Seguridad en Internet (PCs)

Contenido:

- Conocer los principales problemas de seguridad en Internet.
- Aplicar las medidas oportunas que mejoren nuestra seguridad.
- Vídeo: "Consejos para operar con seguridad en Internet".

Riesgos de la navegación por Internet

Hoy en día, los dispositivos informáticos (smartphone, PC), no se consideran como entes aislados, sino que están integrados en redes que a su vez están todas conectadas entre sí (Internet).

Es más, actualmente, el acceso a Internet se realiza mediante sistemas de conectividad que hace que nuestra conexión con Internet esté abierta casi todo el tiempo (smartphone, router).

Los riesgos a la seguridad en los dispositivos informáticos conectados a Internet se pueden clasificar según el objeto del ataque:

- Robo de identidad
- Virus, gusanos y troyanos
- Spyware
- Hackers y crackers
- Phishing y estafas on line
- Spam
- Contenidos Web inapropiados

Los riesgos listados no tienen por qué aparecer de manera aislada, sino que en la mayoría de las ocasiones actúan interrelacionados, de manera conjunta.

Hagamos una breve descripción de cada una de las amenazas.

El robo de identidad

El robo de identidad en Internet tiene siempre un fin ilícito y puede actuar en la búsqueda de diversos objetivos.

Desde su perspectiva más inocua, busca conocer los patrones de navegación del internauta con el fin de conocer sus gustos e intereses y con ello generar respuestas publicitarias con las que invadir al usuario en la búsqueda de que se pueda hacer negocio con él. La tecnología que subyace preferentemente es el uso de **cookies**, pequeños archivos en los que el navegador almacena información del usuario para guardarlo de una sesión a otra.

Cuando un usuario accede a una página de Internet, ésta deja una cookie en su sistema que empieza a llenarse con la huella de su actividad (por dónde ha navegado, que datos ha proporcionado a la red, etc.). Cuando se vuelve a navegar nuevamente por la página, se recoge la información de la cookie.

No todas las cookies son maliciosas. Algunos sitios Web precisan de ellas para poder ofrecer sus servicios al usuario.

La relación de usuarios y sus preferencias de navegación constituyen en sí mismo un negocio lucrativo pues se venden a empresas dedicadas a la publicidad.

Desde una perspectiva algo más agresiva, lo que se busca directamente es capturar los datos de identificación del usuario para posteriormente operar en su nombre en acciones ilegales, o directamente, sustraerle su identidad (login, clave de acceso) con el fin de directamente proceder a robarle en su banca electrónica o realizar compras por Internet y cargárselas a su cuenta bancaria.

Virus, gusanos y troyanos

Los **virus** informáticos tienen dos fines básicos. Por un lado, infectar cuantos más equipos y más rápido, mejor y por otro lado, provocar la pérdida de información, ralentización e incluso el deterioro de la máquina hasta dejarla no operativa.

Si bien los primeros virus informáticos entraban más en la categoría de reto para sus diseñadores, con consecuencias prácticamente inocuas, hoy en día suponen el origen de pérdidas económicas importantísimas a nivel mundial.

Si bien no hay estadísticas fiables al respecto, la consultora americana especializada Computer Economics cifra las pérdidas derivadas del malware (virus, troyanos, gusanos, etc.) en cerca de 92.000 millones de euros en los últimos 10 años, con base en los costes derivados de la pérdida directa de información, las paradas de sistemas y de las cantidades invertidas en la limpieza de los sistemas informáticos.

Los virus modifican el sistema operativo o los programas, que se infectan a medida que se ejecutan en el sistema, camuflándose de diferentes maneras.

A diferencia de éstos, los **gusanos** se replican a sí mismos en una espiral de crecimiento infinito que amplía los procesos ejecutados en la memoria de los sistemas. Una característica específica de éstos es que el sistema se va ralentizando poco a poco hasta ser casi imposible su adecuado manejo.

Los **troyanos** no se comportan como un virus, sino que al igual que el caballo de Troya de la mitología griega, abre puertas para que los hackers puedan controlar nuestro equipo informático sin nuestro consentimiento, con dos fines básicos: conocer todo lo que hacemos para robarnos nuestras credenciales e identidad, y/o operar directamente desde él para realizar operaciones fraudulentas sin nuestro conocimiento.

La infección de troyanos suele venir acompañada de la instalación de programas aparentemente inocuos que se descargan gratuitamente desde Internet, o mediante acciones asociadas a un correo electrónico y página Web en la que el usuario lo activa sin querer al hacer clic en un determinado enlace o botón.

Spyware

El spyware es un pequeño programa que se introduce en el ordenador normalmente por un virus o un troyano y que se dedica a recopilar la información que el usuario contenga en su equipo y la procedente de su experiencia de navegación por Internet, intentando capturar identificaciones de usuarios y contraseñas, así como otros datos, ya explicados en el apartado robo de identidad. El troyano envía estos datos a través de Internet al ordenador del pirata informático, que recibirá todos los datos sin necesidad de moverse de su sitio.

El sistema de spyware también es utilizado en ocasiones para la vigilancia de los empleados en las grandes corporaciones con el fin de comprobar si sus actividades con el ordenador de la empresa se adecúan a las normas establecidas en la correspondiente corporación.

Hackers y crackers

Los hackers y los crackers son los individuos que están detrás de los procesos de vulneración de la seguridad que estamos describiendo.

Los **hackers** se dedican a la búsqueda de agujeros de seguridad con el fin de explotarlos para acceder a sistemas aparentemente securizados. A diferencia de los **Crackers**, que vulneran los sistemas para realizar acciones delictivas, los Hackers, al menos en su origen, buscan más bien el prestigio personal de ser capaces de encontrar la manera de entrar en sistemas altamente protegidos.

Phishing y estafas on line

La variedad de métodos para realizar fraudes en línea, es tan amplia que sería imposible describirla brevemente.

El **phishing** está íntimamente relacionado con la ingeniería social. Lo que se busca es que sea el propio usuario el que proporcione sus datos de acceso y contraseña a determinados servicios, normalmente de tipo bancario, con el fin de proceder posteriormente a suplantar su identidad para hacer operaciones bancarias no autorizadas con sus cuentas.

Suele comenzar con un correo electrónico en el que argumentando problemas de seguridad u

operaciones de mantenimiento del banco se nos solicita que volvamos a confirmar nuestros datos de acceso y contraseña en una página que suplanta la identidad de nuestra entidad bancaria, con lo que el robo de credenciales queda efectuado.

Spam

El Spam, también llamado correo basura, es como su nombre indica, correo no deseado que recibimos en nuestro buzón.

La finalidad es doble: Por un lado, tiene un objeto meramente publicitario. Es como el buzoneo del mundo real, en el que nos depositan cantidades ingentes de papel de propaganda en nuestro buzón, pero en el mundo virtual. Normalmente va asociado a la información que sobre nuestra experiencia de navegación se ha obtenido por alguno de los medios descritos anteriormente, de manera que la publicidad que recibamos sea inicialmente de nuestro interés, aunque no siempre es así. Actualmente está muy extendido el Spam referido a la venta de medicamentos, viagra sobre todo.

Por otro lado, los correos de Spam suelen ser fuente de entrada de virus, troyanos, e intentos de phishing, por lo que hay que tener especial cuidado con ellos.

Sistemas de protección

Ya hemos descrito el contexto y los posibles riesgos a la hora de enfrentarnos al problema de la seguridad informática y a la navegación por Internet.

Identificados los problemas potenciales vamos a ahora a centrarnos en intentar ver las posibles soluciones a los problemas planteados, que aun siendo seguramente por casi todos conocidas, no terminan de aplicarse plenamente ni siquiera en los entornos empresariales más rigurosos, cuanto menos en el ámbito de la escuela y del hogar.

Sistemas de protección local

Desde el punto de vista de la protección de nuestro dispositivo, en su perspectiva local, hay tres aspectos básicos a tener en cuenta, fáciles de implementar y que mejorarán sustancialmente nuestra experiencia de seguridad:

1.- Mantener actualizado el sistema operativo y el software instalado.

Es fundamental, para evitar posibles agujeros de seguridad en los sistemas derivados de las vulnerabilidades explicadas anteriormente, que mantengamos permanentemente actualizado nuestro sistema y el software instalado. Para ello, en la actualidad, los sistemas de actualización automática de los sistemas operativos nos facilitan enormemente la labor, al detectar de manera autónoma la configuración de nuestros sistemas y la necesidad de actualización, al igual que ocurre con la mayoría de los programas instalados.

2.- Cambiar periódicamente la contraseña de acceso al sistema.

Sea por el método que sea, si un usuario consigue las claves de acceso a un sistema, tendrá vía libre para operar con él sin nuestro consentimiento.

Para minimizar los riesgos derivados se debe cambiar con frecuencia la clave de acceso al sistema, utilizando para su configuración **al menos una longitud de 8 caracteres alfanuméricos** en los que combinar mayúsculas y minúsculas, letras, números y símbolos del tipo %, & o $.

Evidentemente hay que evitar palabras con significado común y relacionado con nuestro entorno próximo y no dejarlas al alcance de cualquiera en las proximidades del ordenador.

Como hoy en día es habitual tener múltiples usuarios y contraseñas para acceso no sólo al equipo local sino a múltiples sitios Web, existen programas que nos ayudan a recordárnoslas y las almacenan encriptadas. Uno de los mejores es Norton Password Manager, aunque existen multitud de sistemas que hacen lo mismo.

En la actualidad, las tarjetas criptográficas, y sobre todo la extensión del uso del DNI electrónico, permiten el almacenamiento de los certificados digitales necesarios para la identificación en la mayoría de los sitios de Internet (banca electrónica, servicios de la administración, etc.), aumentando con ello los niveles de seguridad y de privacidad que se pueden aplicar a los equipos informáticos y a la navegación por Internet.

3.- Instalar y mantener actualizado un programa antivirus.

Los programas antivirus monitorizan de manera permanente el sistema en busca de software malicioso en ejecución o en estado latente, con el fin de identificarlo, dar la alarma y si fuera posible desinfectar el equipo o al menos aislar el virus.

Existen múltiples sistemas antivirus de diferentes empresas y algunas soluciones gratuitas aunque es

difícil establecer cuál de todas ellas es la mejor puesto que las comparativas realizadas por revistas especializadas usan unos parámetros muy diversos de evaluación y no exentos de influencias de las compañías explotadoras de las soluciones.

El Ministerio de Industria, Turismo y Comercio de España cuenta con un organismo autónomo dedicado a la seguridad informática denominado INTECO (Instituto Nacional de Tecnologías de la Comunicación) accesible a través de la dirección www.inteco.es que ofrece ayuda y consejos sobre soluciones de seguridad y antivirus de manera gratuita.

La importancia de las actualizaciones de seguridad

Las actualizaciones son añadidos o modificaciones realizadas sobre los sistemas operativos o aplicaciones que tenemos instalados en nuestros dispositivos y cuya misión es mejorar tanto aspectos de funcionalidad como de seguridad.

Si no mantenemos nuestros equipos al día nos exponemos a todo tipo de riesgos: robo de información, pérdida de privacidad, perjuicio económico, suplantación de identidad, etc.

Por tanto si queremos disfrutar de las ventajas de la tecnología debemos:

- Vigilar el estado de actualización de todos nuestros dispositivos y aplicaciones.
- Elegir la opción de **actualizaciones automáticas** siempre que esté disponible.
- Instalar las actualizaciones tan pronto como se publiquen, especialmente las de los sistemas operativos, navegadores y programas antivirus.
- Ser cuidadosos con las aplicaciones que instalamos, huyendo de fuentes no confiables y vigilando los privilegios que les concedemos.
- *Evitar hacer uso de aplicaciones y sistemas operativos antiguos que ya no dispongan de actualizaciones de seguridad.*

Vídeo "Sigue sin actualizar...": https://youtu.be/aGggJPdW6MQ

Vídeo actualizar Windows: https://www.youtube.com/watch?v=sEGY5FgJqJo

***Vídeo** actualizar los navegadores:*

https://youtu.be/RqlZAx-9cHk?list=PLt0qyS-HSB2T53KELUGfcNWAJt44A4ITh

¿Por qué son tan importantes las actualizaciones?

Cualquier programa es susceptible de tener fallos de seguridad. Por este motivo, puede necesitar ser actualizado independientemente del dispositivo en el que se encuentre instalado. **Esto incluye los programas y sistemas operativos** de ordenadores, tabletas, smartphones, consolas de videojuegos e incluso televisiones inteligentes.

Las actualizaciones de software no son un fastidio. Al contrario, son esenciales para mantener la seguridad de nuestros dispositivos.

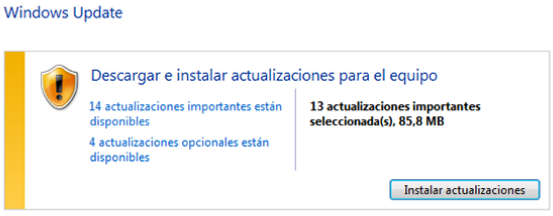
Debemos ser conscientes de que en nuestros dispositivos también hay instalados navegadores, programas, *plugins,* etc. que por supuesto, también necesitan ser actualizados para mantenerlos al día y bien protegidos.

Un caso especial, son las actualizaciones de las herramientas antivirus ya que sólo serán eficaces si están a la última. De nada sirve tener instalado un antivirus si no es capaz de detectar las últimas amenazas que circulan por la red.

Importante, no debemos confundir tener una aplicación actualizada con tener la última versión. Podemos tener instalado y actualizado Microsoft Office 2007 a pesar de no tratarse de la última versión de este paquete de herramientas ofimáticas. Los fabricantes no sólo comercializan nuevas versiones que incorporan mejoras, sino que mantienen un largo periodo de tiempo las antiguas versiones a través de actualizaciones.

¿Quién se encarga de publicarlas?

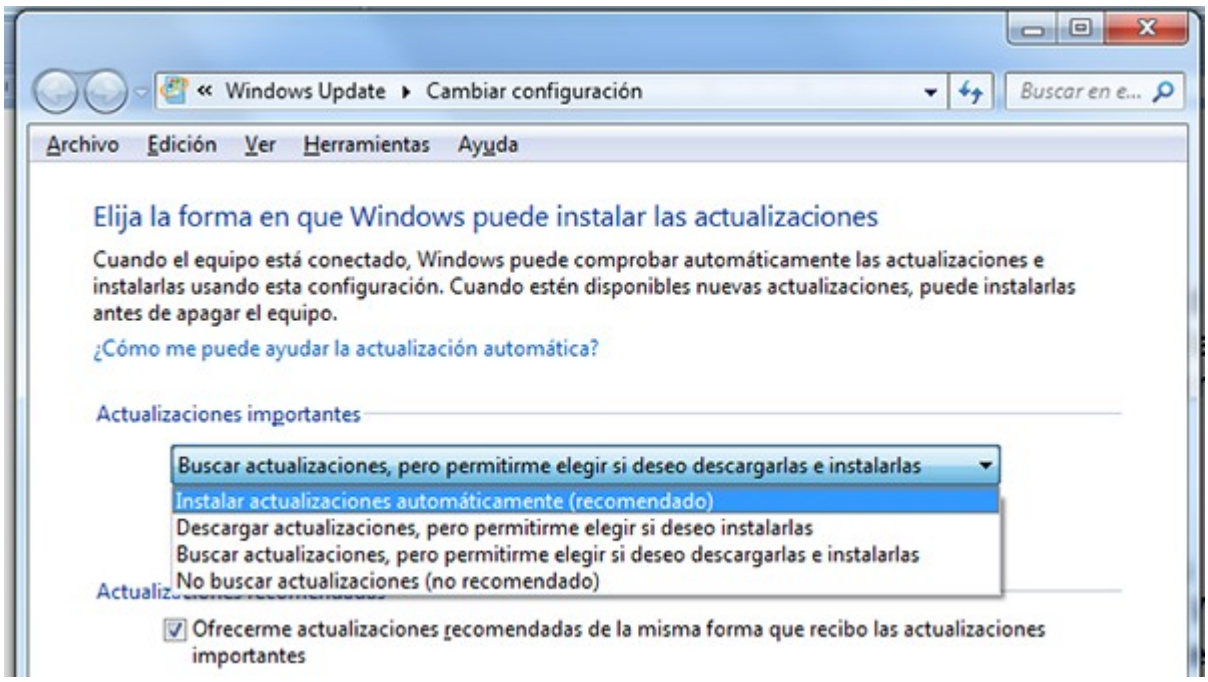
Las actualizaciones son elaboradas y ofrecidas por los propios desarrolladores y fabricantes. En algunos casos publican los parches (así se llaman también las actualizaciones de seguridad) con gran rapidez. En otras ocasiones, los fabricantes tienen que adaptar los parches a sus dispositivos y el proceso no es tan rápido. En este caso último caso poco podemos hacer más allá de ser conscientes del riesgo y no realizar acciones que nos puedan comprometer hasta que la actualización esté disponible.



Qué debemos hacer ante una nueva actualización

Hemos de ser conscientes del riesgo que supone utilizar un equipo no actualizado. Una vez que se hace público un fallo de seguridad, cualquiera con los conocimientos adecuados puede utilizarlo para causarnos un perjuicio. Por tanto, todos hemos de adoptar el hábito de mantener nuestros dispositivos al día.

En muchos casos, las aplicaciones y dispositivos disponen de opciones de **actualización automática**, de manera que las instalan, de forma transparente para nosotros, tan pronto el fabricante o desarrollador las publican. Esta es la opción más recomendada ya que evita que tengamos que estar nosotros pendientes de esta tarea, que en ocasiones resulta un poco molesta.



Para facilitarnos el trabajo, existen herramientas que nos ayudan a saber si nuestros equipos están a la última. Un ejemplo es PSI (Personal Software Inspector), que recopila el software que está instalado en el sistema y alerta de las aplicaciones que no están actualizadas. De esta manera cubrimos aquellas aplicaciones que no poseen un sistema de actualizaciones automático.

Algunas precauciones

Los delincuentes han descubierto que la instalación de parches constituye un nuevo modo de infectar un dispositivo. Por ello ciertos sitios de Internet y ciertas aplicaciones nos ofrecen la instalación de **actualizaciones falsas**. Al aceptarlas, nuestro equipo quedaría infectado. Por tanto, no debemos instalar nada que no provenga de los canales oficiales que proporcionan los fabricantes

y desarrolladores de los dispositivos o el software.

Debemos huir de sitios "pirata", especialmente de aquellos que ofrecen aplicaciones o servicios gratuitos o extremadamente baratos.

Otra situación que debemos tener en cuenta es la instalación o actualización de una aplicación que necesita ciertos privilegios para funcionar correctamente. Es recomendable revisarlos, para evitar que individuos maliciosos que buscan tomar control de nuestro dispositivo puedan usarlos. En cualquier caso, instalemos aplicaciones sólo de fuentes de confianza y siempre revisemos los privilegios por si fuesen excesivos o innecesarios para el propósito a que están destinadas.

Cómo actualizar plugins del navegador

Todos los complementos del navegador deberían estar actualizados, pero hay tres, que son de vital importancia que estén actualizados SIEMPRE. Hablamos de **Adobe Reader, Adobe Flash Player y Java.**

Adobe Reader

Adobe Reader es un programa creado por Adobe que permite visualizar documentos en formato PDF.

Para saber qué versión de Adobe Reader tienes instalada en el equipo, selecciona la opción "**Acerca de Adobe Reader…**" del menú **Ayuda**.

Para actualizar la versión de Adobe Reader en tu ordenador, te recomendamos que desinstales la versión antigua, haciendo uso del "Panel de Control" de Windows, e instales la nueva versión del programa. Puedes descargar Adobe Reader de forma gratuita desde la página web de Adobe.

Más información sobre cómo actualizar Adobe Reader en tu navegador:

- Internet Explorer
- Firefox
- Chrome

Además, te recomendamos que **actives las actualizaciones automáticas** durante el proceso de instalación de programa. De esta forma, siempre que se publique actualizaciones de Adobe Reader, se instalarán en tu ordenador.

Adobe Flash Player

Flash Player es un programa creado por Adobe que permite visualizar contenido y aplicaciones interactivas en la Web.

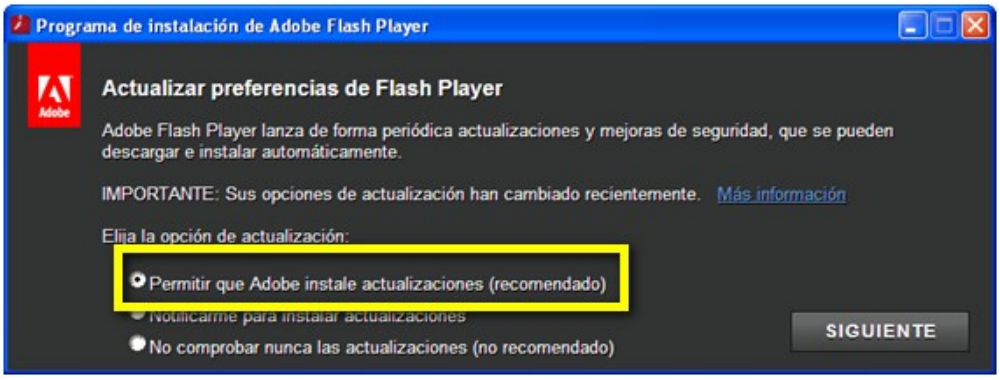
Para saber qué versión de Adobe Flash Player tienes instalada en el equipo, accede a la página Acerca de Flash Player o pulsa el botón derecho del ratón en un contenido de Flash, y selecciona la opción de «Acerca de Adobe Flash Player».

Para actualizar la versión de Adobe Flash Player, te recomendamos que desinstales la versión antigua, haciendo uso del "Panel de Control" de Windows, e instales la nueva versión del programa. Puedes descargar Adobe Flash Player desde la página web de Adobe con el navegador web que desea actualizar.

Más información sobre cómo actualizar Adobe Flash Player en tu navegador:

- Internet Explorer
- Firefox
- Chrome

Te recomendamos que **actives las actualizaciones automáticas** durante el proceso de instalación de programa. De esta forma, siempre que se publique actualizaciones de Adobe Flash Player, se instalarán en tu ordenador.

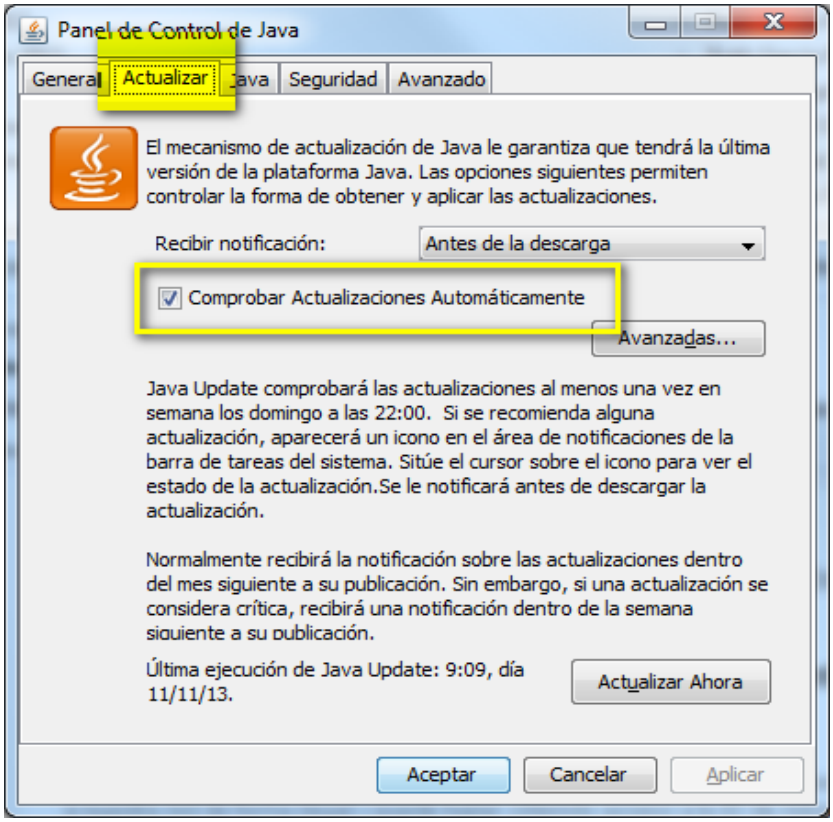


Java

Java es un lenguaje de programación con el que están creados muchos de los programas y aplicaciones del ordenador, páginas web, etc. Por tanto, para poder hacer un uso correcto de las funcionalidades que éstos nos ofrecen (jugar online, chatear, ver imágenes en tres dimensiones, etc.), es necesario tenerlo instalado en el equipo.

Para saber qué versión de Java tienes instalada en el equipo, accede a la página verificar la versión de Java y sigue los pasos que te indiquen si fuera necesario actualizarlo. También puedes descargar la última versión de Java desde su página web.

Te recomendamos que **actives las actualizaciones automáticas** durante el proceso de instalación del programa. De esta forma, siempre que se publique actualizaciones de Java, se instalarán en tu ordenador. También puedes configurar las actualizaciones automáticas desde el Panel de Control de Java.



Más información sobre cómo actualizar Java en tu navegador:

- Internet Explorer
- Firefox
- ***Chrome***

Las cuentas de usuario

Una cuenta de usuario es una colección de información que indica al sistema operativo los archivos y carpetas a los que puede tener acceso un determinado usuario del equipo, los cambios que puede realizar en él y sus preferencias personales, como el fondo de escritorio o el protector de pantalla.

Para usar el ordenador de una manera organizada y segura se recomienda crear una cuenta por cada usuario que vaya a utilizar el ordenador. De esta forma, cada usuario podrá tener su propio escritorio, con una configuración y preferencias

personalizadas.

- El usuario administrador debe relegarse a los casos en los que sea necesario.
- Para el resto de usos del equipo, hay que utilizar usuarios estándar.

Tipos de cuentas de usuario

Para poder gestionar las cuentas de usuario de un ordenador, crearlas, eliminarlas o cambiar sus características es necesario que exista un usuario especial con permisos para administrarlas.

Este es el **usuario administrador**. Sólo los usuarios de este tipo pueden instalar aplicaciones en el ordenador o modificar aspectos importantes de la configuración, como la conexión a Internet.

Todo equipo debe tener una cuenta de usuario administrador, para configurarlo y administrar el resto de cuentas de usuario que serán las de los usuarios normales, los **usuarios estándar**, para el uso cotidiano del ordenador.

Existe un tercer tipo de cuenta: el **usuario invitado** que sirve para que usuarios sin una cuenta personal, pueda iniciar una sesión y utilizar el equipo puntualmente.

El uso de distintas cuentas de usuario en un ordenador tiene las siguientes ventajas:

- AUMENTA LA PRIVACIDAD

  Permiten separar la información que almacena cada usuario en su cuenta. Muy útil, si te interesa que nadie acceda a tu documentación almacenada porque contiene datos bancarios, fotos y documentación privada.

- MEJORA LA SEGURIDAD

  Es posible limitar el daño, que pueda ocasionar un virus en el ordenador, en caso de que uno de los usuarios infecte el ordenador, al descargar un fichero adjunto del correo electrónico que contenía algún virus, al introducir un USB que estaba infectado o al visitar alguna página web maliciosa.

- PERMITE LA PERSONALIZACIÓN

  Se puede configurar a tu gusto el escritorio del ordenador -colores, tamaño de los iconos, tamaño texto, fondo de pantalla, etc.- tener tus páginas web favoritas en el navegador, etc.

Vídeo "Crear cuenta de usuario en Windows 10": *https://youtu.be/g89W7C09iBQ*

Para obtener más información sobre las cuentas de usuarios en Windows, consultar:

- Preguntas frecuentes sobre cuentas de usuario en Windows 7
- Preguntas frecuentes sobre cuentas de usuario en Windows 8
- Preguntas frecuentes sobre cuentas de usuario en Windows 10

También puedes consultar *información detallada de la gestión de cuentas de usuario en entornos Mac OS X* y en *Xubuntu*.

Las cuentas de usuario y la seguridad

El uso de la cuenta de administrador debe limitarse a aquellas situaciones en las que necesitamos disponer de privilegios: realizar cambios en la configuración, instalar una nueva aplicación, dar de alta un nuevo usuario, etc. Al finalizar estas tareas, debemos seguir trabajando con una cuenta estándar.

Cualquier cosa que hagamos con la cuenta de administrador afecta a todo el ordenador, y por tanto al resto de cuentas de usuario. Si cometemos un error o un descuido como administradores, esto afecta a todos los usuarios.

Además, si un virus infecta el ordenador cuando estamos utilizando una cuenta de administrador, podrá tener control total sobre el equipo, resultando más difícil de eliminar. Sin embargo, si la infección se produce utilizando una cuenta de usuario estándar, la limitación en los permisos reducirá mucho los efectos nocivos del virus.

Es muy importante **habilitar el uso de contraseñas** para poder abrir una sesión en el equipo desde el punto de vista de la seguridad. En el caso de las cuentas de usuario administrador esta práctica es necesaria dados los permisos de administración que estas cuentas tienen sobre las otras cuentas y sobre la configuración del equipo. Para el resto de cuentas de usuario también es necesario establecer una contraseña de acceso para proteger el espacio privado de cada usuario del equipo.

Debemos saber que la cuenta de usuario invitado tiene los mismos privilegios que un usuario estándar, pero es anónima y sin contraseña. Por defecto, viene deshabilitada, y desde el punto de vista de la seguridad es conveniente que se mantenga así.

Consejos para minimizar los riesgos en la navegación por Internet.

Consejos para la protección del equipo

1. Mantente informado sobre las novedades y alertas de seguridad.

2. Mantén actualizado tu equipo, tanto el Sistema Operativo como cualquier aplicación que tengas instalada.

3. Haz copias de seguridad con cierta frecuencia, para evitar la pérdida de datos importante.

4. Utiliza software legal que suele ofrecer garantía y soporte.

5. Utiliza contraseñas fuertes en todos los servicios, para dificultar la suplantación de tu usuario (evita nombres, fechas, datos conocidos o deducibles, etc.).

6. Utiliza herramientas de seguridad que te ayudan a proteger / reparar tu equipo frente a las amenazas de la Red.

7. Crea diferentes usuarios, cada uno de ellos con los permisos mínimos necesarios para poder realizar las acciones permitidas.

Consejos para una navegación segura.

1. Para evitar virus, descarga los ficheros solo de fuentes confiables.

2. Descarga los programas desde las páginas oficiales para evitar suplantaciones.

3. Analiza con un antivirus todo lo que descargues antes de ejecutarlo.

4. Mantén actualizado el navegador para protegerlo contra los últimos ataques.

5. Como apoyo para saber si una página es confiable utiliza analizadores de URLs.

6. Configura tu navegador para que sea seguro.

Ten precaución con las contraseñas que guardas en el navegador, y utiliza siempre una contraseña maestra.

Consejos para el uso seguro del correo electrónico.

1. Desconfía de los correos de remitentes desconocidos, ante la duda elimínalo.

2. No abras ficheros adjuntos sospechosos procedentes de desconocidos o que no hayas solicitado.

3. Utiliza el filtro anti-spam y marca los correos no deseados como correo basura.

4. Ten precaución con el mecanismo de recuperar contraseña, utiliza una pregunta que sólo tu sepas responder.

5. Analiza los adjuntos con un antivirus antes de ejecutarlos en tu sistema.

6. Desactiva la vista previa y la visualización en HTML de tu cliente de correo para evitar el posible código malicioso que pueda estar incluido en el cuerpo de los mensajes.

7. No facilites tu cuenta de correo a desconocidos ni la publiques *'alegremente'*.

8. No respondas a mensajes falsos, ni a cadenas de correos para evitar que tu dirección se difunda.

9. Cuando reenvíes mensajes a múltiples destinatarios utiliza la copia carbón oculta –CCO o BCC- para introducir las direcciones

Consejos para las transacciones económicas seguras por Internet

1. Observa que la dirección comienza por https que indica que se trata de una conexión segura porque la información viaja cifrada.

2. Asegúrate de la legitimidad de la página; con la barra de navegación en verde total confianza, con la barra en azul debemos conocer previamente que esa página coincide con la entidad solicitada.

3. Ten en cuenta que tu banco NUNCA se pondrá en contacto contigo para pedirte información confidencial.

4. Evita el uso de equipos públicos (cibercafés, estaciones o aeropuertos, etc.) para realizar transacciones comerciales.

5. Desactiva la opción 'autocompletar' del navegador si accedes desde un equipo distinto al habitual o compartes tu equipo con otras personas.

6. Cierra tu sesión cuando acabes, para evitar que alguien pueda suplantarte.

7. Configura tu navegador para que puedas realizar cualquier transacción económica de forma segura.

Consejos para la participación segura en redes sociales

1. Lee las políticas de uso y privacidad de los diferentes servicios antes de utilizarlos, sobre todo lo relacionado con la política de privacidad y la propiedad última de los que se publica en la red social.

2. Piensa antes de publicar, no sea que luego te arrepientas.

3. Valora que información deseas revelar y controla quién puede acceder a ella.

4. Controla tu lista de contactos, y antes de agregar a alguien tomate tu tiempo para asegurarte de su confianza.

5. Las redes sociales contienen las mismas aplicaciones que utilizan los atacantes para propagar los virus –correo, mensajería, navegación, etc.-, mantén las mismas recomendaciones.

6. Utiliza contraseñas seguras para que no te suplanten.

7. Si crees que estás siendo víctima de acoso contacta inmediatamente con el servicio de atención exponiéndole tu caso.

Consejos específicos para la experiencia segura de los menores en Internet

1. Educa al menor sobre los posibles peligros que puede encontrar en la red.

2. Acompaña al menor en la navegación cuando sea posible, sin invadir su intimidad.

3. Advierte al menor de los problemas de facilitar información personal (nombre, dirección, teléfono, contraseñas, fotografías, etc.) a través de cualquier canal.

4. Desaconséjale participar en charlas radicales (provocadoras, racistas, humillantes, extremistas, etc.) ya que pueden hacerle sentir incómodo.

5. Infórmale de que no todo lo que sale en Internet tiene que ser cierto, ya que pueden ser llevados a engaño con facilidad.

6. Indique claramente a su hijo que la comisión de delitos también se puede realizar a través de Internet y que el desconocimiento de la ley no exime de su cumplimiento. Acciones como la descarga ilegal de programas, películas, música, el acoso a compañeros, etc., están severamente penadas por la ley.

7. Presta atención a sus 'ciber-amistades' en la misma medida que lo haces con sus amistades en la vida real.

8. Pídele que te informe de cualquier conducta o contacto que le resulte incómodo o sospechoso.

9. Vigila el tiempo de conexión del menor a Internet para evitar que desatienda otras actividades.

10. Crea una cuenta de usuario limitado para el acceso del menor al sistema.

Consejos sobre el acceso a Internet en el hogar

1. Coloque el ordenador o dispositivo de acceso a Internet en un lugar común. Podrá

comprobar discretamente los lugares que visita su hijo/a.

2. Acompañe a su hijo/a en la experiencia de navegación por Internet, en la búsqueda de información y en el juego, procurando ser un partícipe más y no como elemento controlador. Cuanta más confianza tenga su hijo/o en Usted y más percepción de que se le respeta, más fácil le será contarle todo lo que hace.

3. Sobre todo, hable con su hijo/a. Una buena comunicación es el cauce perfecto para prevenir los riesgos y para ayudarle rápidamente en caso de apuro.