.
- Instalar un software anti-Spam que bloquee los posibles correos Spam que lleguen a nuestra dirección.
- Instalar un software antivirus que permita escanear los correos entrantes y sobre todo los anexos que incluyan.
- No creer los mensajes que alertan sobre algún tipo de peligro ya que son utilizados para recopilar cuentas de correo activas.
- Es recomendable tener una cuenta secundaria para solicitar información en páginas Web, participar en foros, etc., y de esta forma hacer accesible nuestra cuenta principal solo a personas de confianza.
- Y sobre todo, utilizar el sentido común, si el correo recibido parece un virus o spam, lo mas probable es que lo sea, por ello, es mejor no abrirlo.

Mención especial merecen las cadenas de mensajes ya que son uno de los engaños más utilizados por las empresas que se dedican a recopilar correos electrónicos para el envío de spam, convirtiéndose en una de las mayores lacras de Internet.

Estas cadenas son conocidas como Hoaxes, y su objetivo principal es la recopilación de cuentas de correo electrónico para posteriormente enviar e-mails con fines comerciales. Estos correos tratan de ganar la confianza de los usuarios aportando datos que parecen ciertos y proponiendo una serie de acciones, ninguna empresa va a dar dinero a alguien por el número de correos enviados para una operación a corazón abierto, ni eliminarán la cuenta si no envías un mail.

Una buena forma de reenviar de forma segura mails a varios de nuestros contactos es utilizar la copia oculta, la copia oculta hace que no se muestre en los destinatarios todos los contactos a los que se les ha enviado el mail. Para enviar un mensaje de esta forma se debe poner a todos los destinatarios en la línea denominada como “CCO” en vez de en la línea “Para”. También es importante al reenviar un mensaje eliminar todas las direcciones de correo que aparecen en el cuerpo del mismo, para evitar reenvíos con spam.

12. Permitir o no permitir las cookies

¿Qué son exactamente las cookies?

Se ha definido “cookie” en el capítulo de Amenazas en Internet como un conocido mecanismo que almacena información sobre un usuario de internet en su propio ordenador y permite identificar las páginas web que visita mediante la asignación de una identificación individual.

En realidad, suelen ser archivos de texto que guardan algunas páginas Web en la carpeta temporal del ordenador, para recordar algunos datos concernientes al usuario y la visita que realizada a su página web. Almacena información como las preferencias de visualización, nombre y contraseña, productos visualizados, etc.

Al ser archivos de texto son elementos pasivos, es decir, no pueden emprender ninguna acción en el equipo, ni pueden infectarlo con ningún tipo de malware, también son difícilmente editables.

El objetivo de las cookies es facilitar la navegación de los usuarios permitiendo personalizar y adecuar las páginas por las que navegan habitualmente a sus gustos y hábitos de navegación. Por este motivo, el uso de algunas cookies se puede entender que vulnera la intimidad del usuario, incluso algunos virus pueden acceder al equipo y recuperar las cookies almacenadas para estudiar nuestros hábitos de navegación, por ejemplo, en nuestros bancos.

En cualquier caso, los navegadores más comunes como puede ser Internet Explorer, Mozilla Firefox, Netscape, etc., se pueden configurar para no recibir cookies o recibir solo de webs especificas, pero siempre hay que tener en cuenta que determinadas páginas web necesitan del uso de cookies para su correcto funcionamiento, por ejemplo las páginas que ofrecen comercio electrónico basado en carrito de la compra.

13. Fraudes a través de Internet

Internet se ha configurado en la actualidad como un medio de comunicación más en nuestra vida cotidiana, además permite la búsqueda y recuperación de información y la realización de compras y negocios. En el comercio electrónico y la búsqueda de nuevos negocios existen amenazas al desconocer la identidad del usuario con el que se contacta.

Son destacables las técnicas de Ingeniería Social, que consisten en engañar al usuario para provocar que facilite datos personales, cuentas bancarias, nº tarjeta de crédito, claves, etc.

Los fraudes a través de Internet son cada día más profesionales y más difíciles de distinguir, por lo que toda precaución para evitarlos es poca. De todos los fraudes conocidos vamos a destacar algunos, por ser los más comunes, sobre los que conviene estar prevenido:

Phishing:

Citado en el apartado de amenazas en Internet, quizá es el más conocido, ya que se ha dado a conocer en los medios de comunicación al afectar, sobre todo, a distintos bancos.

Esta estafa consiste en engañar al usuario suplantando la identidad de una empresa o entidad pública, solicitándole datos. El contacto con el usuario suele producirse de varias formas, desde mensajes a móviles, llamadas telefónicas, webs falsas, etc., aunque la más extendida es mediante correo electrónico. De esta forma se hace creer al usuario que realmente los datos solicitados proceden del sitio oficial cuando en realidad no lo es. En el contacto con el usuario se trata de averiguar sus datos, claves, cuentas bancarias, números de tarjeta de crédito, etc., en definitiva todos los datos posibles, para un uso fraudulento posterior como la realización de compras por Internet con tarjeta de crédito o la realización de cargos en su cuenta bancaria.

La mayoría de los programas anti-phishing trabajan identificando contenidos phishing en sitios web y correos electrónicos. Algunas aplicaciones anti-phishing pueden, por ejemplo, integrarse con los navegadores web y clientes de correo electrónico como una barra de herramientas que muestra el dominio real del sitio visitado.

Una medida muy eficaz es el sentido común, ningún banco u organización va a pedir su contraseña por mail.

Webs falsas de recargas:

Aprovechando el extraordinario aumento del uso de la telefonía móvil, varios estafadores han creado páginas falsas para recarga de teléfonos móviles, prometiendo recargas extras o más económicas y solicitando para la realización de la recarga sus datos personales y un numero de cuenta o tarjeta.

El único fin que persiguen estas páginas, al igual que las anteriores, es conseguir los datos del usuario, no realizando nunca la recarga solicitada.

Para evitar estos dos tipos de estafas (Phishing y webs falsas de recargas), se aconseja realizar siempre todas las operaciones a través de las páginas oficiales de los proveedores, y en caso de duda pedir información sobre la solicitud de datos recibida.

Phishing-car:

Este tipo de estafas va en aumento, utilizando páginas de ventas de coches similares a empresas de prestigio y realizando ofertas llamativas de vehículos lujosos a muy bajo precio. En estas páginas solicitan el pago previo de una señal para la reserva del vehiculo.

Lo más destacable para darse cuenta de este tipo de fraudes es que el pago de la señal se realiza por medio de empresas de envío de dinero a otros países, que el vendedor le oferta la entrega a domicilio, que en un alto porcentaje de los casos el vehiculo que venden se encuentra fuera del país, de manera que el usuario solo puede verlo en fotos, que le piden una importante cantidad de dinero como primera señal y que la captación de los usuarios suele ser mediante anuncios en paginas de venta de coches de segunda mano o por email.

Loterías falsas:

Este tipo de estafas suele realizarse por mail, enviando al usuario un correo donde informan que ha sido agraciado con un premio de lotería. Cuando el usuario contesta al mail le solicitan sus datos bancarios para realizar el ingreso del falso premio.

En otros casos se solicita una parte del importe del premio para cobrarlo entero, ya que al ser una lotería de otro país debe pagar impuestos.

Ofertas falsas de trabajo:

Este tipo de estafas consiste en la captación de personas por medio de correos, anuncios en webs de trabajo, chats, etc., donde empresas ficticias ofrecen trabajar cómodamente desde casa y cobrando altos beneficios.

En el trabajo se solicita al usuario una cuenta bancaria, donde el usuario recibirá transferencias bancarias, para posteriormente enviar el dinero a países extranjeros. Incluso en algunos casos envían un contrato falso para hacer mas creíble la oferta.

Sin saberlo, la victima está blanqueando dinero obtenido por medio del Phishing.

14. Utilizando programas de Mensajería instantánea

Se conoce como Mensajería Instantánea a un conjunto de programas para enviar y recibir mensajes instantáneos con otros usuarios conectados a Internet u otras redes.

La mensajería instantánea se ha convertido en uno de los sistemas mas utilizados para el intercambio de mensajes entre usuarios, debido a que la comunicación entre los participantes es en tiempo real y además, avisa cuando algún contacto se conecta o alguien quiere entablar una conversación.

Todos los productos de mensajería instantánea están basados en la conexión directa de los usuarios con su servidor y este a su vez con otros servidores.

Hoy día, los programas de mensajería no se limitan al intercambio de mensajes, sino que permiten el envío de archivos, compartir carpetas, realizar llamadas de voz, videoconferencias, etc., incluso en algunos es posible permitir a usuarios tomar el control de nuestro equipo.

Existen varios problemas de seguridad en el uso de este tipo de mensajería, destacando el factor humano, un hacker no necesita conocer la IP de un usuario para enviarle malware, ya que, para el es un contacto, lo único que tiene que hacer es convencer al usuario para que se lo descargue.

Para hacer más seguras las comunicaciones a través de este tipo de programas es recomendable no facilitar información personal confidencial a través de este tipo de programas y no abrir imágenes, ni descargar archivos o acceder a vínculos de mensajes de desconocidos.

Existe la posibilidad de que nuestro interlocutor no sea realmente quien pensamos que es. Algunos delincuentes han utilizado este método para sacar información o quedar con sus victimas haciéndose pasar por otras personas.

15. Utilizando programas de intercambio P2P

Los programas de intercambio de archivos P2P como emule, kazaa, BitTorrent, etc., cada vez son mas utilizados por los usuarios de Internet para compartir y descargar archivos compartidos de los demás usuarios. La traducción mas utilizada para P2P (peer to peer) es “de igual a igual”, que describe este tipo de programas.

Los usuarios de este tipo de redes actúan a la vez como clientes y servidores de los demás usuarios de la red. Estas redes se basan principalmente en la filosofía e ideales de que todos los usuarios deben compartir.

Son los usuarios los que controlan lo que comparten, y esto hace que se puedan encontrar contenidos que no son lo que dicen ser, malware, archivos ilegales protegidos con derechos de autor, etc., se mezclan con contenidos generados por los usuarios que los comparten.

En todo momento hay que respetar la propiedad intelectual y los derechos de autor por lo que este tipo de redes de intercambio deben utilizarse siempre cumpliendo la legislación vigente.

Uno de los principales peligros de descargar software de redes P2P es el anonimato de los usuarios ya que es el servidor de la red el que redirige a los demás usuarios.

El uso de las redes P2P debe realizarse siempre con la mayor protección posible para nuestra información, (antivirus, antispam, firewall, etc.), buscando virus en cada archivo sospechoso.

16. Control del acceso a Internet por menores

Internet es apasionante para los menores, con interesantes formas de comunicación y aprendizaje, que no dudan en aprovechar por completo. Cada vez hay más niños que se conectan a Internet con frecuencia, para comunicarse con los amigos, trabajar en proyectos escolares y jugar. Se debe tener en cuenta que Internet ofrece múltiples ventajas pero también alberga peligros, es un mundo que contiene imágenes y lenguaje inadecuado y en el que los navegantes pueden esconder fácilmente su identidad.

Los padres deben vigilar las actividades de sus hijos en Internet, en especial, en los contactos con otros usuarios.

Estos son algunas recomendaciones para proteger a los menores y enseñarles a manejar Internet:

1. Lo más importante es mantener una buena comunicación con los menores, hablando sobre los distintos contenidos webs que se pueden encontrar por Internet, en correos electrónicos, etc., invitándoles a que confíen en nosotros cuando vean texto o imágenes inadecuadas.
2. Vigilar las distintas actividades que realiza el menor en Internet, como la mensajería instantánea, descargas, accesos a páginas webs y juegos virtuales.
3. Enseñar a los menores a no dar información personal cuando naveguen por Internet.
4. Proteger las contraseñas creando nombres genéricos que no revelen ningún tipo de información personal.
5. Enseñar a los menores a nunca hablar con extraños cuando estén en línea, y si un extraño les formula preguntas desagradables o hace que se sientan mal, deben desconectarse e informar inmediatamente.
6. Y la última y no menos importante, una vez que se ha educado a los menores y se han establecido algunas directrices demuéstreles confianza, asegurándose que comprenden su preocupación.

INICIATIVAS DE LA ADMINISTRACIÓN REGIONAL DE MURCIA.

El Plan Estratégico de la Región de Murcia 2007-2013 es la apuesta del Gobierno Regional para impulsar a la Región de Murcia durante los próximos 7 años. Entre sus principales objetivos incluye el Fomento de la Sociedad del Conocimiento con el objetivo estratégico de aumentar el uso de las TIC en la ciudadanía, apoyado en el número de hogares con Banda Ancha, el porcentaje de personas que han comprado por Internet en los últimos tres meses o el uso de los servicios de la e-administración por parte de los ciudadanos.

Por su parte el Plan de Desarrollo de la Sociedad de la Información 2005-2007, recoge líneas de apoyo para la puesta en marcha, de una forma inmediata, de la Sociedad del Conocimiento entre la ciudadanía, así ayudas para adquisición de ordenadores para el hogar, ayudas para la incorporación de la banda Ancha en el hogar, ayudas a colectivos desfavorecidos para su incorporación a la Sociedad de la Información, proyectos de Alfabetización Tecnológica, Formación, Sensibilización, etc., son un conjunto de oportunidades para que los ciudadanos no quedemos descolgados de la Sociedad del Conocimiento.

El apoyo institucional y la evolución de la tecnología han permitido que los indicadores relacionados con la presencia de ordenadores en los hogares crezcan anualmente convergiendo con los modelos europeos, sin embargo, el problema de la seguridad de la información no ha seguido un esfuerzo paralelo a la incorporación de tecnología, el resultado es que existe un problema derivado del uso de la tecnología que necesita respuestas urgentes.

Tal y como se destacó en el primer capítulo, esta guía de seguridad se presenta con el objetivo de sensibilizar a los ciudadanos sobre la importancia de la seguridad en el uso de las nuevas tecnologías, recomendando soluciones sencillas que permitan su incorporación a la Sociedad del Conocimiento de forma segura y controlada, evitando riesgos innecesarios y problemas por desconocimiento de ese nuevo mundo que es Internet.