

PROTECCIÓN Y USO SEGURO DEL PC Y OTROS DISPOSITIVOS



Protección y uso seguro del PC y otros dispositivos.

2013.

Autores:

Rafael Muruaga Ugarte

Marcos Corrada Arjona

Nuria Martínez Fernández

Impresión.

Depósito Legal.

Diseño.

PRESENTACIÓN DEL MANUAL

EAP

PROLOGO

A lo largo de esta guía, se van a recoger cuales son los riesgos que presenta un equipo informático y otros dispositivos, atendiendo a todas las vulnerabilidades y brechas de seguridad que aparecen en un sistema y que se derivan de los distintos usos que se hacen de los mismos.

El ámbito de la informática es muy amplio y es difícil abordar todos los temas en una guía breve como ésta, por lo que se expondrán aquellos riesgos que se consideran más críticos para el uso de un equipo informático o un móvil para el usuario en el uso habitual tanto en el ámbito profesional como personal.

El curso inicia con un enfoque general de la evolución de la seguridad en los equipos informáticos a lo largo de los últimos tiempos, donde la principal evolución es que se ha cambiado la idea de protección únicamente sobre los sistemas para hacerla extensible también a la seguridad sobre la información. Dentro de la introducción se va a definir un concepto que se va a utilizar frecuentemente en la guía que es la definición de vulnerabilidad.

A lo largo del documento se va a facilitar al usuario cuestiones prácticas de seguridad sobre los sistemas para que las pueda aplicar en la securización de los equipos que se utilizan de forma habitual.

Primero se introducen unas recomendaciones de seguridad básicas que se deben adoptar de manera obligatoria sobre los equipos informáticos para asegurar un uso seguro de los mismos que incluye las actualizaciones, la creación de distintas cuentas de usuarios y la utilización de un antivirus correctamente actualizado. Una vez que se recogen los principios que se deben aplicar para obtener una seguridad general en el equipo, se introducen recomendaciones de seguridad para otras utilidades que presentan los equipos informáticos y otros dispositivos, que los usuarios pueden utilizar o no en función de las necesidades y uso de las mismas. Algunos ejemplos que se recogen son la seguridad de las redes WiFi, seguridad de los navegadores, recomendaciones para obtener contraseñas seguras, securización de pendrives, securización de móviles, etc.

Por último una vez que se abordan todos los puntos para obtener sistemas seguros y adoptar un uso responsable de los mismos, se van a facilitar herramientas en las que no es necesario pagar licencias de uso que van a ayudar a cubrir algunas de las necesidades de seguridad que se plantean en el manual.

En todos los módulos de la guía se van a introducir recomendaciones de seguridad para que los usuarios puedan aplicar en el uso diario de herramientas informáticas y además se facilitan algunas herramientas que se pueden utilizar para aplicarlas en la consecución de los objetivos de seguridad que se plantean. Se trata por lo tanto de un curso de presentación de aplicaciones prácticas para el usuario por lo que se va a buscar que los usuarios tengan una alta participación en el mismo.

Protección y uso seguro del PC y otros dispositivos

Protección y uso seguro del PC y otros dispositivos.

Unidad 1: Introducción.

Evolución de la seguridad.

Definición Vulnerabilidad.

Unidad 2: Protección.

Elementos básicos para no quedar infectado.

Actualización de software

Cuentas de usuario

Antivirus

Para obtener una seguridad completa

Redes WiFi

Mantener el navegador seguro

Contraseñas seguras

Cortafuegos

Portátiles

Pendrive o Memoria USB

Móviles

Antes de que sea demasiado tarde...

Unidad 3: Recursos y utilidades

KeePass Password Safe

USB Safeguard

Restauración del sistema en Windows XP

Copia de seguridad del equipo y restaurar el sistema en Windows XP

Introducción del Módulo y Objetivos ó Expectativas de aprendizaje.

En el módulo de Protección y uso seguro del PC y otros dispositivos, se van a abordar unas recomendaciones para minimizar los riesgos de seguridad para el uso de PC y otros dispositivos. Para evitar problemas de seguridad que pudieran ocasionar una mala configuración, o un mal uso por desconocimiento por parte del usuario.

Un vez que se haya finalizado el módulo, el usuario debería tener una visión global de los riesgos y vulnerabilidades relacionados con el uso de PC y los dispositivos móviles a través de los que se puede conectar a Internet (móviles, *tablets*, etc). Así como conocer unas buenas prácticas que se recomienda sean observadas para el uso seguro de los mismos. Además conocerá algunas aplicaciones que le ayudaran a lograr ese objetivo.

Contenido

1. Introducción.	10
1.1. Evolución de la seguridad.....	10
1.2. Definición de “Vulnerabilidad”	11
2. Protección.	13
2.1. Elementos básicos para no quedar infectado.	13
2.1.1. Actualización de software	13
2.1.2. Cuentas de usuario.....	16
2.1.3. Antivirus	17
2.2. Para obtener una seguridad general.....	19
2.2.1. Redes WiFi.....	19
2.2.2. Mantener el navegador seguro.....	21
2.2.3. Contraseñas seguras	28
2.2.4. Cortafuegos.....	33
2.2.5. Portátiles	34
2.2.6. Pendrive o Memoria USB	36
2.2.7. Móviles.....	37
2.2.8. Antes de que sea demasiado tarde.....	39
3. Recursos y utilidades.....	42
3.1. KeePass Password Safe	44
3.2. USB Safeguard	54
3.3. Restauración del sistema en Windows XP	57
3.4. Copia de seguridad del equipo y restaurar el sistema en Windows XP	60
Bibliografía.	67

1. Introducción.

Hoy día, se puede afirmar sin temor a equivocarse, que las organizaciones y las empresas, pueden aprovechar las tecnologías de la información en su beneficio, pero también se debe ser consciente de los riesgos y amenazas asociados al uso de estas tecnologías y conocer la forma en que las empresas y las organizaciones pueden enfrentarse a ellas.

Alcanzar un adecuado nivel de seguridad es una tarea que pasa por desarrollar acciones en los distintos ámbitos de la materia, como son el técnico, el jurídico o normativo y el organizativo. Pero además, las organizaciones y las empresas, las componen personas y estas son uno de los eslabones más importantes de la cadena de la seguridad y también uno de los más débiles. Es por ello que, implantar seguridad en las organizaciones, pasa necesariamente por la formación e información a todas las personas que forman parte de la organización, independientemente del tamaño de esta y del perfil al que pertenezca.

1.1. Evolución de la seguridad

La seguridad como concepto ha evolucionado a lo largo del tiempo, comenzando con el enfoque de seguridad informática, cuyo alcance estaba limitado a la protección de los sistemas e infraestructuras, otorgándoles un gran protagonismo, por encima de otros activos, como la información.

La seguridad informática, carecía de metodologías y criterios para el diseño, selección y aplicación de medidas de seguridad. En este enfoque, se consideraba que, a través de herramientas y medios técnicos era posible detener o minimizar cualquier amenaza, alcanzando un nivel de seguridad, que en muchas ocasiones, estaba por encima de las necesidades reales de la organización o cuyas medidas eran implantadas sin un criterio claro o adecuado.

Con la proliferación de las redes de comunicaciones, el abaratamiento del acceso a Internet y la aparición de los dispositivos portátiles, la naturaleza y ámbito de los sistemas a proteger cambió, lo que trajo consigo una evolución del concepto de seguridad, que fue sustituido por la seguridad de las tecnologías de la información y las comunicaciones o seguridad TIC.

Este nuevo enfoque supuso una mejora sustancial respecto al anterior, puesto que no solo incorporaba nuevos sistemas e infraestructuras, como aquellas destinadas a las comunicaciones, sino que además, otorgaba más importancia a la información como activo, por encima de otros. Así mismo, comenzaron a desarrollarse metodologías para el diseño, selección e implantación de medidas de seguridad y la seguridad cada vez tenía más importancia dentro de las organizaciones.

Poco a poco la seguridad comenzó a salir de los departamentos técnicos y de sistemas, para convertirse en un elemento integrado en cualquier actividad o proceso de negocio. Por otro lado, la aparición de normativa y legislación relativa a las tecnologías de la información, impulsó el desarrollo del concepto de seguridad jurídica, así como la seguridad desde un punto de vista organizativo.

Finalmente, todo ello se integró en un concepto nuevo, mucho más amplio y cuya característica principal es considerar la información como el activo de mayor importancia y en torno al cual se desarrolla toda una metodología con un único objetivo, proteger la información.

A continuación se puede ver un sencillo diagrama que muestra la evolución que ha seguido, de forma muy simplificada, el concepto de seguridad.



Tal y como se ha indicado, la seguridad de la información desarrolla el concepto de seguridad en torno al activo más importante de cualquier organización: la información. A través de una metodología relativamente sencilla pero muy completa, se diseñan y seleccionan las medidas de protección adecuadas, de acuerdo con criterios de importancia de los activos a proteger, nivel de amenaza y riesgo al que están expuestos.

A través de esta metodología se busca alcanzar un nivel de seguridad adecuado y suficiente para la organización, de forma progresiva, a través de fases o ciclos, en cada una de las cuales va mejorando el nivel de seguridad hasta alcanzar el nivel deseado.

Una vez alcanzado dicho nivel, es necesario mantenerlo, ya que las organizaciones cambian y evolucionan en el tiempo, junto con su entorno, lo que supone que, una organización que se considere “segura” en el momento actual, no tiene porque serlo dentro de un año.

Por todo ello, en la actualidad se habla de Sistemas de Gestión de la Seguridad de la Información (SGSI), de forma que la seguridad es entendida como un sistema de gestión y como parte de un proceso de mejora constante.

1.2. Definición de “Vulnerabilidad”

Una vulnerabilidad o fallo de seguridad, es todo aquello que provoca que los sistemas informáticos funcionen de manera diferente para lo que estaban pensados, afectando a la seguridad de los mismos, pudiendo llegar a provocar entre otras cosas la pérdida y robo de información sensible.

Para entenderlo mejor se utilizará una analogía con el mundo real. Es fácil imaginar qué ocurriría si se dejará abierta la puerta del domicilio o el coche, y es que se tendrían bastantes posibilidades de que al menos sustraieran las pertenencias. El descuidar este detalle no implica que se sea objeto de un hurto, pero sí que se encuentra predisposición a que se produzca. En este sentido la única manera de protegerse sería cerrando la puerta. En el mundo de las vulnerabilidades informáticas el funcionamiento es muy similar; existe un **agujero de seguridad** y mientras éste permanezca abierto se estará predispuesto a sufrir un ataque que utilice dicho agujero.



En un plano más formal el término vulnerabilidad, se puede definir como la posibilidad de que una amenaza se materialice sobre un activo. En este contexto se debe entender "activo" como un recurso del sistema de información o relacionado con éste, necesario para que la organización funcione correctamente y alcance los objetivos propuestos. Esto incluye tanto elementos físicos como abstractos: información, servicios, etc. Y una "**amenaza**" es definida como un evento que puede desencadenar un incidente en la organización, produciendo daños materiales o pérdidas inmateriales en sus activos. Por ejemplo la pérdida de información, deterioro de hardware, indisponibilidad de un servicio, etc.

Aunque esta modulo se centra en los fallos de seguridad basados en software, asumiendo que son los más empleados para realizar intrusiones e infectar sistemas, también existen otro tipo de vulnerabilidades que se centran en el ámbito físico. En este sentido se puede pensar que se está completamente protegido desde el punto de vista de ataques informáticos, virus, etc. Pero puede que no sirva de nada todo ese esfuerzo si por el contrario no se ha previsto cómo hacer frente ante un posible incendio o se permite el acceso no autorizado a la sala de servidores (CPD).

2. Protección.

Unos buenos hábitos al utilizar los servicios que brinda Internet –navegación, correo, redes sociales, etc.- son fundamentales para no exponerse a riesgos innecesarios. Pero no todas las amenazas se pueden evitar si no se protege correctamente el sistema, se puede ser víctima de virus y usuarios maliciosos simplemente al conectarse o navegar por Internet.

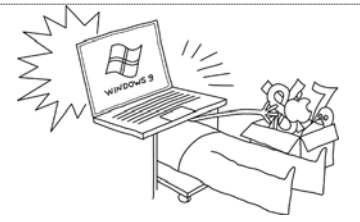
Por lo tanto, aparte de aplicar las buenas prácticas del modulo anterior, se deberán tener en cuenta, para mejorar la seguridad de los sistemas, las siguientes indicaciones para configurar los equipos y evitar que sean vulnerables.

2.1. Elementos básicos para no quedar infectado.

Los principales elementos que se deben tener en cuenta para tener un sistema robusto con el que sentirse seguro en la red serán descritos en los siguientes apartados.

2.1.1. Actualización de software

La mejor forma de proteger los sistemas es que estén actualizados con los últimos parches o aplicaciones, ya que evitan que los virus puedan encontrar vulnerabilidades y por tanto minimizan el riesgos a que sean utilizadas para atacar y lograr infectar o dañar el equipo. Activar las actualizaciones automáticas del sistema es por tanto una protección antivirus. Que nos permitirá navegar por la red de una forma mucho más segura y haciendo el proceso de actualización de una manera rápida y sencilla.



Los virus -de forma análoga a como haría un ladrón al intentar entrar a robar a una casa- aprovechan cualquier resquicio en el sistema a través del cual infectarlo. Los fabricantes de software, conocedores de que los atacantes andan al acecho, corrigen los agujeros de seguridad y lanzan las respectivas actualizaciones para proteger a sus clientes. Por ello, es de vital importancia actualizar los sistemas -tanto el sistema operativo como el resto de aplicaciones- tan pronto como sea posible.

Cuanto más tiempo se tarde en actualizar, más probabilidades existirán de quedar infectado.

Actualizar regularmente el sistema y aplicaciones

Las actualizaciones de software vienen justificadas por diferentes motivos:

- Reparar los posibles agujeros de seguridad -vulnerabilidades- existentes.
- Proporcionar nuevas funcionalidades o mejoras en las anteriores.

El proceso de actualización consiste básicamente en descargar de la página web del fabricante del programa los ficheros necesarios (parches o nuevas versiones).

Actualizaciones automáticas

Aunque es posible actualizar los programas manualmente, lo más sencillo y seguro es hacerlo de manera automática. De forma que el propio sistema busque las actualizaciones, las descargue e instale sin la intervención del usuario.

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

Actualizaciones automáticas del sistema operativo

En función del fabricante:

Microsoft Windows

Microsoft publica las actualizaciones únicamente los segundos martes de cada mes, salvo incidentes críticos que requieran de una actualización más inminente.

Permite configurar las actualizaciones para su descarga de forma automática. Para ver como activar o desactivar:

- Windows XP: <http://windows.microsoft.com/es-es/windows-xp/help/setup/setup-automatic-updates>
- Windows Vista: <http://windows.microsoft.com/es-es/windows-vista/turn-automatic-updating-on-or-off>
- Windows 7: <http://windows.microsoft.com/es-es/windows7/turn-automatic-updating-on-or-off>

Apple

Permite configurar las actualizaciones para su descarga diaria (recomendada), semanal o mensual.

Para versiones anteriores a Mac OS X v10., que no disponen de actualizaciones automáticas, hay que forzar la descarga manualmente.

Ubuntu

Por defecto avisa de la disponibilidad de nuevas actualizaciones, para que el usuario inicie su descarga. Es posible configurarlo para que se actualicen de forma automática.

Actualizaciones automáticas del navegador

El navegador, al utilizarlo para visitar páginas web, es una de las aplicaciones más expuestas a posibles amenazas.

En función del fabricante:

Internet Explorer

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

Ante grandes actualizaciones, como el paso de Internet Explorer 7 a Internet Explorer 8, es necesario confirmar el proceso (recomendado).

Mozilla Firefox

Se actualiza de forma automática por defecto. Al ejecutarlo, busca actualizaciones, no sólo del navegador, sino de todos los accesorios (complementos o plugins) instalados. Lo descarga y pide permiso para reiniciarlo.

Google Chrome

Se actualiza de forma automática por defecto. Al ejecutarlo, busca actualizaciones, no sólo del navegador, sino de todos los accesorios (complementos o plugins) instalados.

Safari

Se actualiza de forma automática por defecto. Al ejecutarlo, busca las actualizaciones; si las encuentra muestra una ventana con información acerca de la actualización y de cómo instalarla.

Para forzar la actualización se haría del mismo modo que al actualizar el software del sistema operativo.

Actualizar el resto de aplicaciones

Aunque hay aplicaciones más expuestas a las amenazas, no se debe olvidar del resto.

Volviendo a la analogía del ladrón de casas. Para protegerse del robo se debe cerrar la puerta de entrada y ventanas que dan a la calle – sistema operativo y navegador - pero sin descuidar otros pequeños puntos de entrada, lo que serían el resto de aplicaciones.

Para comprobar el nivel de actualización del resto de programas se pueden utilizar la siguiente herramienta:

Secunia Online Software Inspector.

Secunia Online Software Inspector (OSI) es una aplicación que muestra qué programas del ordenador están desactualizados junto con enlaces a páginas web desde las que se pueden descargar las actualizaciones.



Este programa se ejecuta a través del navegador por lo que es muy fácil y cómodo de ejecutar, aunque necesita que se encuentre instalado Java en el ordenador.

- Acceso aplicación: http://secunia.com/vulnerability_scanning/online/?lang=es

2.1.2. Cuentas de usuario

Para reducir el riesgo de virus se debe utilizar una cuenta de usuario apropiada. La cuenta de administrador sólo se debe usar en momentos puntuales.

Si un virus infecta el sistema, obtendrá acceso al equipo a través de la cuenta de usuario que se esté utilizando en ese momento. Por lo que si el incidente se produce al utilizar con una cuenta de administrador, el virus tendrá control total sobre el equipo, con total libertad para realizar la actividad maliciosa para la que fue diseñado. Si por el contrario se trabaja con una cuenta limitada, los efectos nocivos del virus serán mucho menores.



Utilizar diferentes cuentas de usuario, dependiendo del uso que se vaya a hacer del ordenador, constituye una buena práctica de seguridad.

La función de las cuentas de usuario

Las cuentas de usuario de los sistemas operativos han sido creadas para favorecer la gestión de los datos de las personas que utilizan el equipo y las labores que pueden desarrollar en el mismo.

- Desde el punto de vista de uso del equipo, el tener una cuenta propia permite al usuario personalizar el sistema a sus gustos y preferencias; que pueden ir desde cambiar el fondo de escritorio a configurar diferentes aspectos del navegador.
- Desde el punto de vista de la seguridad, se tiene un mayor control sobre el sistema, ya que a cada usuario sólo se le permite realizar aquellas tareas que estén dentro de su cometido. Lo que facilita que un ordenador pueda ser utilizado por varios usuarios de manera más segura, o que un mismo usuario pueda tener diferentes cuentas en función de los usos que le vaya a dar, trabajo y ocio por ejemplo.

Las cuentas de usuario están asociadas a un nombre y una contraseña, que por motivos obvios de seguridad, sólo el dueño debe conocer.

Tipo de cuentas

Los sistemas operativos tienen definidos por defecto diferentes tipos de cuentas:

- **Cuenta de administrador.** Permite tener el control total del equipo, y por tanto realizar todo tipo de actividades; instalar un programa, agregar un nuevo componente de hardware, configurar la conexión a Internet, etc. Todo sistema debe tener una cuenta de administrador, que será la que utilicemos para habilitar el resto de cuentas de usuario.
- **Cuenta limitada.** Permite el correcto desarrollo de las actividades cotidianas -navegador, programas de ofimática, reproductores de audio y video, etc-, pero no permite acciones que puedan repercutir en le correcto funcionamiento del sistema.
Otra diferencia sustancial es que las acciones realizadas en estas cuentas no afectan al resto de cuentas, sin embargo, las que se realicen como administrador sí se propagan al resto.
- **Cuenta de invitado.** Similar a la limitada, con la diferencia de que no está protegida por contraseña. Está pensada para que usuarios que no tienen una cuenta propia en el equipo puedan utilizarla en un momento puntual, como ver el correo o navegar. En la medida de lo posible no se recomienda su uso.

Seguridad en las cuentas

Las cuentas de administrador no están pensadas para utilizarlas en el día a día, suponiendo un riesgo para la seguridad.

En el uso diario se recomienda utilizar, para cada uno de los usuarios del sistema, una cuenta con privilegios limitados con las que poder desempeñar las actividades cotidianas. Ya que al utilizar habitualmente la cuenta limitada, ya que solo es necesario recurrir a la de administrador en momentos puntuales, se evita que los virus puedan manipular el PC.

Los sistemas más modernos, como Windows 8/7/Vista, Mac y Ubuntu, ya ejecutan por defecto los programas de forma limitada para reducir el riesgo de infección por virus y otras amenazas. Y al detectar que se quiere realizar una operación potencialmente peligrosa, solicitan la contraseña de la cuenta de administrador para validarlo.

2.1.3. Antivirus

Se debe confiar en el antivirus como última defensa. Ya que es la herramienta que eliminará el virus, una vez que ya ha llegado a ingresar al sistema de alguna de las siguientes formas:

- **Exploutando una vulnerabilidad:** cualquier programa del ordenador puede tener una vulnerabilidad que puede ser aprovechada para introducir programas maliciosos en el ordenador. Es decir, todos los programas que haya instalados en el equipo, ya sean: Sistemas Operativos - Windows, Linux, MAC OS, etc-, navegadores Web -Internet Explorer, Firefox, Opera, Chrome, etc-, clientes de correo -Outlook, Thunderbird, etc- o cualquier otra aplicación -reproductores multimedia, programas de ofimática, compresores de ficheros, etc-, es posible que tengan alguna vulnerabilidad que sea aprovechada por un atacante para introducir programas maliciosos. Para prevenir quedarse infectado de esta forma, recomendamos tener siempre actualizado el software el equipo.
- **Ingeniería social:** apoyado en técnicas de ingeniería social para apremiar al usuario a que realice determinada acción. La ingeniería social se utiliza sobre todo en correos de phishing, pero puede ser utilizada de más formas, por ejemplo, informando de una falsa noticia de gran impacto, un ejemplo puede ser alertar del comienzo de una falsa guerra incluyendo un enlace en que se puede ver más detalles de la noticia; a donde realmente dirige el enlace es a una página Web con contenido malicioso. Tanto para los correos de phishing como para el resto de mensajes con contenido generado con ingeniería social, lo más importante es no hacer caso de correos recibidos de remitentes desconocidos y tener en cuenta que su banco nunca le va a pedir sus datos bancarios por correo.
- Por un **archivo malicioso:** esta es la forma que tienen gran cantidad de troyanos de llegar al equipo. El archivo malicioso puede llegar como adjunto de un mensaje, por redes P2P, como enlace a un fichero que se encuentre en Internet, a través de carpetas compartidas en las que el gusano haya dejado una copia de sí mismo. La mejor forma de prevenir la infección es analizar con un antivirus actualizado todos los archivos antes de ejecutarlos, a parte de no descargar archivos de fuentes que no sean fiables.
- **Dispositivos extraíbles:** muchos gusanos suelen dejar copias de sí mismos en dispositivos extraíbles para que automáticamente, cuando el dispositivo se conecte a un ordenador, ejecutarse e infectar el nuevo equipo. La mejor forma de evitar quedarse infectados de esta manera, es deshabilitar el autoarranque de los dispositivos que se conecten al ordenador.

En la actualidad, es prácticamente imposible navegar sin estar debidamente protegidos ante las amenazas

escondidas detrás de cada sitio que visitamos. Los engaños son muchos, y las probabilidades de ser víctimas de un ataque de virus o malwares también. Es por ello que una de las mejores tácticas para prevenir ser infectados es la utilización de un buen antivirus.

Un antivirus debe estar siempre actualizado para poder obtener una lista de virus que realizan ataques diarios. Por esta razón, la mayoría de los fabricantes de antivirus suministran actualizaciones gratuitas a través de Internet. La actualización de las listas de virus es extremadamente importante para la eficacia del software de seguridad.



¿Porqué instalar un antivirus?

Si un equipo no tiene un antivirus, no tiene la capacidad de remover los virus que puedan llegar a atacar al sistema y el equipo quedará vulnerable a ataques como:

- Emails infectados, con anexos ejecutables peligrosos cuando son ejecutados.
- Sitios webs en internet infectados que lo llevan a descargar un código malicioso en su computadora, denominado Worms.
- Documentos de oficina, como Word y Excel, con Macros que atacan al Sistema Operativo.
- Spyware introducido por los virus para espiar datos personales. Algunos antivirus también detectan Spyware.



Consecuencias de no remover un virus

Ser afectado por un virus informático puede traer consecuencias gravísimas, dependiendo de la información que guarda en el equipo, o en el equipo de la empresa.

Los efectos más comunes ante una infección pueden ser:

- **Perder datos importantes** que no fueron guardados en un backup.
- El **sistema** funciona **muy lento** o es imposible utilizar.
- **Fraudes y robo de datos personales**, que son enviados a otras computadoras. Uno de los ejemplos más frecuentes es el robo del número de la tarjeta de crédito.

- **Robo de identidad**, donde su computadora podría ser utilizada por hackers para ejecutar ataques a otras computadoras.

Como se ve, la utilización de un antivirus es fundamental hoy día para que se pueda navegar en internet, leer e-mails y abrir documentos de trabajo que se reciben, sin la preocupación de poder ser alcanzados por un ataque que destruya los datos. Con este software, se pueden remover los virus a medida que estos van apareciendo.



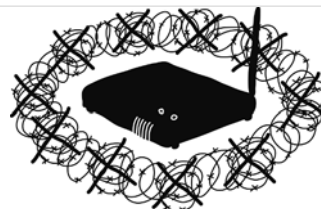
2.2. Para obtener una seguridad general

Se suele decir que la seguridad informática es como una cadena, y que ésta será tan fuerte como el más débil de sus eslabones. Por ello, tampoco se debe olvidar prestar atención a los siguientes elementos:

2.2.1. Redes WiFi

Una red WiFi sin protección puede ser usada por terceros para acceder a Internet, a información privada o para cometer algún fraude, con las implicaciones legales que eso puede conllevar.

La utilización de este tipo de conexión ofrece ventajas asociadas a la movilidad y, teniendo en cuenta los riesgos de seguridad que tienen este tipo de redes, se recomienda emplearlo sólo en las siguientes situaciones:



- Cuando se necesita conectar desde distintos sitios del domicilio y donde no siempre es sencillo llevar cables.
- Cuando se necesita conexión y movilidad al mismo tiempo.
- Cuando el número de equipos que se conectan a Internet en casa es variable.

Cómo proteger la red WiFi

Para asegurar la conexión se pueden implementar las siguientes medidas de fácil aplicación, simplemente con unos conocimientos básicos y la ayuda de los manuales del dispositivo.

Se puede disponer de redes WiFi con un nivel de seguridad aceptable si se utilizan correctamente los medios de protección disponibles

Modificar los datos por defecto de acceso al router

Los routers y puntos de acceso vienen de fábrica con contraseñas por defecto, públicamente conocidas. Se debe cambiar cuanto antes la contraseña por defecto del dispositivo, para evitar que los atacantes puedan tomar el control del router desde el exterior.

Ocultar el nombre de la red

Para evitar que un usuario con malas intenciones pueda visualizar nuestra red, es necesario configurarla para que no se difunda su nombre públicamente. De esta manera si alguien quiere conectarse a ella, solo podrá hacerlo si conoce el nombre de la red de antemano.

Para ocultar la red basta con limitar la difusión del nombre -también llamado SSID-.



Usar un protocolo de seguridad para proteger la red

Mediante protocolos de seguridad se permite el cifrado de la información en función de una contraseña. Los dos sistemas más comunes para asegurar el acceso a la red WiFi son mediante el protocolo WEP y el protocolo WPA.

El mas seguro de ambos es el protocolo WPA, por lo que se recomienda su uso. También es posible utilizar el protocolo WPA2 que es la evolución del WPA, pero no todos los dispositivos lo soportan –se deberá consultar la documentación del dispositivo para ver si acepta WPA2 -.

Independientemente del protocolo que se use, la forma de trabajo es similar. Si el punto de acceso o router tiene habilitado el cifrado, los dispositivos que traten de acceder a él tendrán que habilitarlo también. Cuando el punto de acceso detecte el intento de conexión, solicitará la contraseña que previamente habremos indicado para el cifrado.

Se debe utilizar SIEMPRE un protocolo de seguridad, y en lo posible el protocolo WPA o WPA2

The top screenshot shows a router configuration page for WPA security. The 'Security Mode' dropdown is set to 'WPA Pre-Shared Key'. The 'WPA Algorithms' dropdown is set to 'TKIP'. The 'WPA Shared Key' field contains the text 'WekjRLkskOSLKPeKlaOPKleOSlp'. The 'Group Key Renewal' is set to '3600 seconds'.

The bottom screenshot shows a router configuration page for WEP security. The 'Security Mode' dropdown is set to 'WEP'. The 'Default Transmit Key' is set to '1'. The 'WEP Encryption' dropdown is set to '128 bits 26 hex digits'. The 'Passphrase' field contains 'tekstenuitleg'. A 'Generate' button is visible. Below the passphrase, four keys are listed: Key 1: 2239D45EB87B0554A9E968AE2B, Key 2: 6FAD9B4513E9A9C78741FE54DB, Key 3: 2B21CA1A764DD621A6BF608440, and Key 4: 35A4F3734193E85D7589DFF65F.

Para lograr una mayor seguridad se deben cambiar las contraseñas de acceso cada cierto tiempo y usar contraseñas seguras.

Apagar el router o punto de acceso cuando no se vaya a utilizar

De esta forma se reducen las probabilidades de éxito de un ataque contra la red inalámbrica y por lo tanto de su uso fraudulento.

2.2.2. Mantener el navegador seguro

Cuando se sale de viaje se deben revisar los neumáticos, los niveles...cuando se navega por Internet el vehículo, el navegador, debe tener todos los elementos para hacerlo de forma segura.

En la actualidad el navegador se utiliza para acceder a la mayoría de servicios en Internet.

Al estar expuesto al exterior y manejar gran cantidad de información –entre la que destaca información sensible de servicios bancarios y comerciales- es fundamental utilizarlo y configurarlo de forma segura para evitar ser víctima de un fraude o virus.

Principales elementos y opciones de seguridad

Actualizar el navegador para que esté protegido, a la última

Es fundamental tener actualizado el navegador con la versión más reciente para estar protegido de los nuevos tipos de ataques.

Infórmese más en detalle sobre la importancia de las actualizaciones de software, y como funcionan las actualizaciones automáticas del navegador.

Limitar el uso de ciertas funcionalidades: Java y JavaScript

Los lenguajes Java y JavaScript son utilizados en las páginas para aportar dinamismo y nuevas funcionalidades. Por ejemplo, permiten jugar en línea, participar en sesiones de chat, o calcular los intereses de una hipoteca con un gráfico animado, entre otras muchas cosas.

Por otro lado ambas características pueden utilizarse maliciosamente para propagar virus e infectar el sistema.

Conviene que se aprenda a limitar el uso de estas funcionalidades en las páginas de dudosa confianza, y saber cómo activarlo –para aprovechar todo su potencial- en las que sí sean de confianza.

Bloquear las molestas ventanas emergentes

Se deben de bloquear las pantallas emergentes para evitar que salga publicidad no deseada mientras se navega por una página web.

Gestionar correctamente las contraseñas

Actualmente cada usuario dispone de muchos usuarios y contraseñas seguras que recordar. Para simplificar esta tarea los navegadores permiten gestionarlas, de modo que al visitar de nuevo una página no se tengan que volver a introducir.

Pero en ocasiones esta práctica puede poner en riesgo la seguridad. Por lo que se debe aprender a manejar esta característica del navegador –haciendo uso de la contraseña maestra y limitando el autocompletado- para que las contraseñas no caigan en manos de terceros.

Configurar las cookies para que no afecten a la privacidad

Las cookies, son pequeños fragmentos de información que se almacenan en el ordenador de la persona que visita una página web y que sirven para conservar cierta información entre visitas; preferencias de usuario y hábitos de navegación.

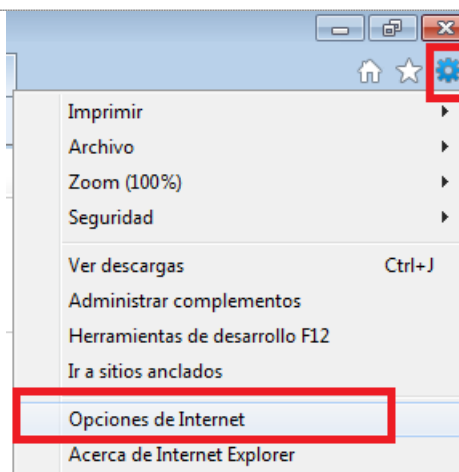
Un uso abusivo de las cookies por parte de terceros puede tener implicaciones importantes en la privacidad, por ello es importante saber como manejarlas.

A continuación se indica como configurar estas medidas en el navegador:

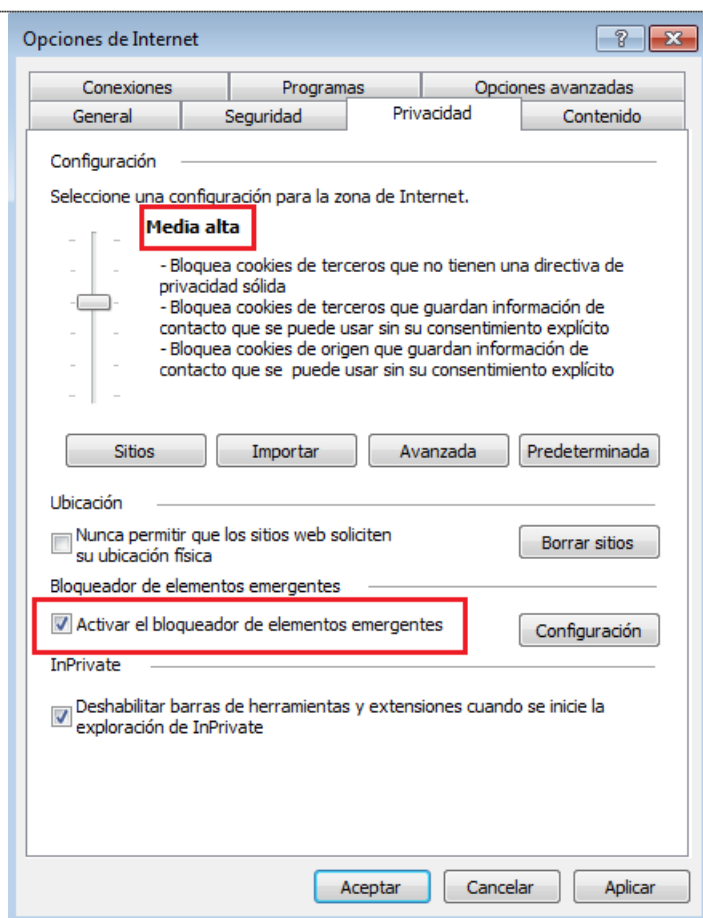
Internet Explorer

Las opciones que se van a explicar son para la versión 9 de Internet Explorer. Para hacer más segura la navegación con este programa siga estos pasos:

1. En el menú del navegador ir a la sección Herramientas (es el icono con forma de engranaje, en la parte superior derecha) y seleccionar «Opciones de Internet»:

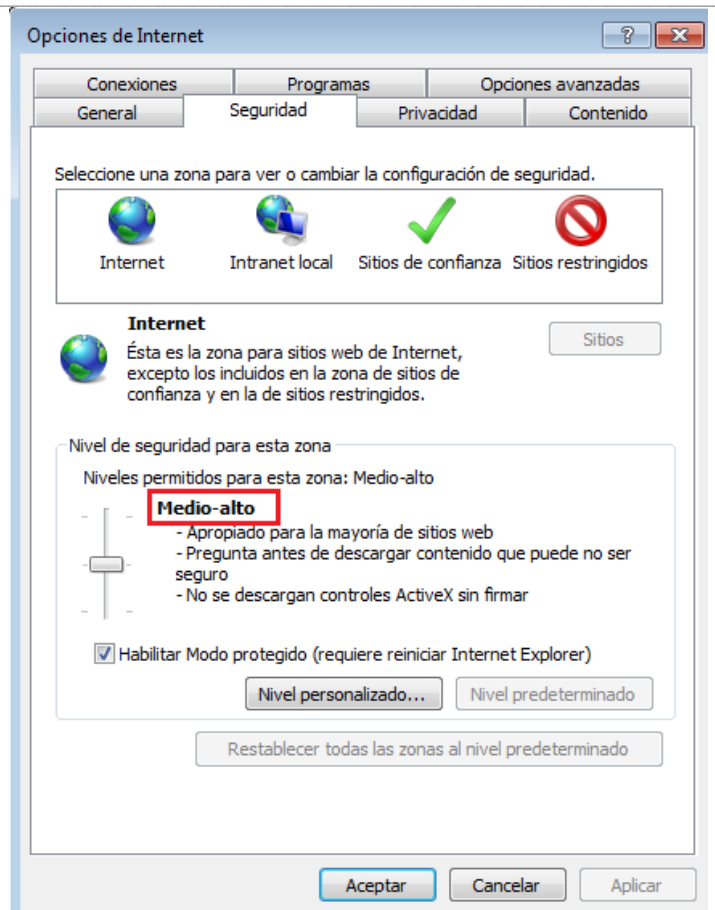


2. A continuación seleccionar la pestaña «Privacidad», donde se debe cerciorar de que esté activado el «bloqueador de elementos emergentes». De esta manera no aparecerán ventanas no deseadas, que en la mayoría de las ocasiones son intentos de fraude.

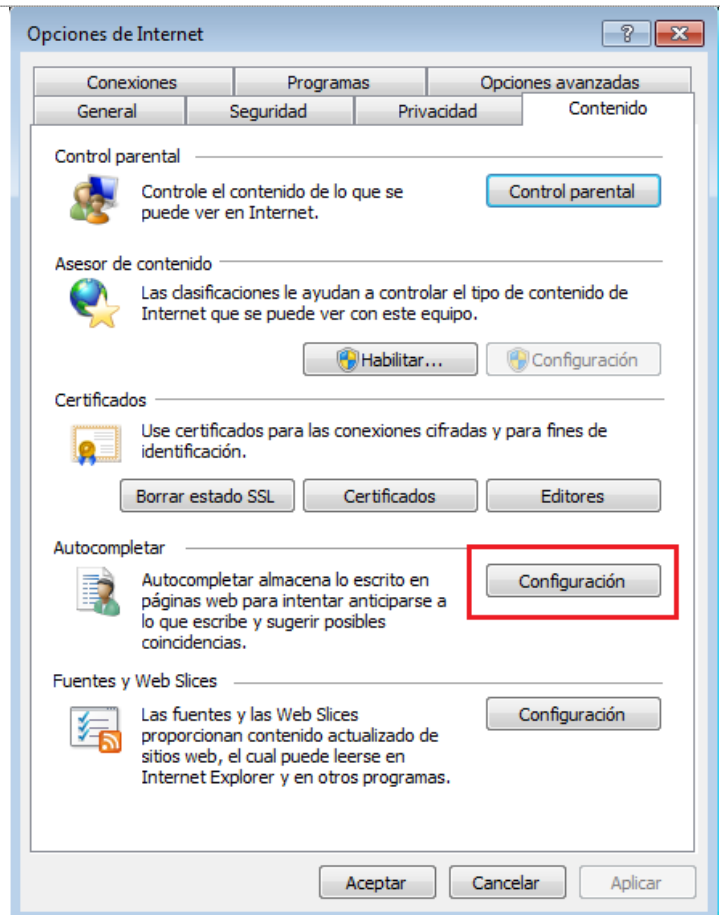


3. En esta misma pestaña, fijar el nivel de configuración, como mínimo, en «Media-alta».

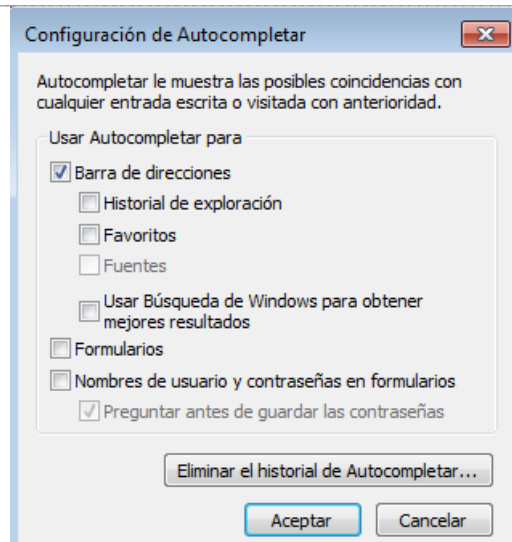
4. Después de realizar los dos pasos anteriores, acceder a la pestaña «Seguridad» y establecer el nivel de seguridad para esa zona de Internet, que siempre deberá ser «Alto» o «Medio-Alto».



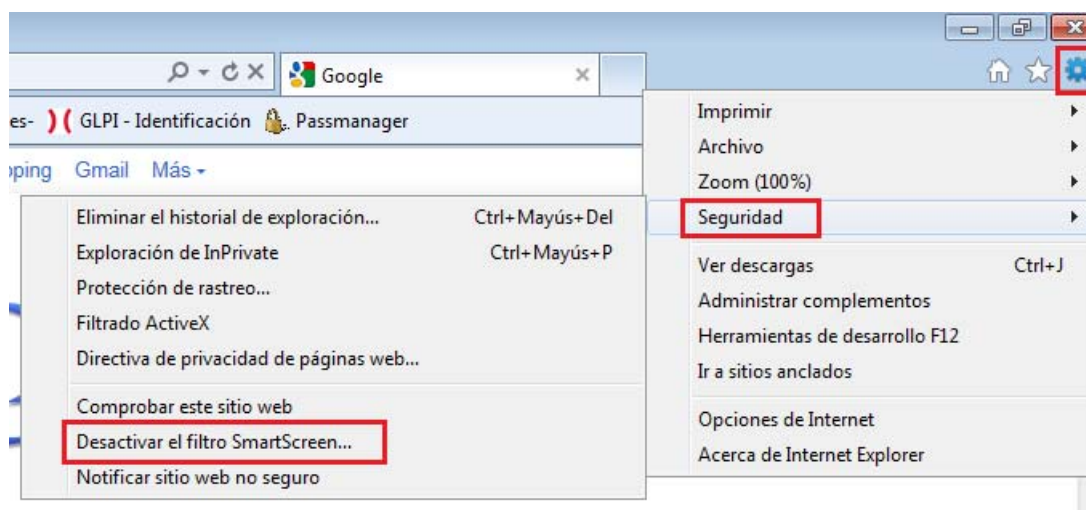
5. Si el ordenador es compartido, es un portátil o se encuentra en un lugar público, es importante configurar la función de autocompletar para que no se guarden las contraseñas, al menos las más importantes. Para ello ir a la pestaña «Contenido» y dentro de ella a «Autocompletar» > Configuración».



En la nueva ventana que aparece por pantalla se pueden ajustar las opciones de guardado de nombres de usuario y contraseñas.



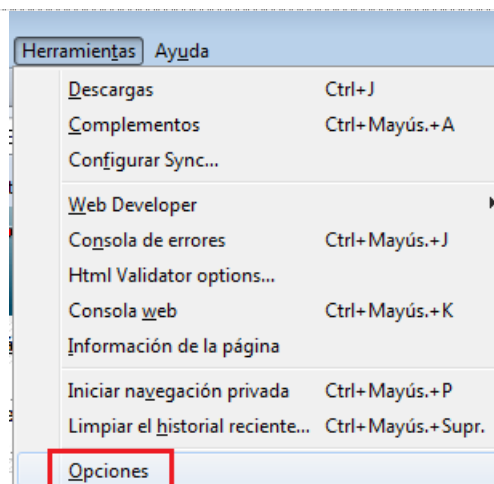
6. Para acabar, diríjase de nuevo al menú «Herramientas» y seleccionare la opción «Seguridad > Filtro SmartScreen» y comprobar que esté activado dicho filtro. Con esta opción se evitará que puedan suplantar la página de su banco o similares.



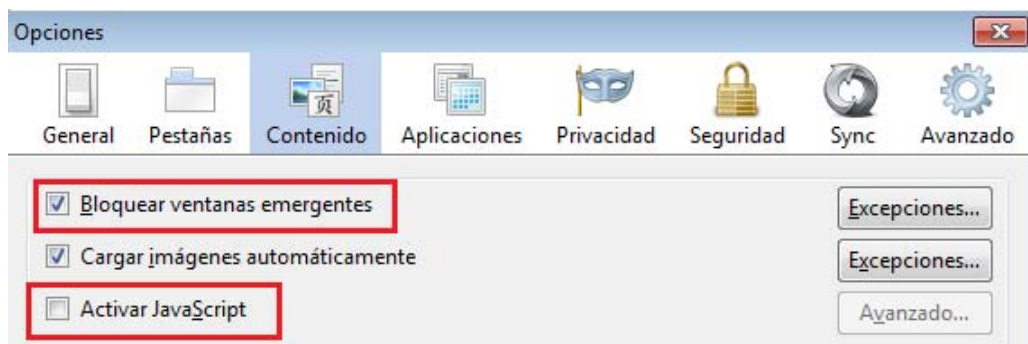
Firefox

Todo lo que te vamos a explicar para la navegación segura con Firefox es para su versión 6. Siga estos pasos:

1. Para evitar la aparición de las molestas ventanas emergentes, que en ocasiones suelen ser intentos de fraude, ir al menú superior (si no aparece, probar a pulsar la tecla ALT) y acceder a «Herramientas > Opciones».



Una vez ahí seleccionar la pestaña «Contenido» y activar la opción «Bloquear ventanas emergentes».

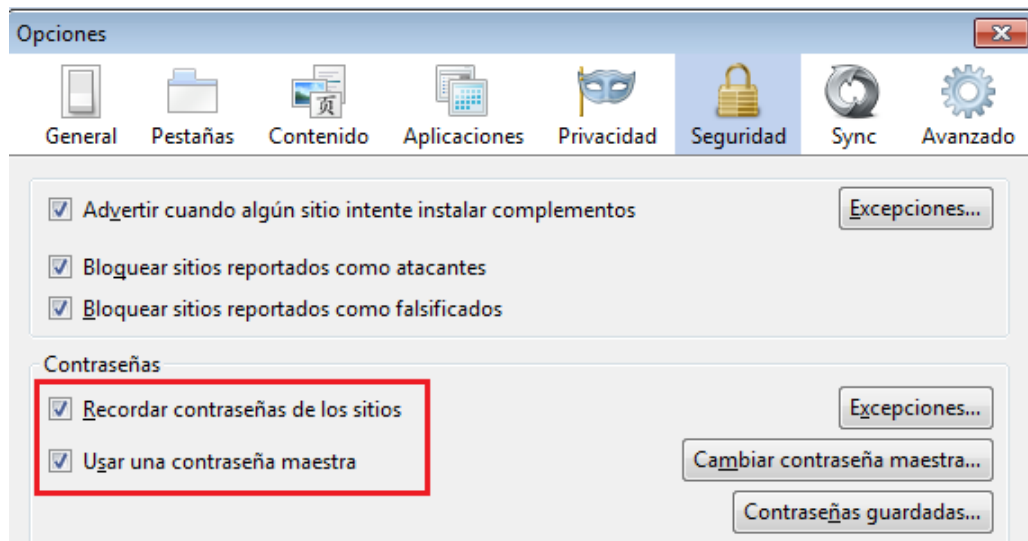


2. En esa misma pestaña, es recomendable que desactivar la ejecución de Java y JavaScript, aunque esto dependerá de la confianza que se tenga en la página accedida. Existen páginas en las que interesará activarlo porque ésta indique que es necesario para su funcionamiento.

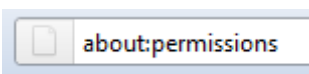
Otra opción es usar complementos de Firefox que permitan ejecutar Java y JavaScript sólo en los sitios de confianza que el usuario indique, como por ejemplo NoScript.

3. Es muy importante que tener cuidado con las contraseñas que se almacenan en el navegador. Al introducir usuario y contraseña en una página aparece un mensaje del navegador preguntando si se desea que la guarde. Si se desea almacenar las contraseñas en el navegador, es recomendable utilizar una contraseña maestra para protegerlas, sobre todo si el ordenador es un portátil que puede ser extraviado o robado. Para ello ir al menú «Herramientas > Opciones > Seguridad», y en el apartado de contraseñas activar la casilla «Usar una contraseña maestra».

Así el navegador almacenará las contraseñas que se deseen, pero para acceder a ellas se deberá introducir la contraseña maestra, que sólo el propietario conozca.



4. Escribiendo en la barra de direcciones about:permissions se accede a una ventana desde la que se pueden manejar opciones de seguridad para diferentes sitios web. Aparecerán aquellos que tengan alguna clase de información guardada (contraseñas, cookies...) y permite elegir cómo se quiere que se maneje esa información.



Se recomienda seleccionar «Bloquear» en todas las opciones, aunque siempre dependerá del sitio web que se trate y de la confianza que se tenga en él.



En cualquier caso

No hay que olvidar que aunque estas configuraciones ayudan a estar protegido, no evitan por completo todos los riesgos. Siempre es necesario apoyarlo con unos buenos hábitos de navegación y con sentido común.

2.2.3. Contraseñas seguras

Por muy seguro que sea un sistema, no servirá de nada si un atacante consigue el nombre y contraseña de un usuario legítimo.

Actualmente, el método más extendido para obtener acceso a información personal que se ha almacenado en un equipo y/o servicios en línea es mediante contraseñas.

La mayoría de las veces una contraseña es la única barrera entre los datos confidenciales y los ciberdelincuentes. Por lo que merece la pena invertir un poco de tiempo y esfuerzo para gestionarlas eficazmente. Utilizar contraseñas robustas evita que suplanten su identidad.



¿Qué debe tener una contraseña para ser realmente segura?

Una buena contraseña debe cumplir, al menos, tres de estas cuatro características:

- Tener números
- Tener letras
- Tener mayúsculas y minúsculas
- Tener símbolos (\$, @, &, #, etc.)

A parte, para que una contraseña sea segura también debe cumplir los siguientes requisitos:

- La longitud no debe ser inferior a siete caracteres. A mayor longitud más difícil de adivinar.
- No debe formarse con números y/o letras que estén adyacentes en el teclado. Ejemplos de malas contraseñas son: 123456, 1q2w3e o 123QWEasd.
- La contraseña no debe contener información que sea fácil de averiguar, por ejemplo, nombre de usuario de la cuenta, información personal (cumpleaños, nombres de hijos, etc.)
- No debe contener palabras existentes en algún idioma. Los ataques de diccionario prueban cada una de las palabras que figuran en el diccionario y/o palabras de uso común.

Buenas prácticas

- No usar la misma contraseña para diferentes cuentas. Sobre todo si son de alto riesgo, como las de los servicios bancarios o comerciales.
- La contraseña es algo privado, no se puede dejar escrita en ningún sitio, y mucho menos al lado del ordenador.
- Cambiar las contraseñas que traen por defecto los dispositivos y servicios en línea. Un ejemplo es el de los router WiFi, que traen por defecto contraseñas públicamente conocidas, que un atacante podría utilizar.
- Limitar el uso de las contraseñas almacenadas en el navegador para los servicios críticos. Si es posible el mejor sitio es la memoria de uno mismo.

Trucos para crear contraseñas seguras

- Usar una frase fácil de memorizar. Una vez hecho esto, se pueden hacer combinaciones con las distintas palabras que componen la frase: utilizar la primera letra de cada palabra, utilizar la última letra de cada palabra, etc.

Ejemplo: Utilizar la primera letra de cada palabra.

Frase: El 4 de Noviembre es mi cumpleaños.

Contraseña: E4dNemc

- Usar una «semilla» y aplicarle un «algoritmo»: En cada lugar donde se deba crear una contraseña, se pensara en una «semilla», que no es más que una palabra que ayude a recordar ese lugar. A la semilla se le aplica un «algoritmo» que es una combinación de pasos que se utilizaran para crear las contraseñas de cualquier sitio. La ventaja de utilizar este método es que sólo será necesario recordar el algoritmo.

Ejemplo: Recordar contraseña de Hotmail.

Semilla: hotmail

Algoritmo: Quitarle las tres primeras letras, poner en mayúsculas la primera letra, añadir al principio el número 82, añadir el final los símbolos *#.

Contraseña: 82Mail*#

Aplicaciones que pueden ayudar

Comprobador de contraseñas:

Cuando no se está seguro de si la contraseña que se ha elegido es lo suficientemente segura, se puede utilizar un medidor de fortaleza de la contraseña:

Comprobador de contraseñas / Password

- Acceso aplicación: <http://password.es/comprobador/>

Gestores de contraseñas:

Cuando se manejan muchas cuentas se vuelve complicado recordar la contraseña asociada a cada una de ellas. Lo peor que se puede hacer en ese caso es optar por utilizar la misma contraseña para todos los sitios, ya que si se descubre la contraseña de acceso a alguna de estas cuentas, un atacante podrá fácilmente acceder al resto de ellas. Para solucionar este problema, existen los gestores de contraseñas.

Un gestor de contraseñas es un programa que se utiliza para almacenar contraseñas. Nos permite recordar todas las contraseñas, claves de acceso y nombres de usuario que se necesitan para acceder a una cuenta o página de Internet. La información se almacena cifrada y sólo se puede acceder a través de una clave.

En el punto 3.1 “Keepass Password Safe”,e puede ver la forma de configurar una de estas herramientas.

Cómo proteger las contraseñas en el navegador

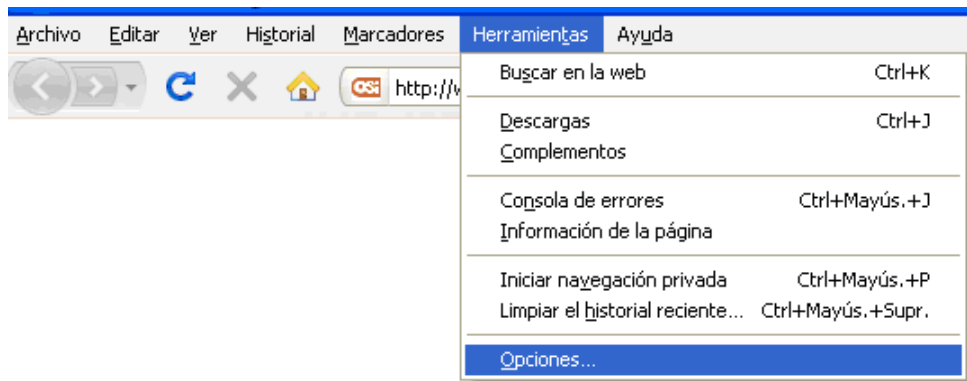
Seguramente el navegador sea el programa que se utiliza para acceder a la mayoría de las cuentas: ver el correo electrónico, acceder a nuestro banco o conectarnos a las redes sociales. Utilizar una contraseña diferente para cada cuenta puede resultar algo lioso, pero actualmente los navegadores disponen de gestores de contraseñas capaces de almacenar los nombres de usuarios y contraseñas utilizados para acceder a los distintos sitios.

Sin embargo, si se comparte el ordenador, guardar en el navegador las contraseñas hace que las personas que también vayan a utilizar el equipo puedan acceder a diferentes sitios Web con las cuentas que estén almacenadas, dejando acceso a otras personas que no deberían tener acceso; es posible evitar este inconveniente y seguir almacenando las contraseñas en el navegador utilizando una contraseña maestra, que se solicitará cada vez que se quiera acceder a alguna cuenta que este almacenada en el navegador. La importancia de utilizar dicha contraseña es muy grande, ya que sin ella, cualquier persona que acceda a al ordenador podrá ver todas las parejas de nombre de usuario/contraseñas que se han utilizado para navegar por Internet.

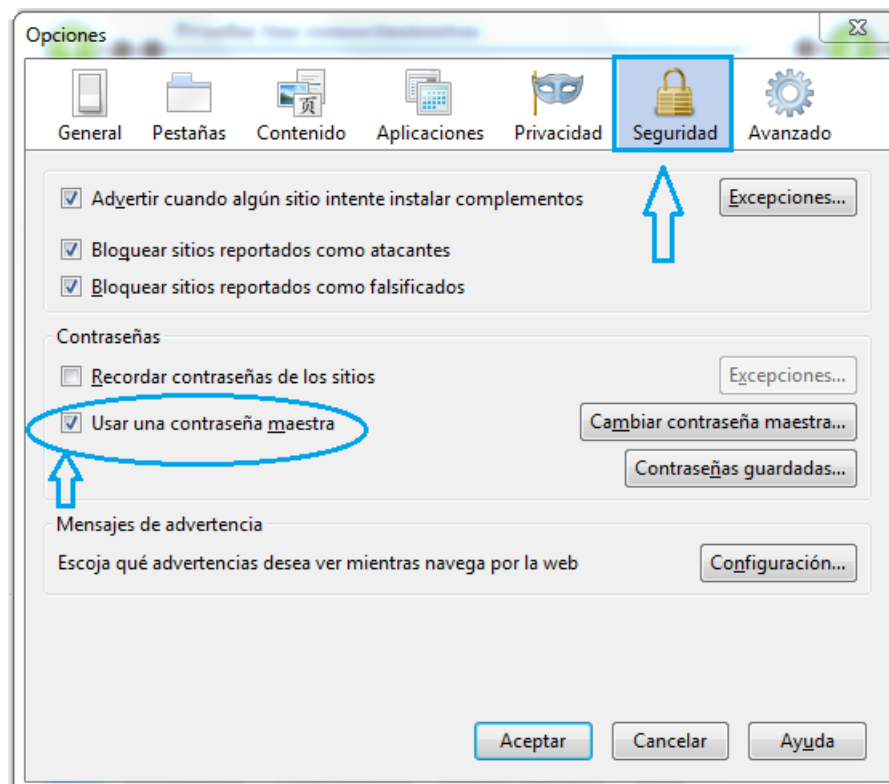
Firefox:

Para proteger las contraseñas almacenadas en el navegador Firefox con una contraseña maestra hay que realizar los siguientes pasos:

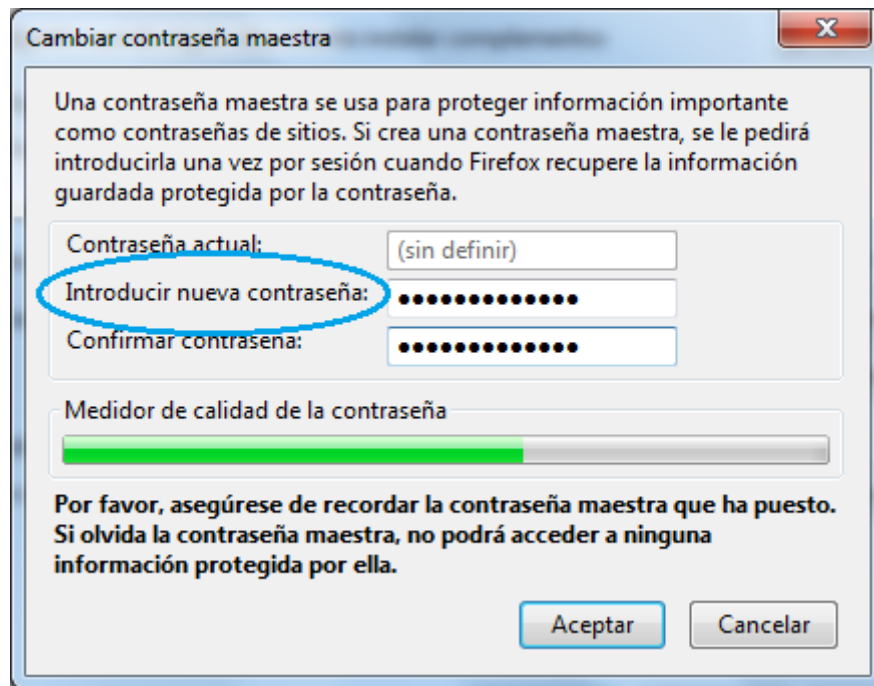
1. Iniciar Firefox
2. Ir al menú «Herramientas», y hacer clic en «Opciones»



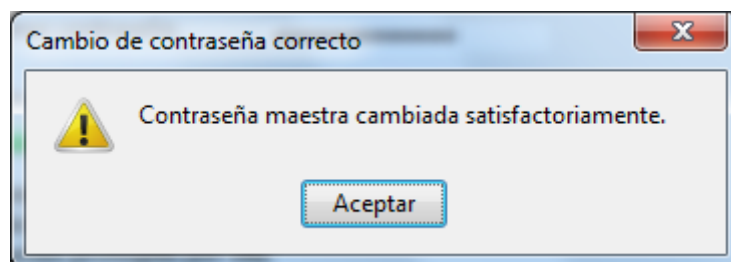
3. Seleccionar el icono «Seguridad» y activar la casilla «Usar contraseña maestra».



4. En el cuadro de diálogo que aparece, se debe introducir la contraseña. Para que la contraseña sea lo más segura posible Firefox proporciona un Medidor de la calidad.



5. Aceptar los cambios realizados. Aparecerá una ventana indicando que la contraseña maestra se ha cambiado correctamente.



6. Reiniciar el navegador para que se hagan efectivos los cambios.

Después de seguir estos pasos, cada vez que se quiera acceder a un sitio del que Firefox tenga guardada la contraseña, pedirá introducir la contraseña maestra para poder acceder a dicho sitio.

A Recordar

“Las contraseñas son como la ropa interior. No puede dejar que nadie la vea, debe cambiarla regularmente y no debe compartirla con extraños”.

“Una contraseña es un secreto que no hay que contar a nadie”.

“Si las llaves de casa no se las deja a nadie, ¿por qué va a dejar sus contraseñas a alguien?”.

“Para evitar que le atraquen por la calle toma ciertas medidas de seguridad: no camina por sitios extraños, lleva bien guardada la cartera, etc. Si quiere evitar que le roben por Internet información personal, dinero, etc. tome también las medidas de seguridad necesarias.”

2.2.4. Cortafuegos

Internet es una red de ordenadores pública y, al igual que se acceden a otros equipos, por ejemplo, para ver páginas Web, el resto también puede tener acceso al equipo. Esta herramienta hace de barrera entre el PC e Internet, y ayudará a proteger el equipo ante:

- Usuarios maliciosos que buscan tener acceso al sistema.
- Virus que se propagan a través de la red saltando de ordenador en ordenador; también conocidos como gusanos.

Un cortafuegos no es la solución a todas las amenazas de la red pero su ausencia sí supone un grave riesgo para la seguridad.

El cortafuegos es una de las principales líneas de defensa. Sin él, tan sólo cuando se conecta un sistema a la red, puede ser víctimas de un virus.

¿Qué hace un cortafuegos?

El principal objetivo de un cortafuegos es permitir al usuario controlar las conexiones que se establecen entre el ordenador e Internet. Para ello se debe indicar qué conexiones se consideran necesarias, y rechazar las que no. Por ejemplo:

- Sí se debe permitir que el fabricante del programa antivirus se conecte al equipo para que pueda descargar los ficheros necesarios con los que reconocer los últimos virus.
- No se debe permitir conexiones de fuentes desconocidas. Para evitarlo, los cortafuegos por defecto bloquean todas las conexiones entrantes y sólo permiten las que se indiquen expresamente.

Lo más complicado de un cortafuegos es configurarlo correctamente, de modo que no se bloqueen conexiones legítimas -navegación, actualizaciones, programas P2P, etc- pero sí el resto. Sin embargo, debido a que los cortafuegos van aprendiendo las reglas según se le van indicando, aunque al principio resulte un poco incómodo confirmar programa a programa a cuál se le permite conectarse a Internet y a cuál no, en pocos días ya estarán definidas las reglas más habituales y se podrá navegar por Internet de forma normal y con más seguridad.

Existen dos tipos de cortafuegos, los de escritorio -internos- y los hardware -externos-, cada uno con sus ventajas e inconvenientes.

Cortafuegos de escritorio/software

Estos cortafuegos hay que instalarlos en cada PC que se vaya a conectar a Internet. Están orientados a usuarios domésticos y, para facilitar su configuración, disponen de un modo de aprendizaje.

Al detectar un intento de conexión a/desde Internet, muestran un aviso indicando el programa que se quiere conectar, y piden la conformidad del usuario para permitir la comunicación. El cortafuegos almacena las decisiones para que sólo se alerte al usuario la primera vez que se realiza la conexión.

Se recomienda disponer de un cortafuegos de escritorio en cada uno de los ordenadores de uso doméstico que se vayan a conectar a Internet

La mayoría de sistemas operativos –entre ellos Windows 7, Vista y XP - lo integran por defecto.

También se pueden utilizar cortafuegos de otros fabricantes instalándolos como cualquier otra aplicación. En ocasiones también vienen integrados en paquetes de seguridad junto a soluciones antivirus. Sin embargo, es muy importante tener en cuenta que sólo puede haber un cortafuegos de escritorio

funcionando en el equipo; por lo que, si se quiere utilizar un cortafuegos que no sea el del sistema operativo, antes de empezar a ejecutar el nuevo cortafuegos, habrá que deshabilitar el de Windows.

Estas herramientas generalmente aportan más información y permiten más control sobre las conexiones, aunque también son más complejas de manejar.

Cortafuegos hardware

Son dispositivos externos que se conectan entre el PC y la red. Con un solo cortafuegos hardware se pueden proteger varios ordenadores que compartan la conexión a Internet.

Muchos de los routers que ofrecen los ISP al contratar la conexión a Internet por ADSL o Wifi se pueden utilizar como cortafuegos. Pero aunque cada vez están más enfocados a usuarios domésticos, siguen siendo más difíciles de configurar que los de escritorio.

Las organizaciones y las empresas usan estos dispositivos como primera defensa de protección ante ataques externos.

2.2.5. Portátiles

El ordenador portátil es muy utilizado, porque en él se puede llevar toda la información que se necesita para trabajar, realizar trámites por la red o disfrutar de algunas aficiones.

Debido a que es un dispositivo pequeño y fácilmente transportable, es más vulnerable a golpes porque se esta llevando continuamente de un sitio a otro, etc. Por lo que no se debe descuidar su seguridad física.

El robo no sólo constituye una pérdida material, sino de la información personal almacenada que los delincuentes pueden aprovechar para realizar algún tipo de fraude, como el robo de identidad, para realizar acciones en su propio beneficio, simulando ser el propietario del portátil el que ha efectuado dicha acción.

Guardar el portátil en un maletín adecuado cuando se transporta, evitará que cualquier golpe pueda dañar el equipo y la información.

Protección

Seguir las siguientes medidas de protección para el portátil:

- Llevarlo siempre consigo, no lo abandonarlo en una mesa, en el coche, lugares públicos, etc. En caso de tener que dejarlo, utilizar un cable de seguridad para sujetarlo a la mesa o a un objeto suficientemente grande. Si se va a dejar en el coche, ocultarlo.
- No dejar abiertas conexiones que lo delaten (bluetooth y/o WIFI). Apagarlas
- Utilizar un maletín/bolsa o mochila lo más discreta posible, que no delate el contenido.
- En los hoteles, durante las ausencias, guardar en un lugar seguro y utilizar un cable de seguridad. Ocultarlo de la vista.
- Si hay posibilidad de hacerlo, registrar el portátil en la página Web del fabricante, de esta forma quedará constancia de la identificación del portátil asociada a una serie de datos personales, y en caso de recuperar el portátil habría un registro del titular del mismo.

Conexión del portátil a la red

Si el portátil se va a conectar a la red donde se encuentre (bares, aeropuertos, hoteles, etc.). Se debe poner especial cuidado a la hora de conectarse, tanto a redes cableadas como redes inalámbricas, de las que no se tenga conocimiento de quién es el administrador.

Las redes no seguras pueden esconder riesgos y amenazas como por ejemplo, la posibilidad de infección y el robo de información.

Cuando se vaya a conectar a redes de terceros en hoteles, aeropuertos, bares, etc. Seguir estos consejos:

- Tener el sistema operativo y el software instalado actualizado
- Tener instalado un antivirus actualizado.
- Activar el cortafuegos.
- No utilizar una cuenta de administrador para navegar
- Poner especial atención cuando se visiten páginas en las que se tengan que indicar datos sensibles: cuentas bancarias, contraseñas, etc.

Información transportable

Ya que dentro del portátil se alberga mucha información personal e importante, para minimizar el impacto en caso de robo se debe:

- Utilizar contraseñas seguras para el inicio de sesión y aquellas aplicaciones que lo permitan. No guardar las contraseñas junto al portátil, maletín, etc.
- Si se van a almacenar las contraseñas en el ordenador, se debe utilizar un gestor de contraseñas
- Utilizar programas de cifrado para los ficheros personales, de forma que si alguien tiene acceso a estos ficheros, que no pueda interpretar su contenido.
- Utilizar contraseñas seguras en los programas del portátil y cifrar los archivos personales para aumentar la seguridad de la información en caso de robo.

En caso de robo

Procedimiento en caso de robo del portátil:

- Denunciarlo a la policía.
- Comunicarlo a la empresa, si es un ordenador corporativo.
- Comunicar al banco que bloquee el acceso a las cuentas hasta que se puedan cambiar las contraseñas.
- Cancelar los certificados digitales necesarios para evitar que se usen en su nombre.
- Modificar las contraseñas de cuentas de correo, redes sociales, servicios de Internet (alojamiento, blogs, foros etc.)
- Mandar un correo a todos los contactos para prevenirles, por si reciben algún correo “sospechoso”.

2.2.6. Pendrive o Memoria USB

Este pequeño dispositivo llamado pendrive ya es obligatorio en el bolsillo de muchos, y algunos hasta ya se les hace difícil la vida sin él, por el hecho de ser un accesorio práctico, fácil de usar y compatible con todos los sistemas operativos del mercado, incluyendo Windows, Mac y Linux.

Técnicamente, el pendrive es un dispositivo portátil de almacenamiento, compuesto por una memoria flash, accesible a través de un puerto USB. La mayoría de nosotros llevamos en nuestro lápiz de memoria o pendrive, programas tales como navegadores web portables, lectores de correo portables, gestores de contraseñas portables, antivirus portables, datos personales, fotografías, etc.



Pero, ¿qué sucedería si se pierde el pendrive o alguien lo conecta a su equipo?.

Además de perder la información (y el dispositivo en sí) los datos estarían al alcance del que lo encontrara, así tendría no sólo las cuentas de correo, por ejemplo, además tendría las contraseñas y quizá otros datos personales.

Para evitar que la información pueda ser utilizada por otras personas, con el riesgo que ello supone, se recomienda protegerla encriptando los datos, de forma que si se pierde el dispositivo, al menos se pueda estar tranquilo de que nadie pueda visualizar y utilizar los archivos y datos personales.

Existen varias herramientas gratuitas que nos permiten encriptar estos dispositivos, en el punto 3.2. “USB Safeguard” se puede ver la forma de configurar y usar una de estas herramientas..

Prevenir infecciones

El intercambio de pendrives para intercambiar archivos o transportarlos a otros sistemas o entre personas es algo muy habitual. Por lo que se tiene que tener cuidado a la hora de conectarlo. La mayoría de los antivirus detectan la conexión de este tipo de dispositivos y se puede lanzar un análisis del antivirus sobre el mismo, pero de no ser así, se debería de lanzar de forma manual un análisis sobre él para evitar que pueda contagiar el equipo.

Cuando se introduce una memoria flash (USB) o un CD en un sistema Windows, se siguen las instrucciones contenidas en un archivo llamado "autorun.inf". Normalmente se utiliza para ejecutar los instaladores de los CD's. Sin embargo, hay ocasiones en las que están dentro de una memoria flash e indican ejecutar un virus que se autocopia en el PC. Como se lleva una memoria de un PC a otro, el virus se difunde si el antivirus no lo detecta. Por lo que se recomienda deshabilitar esta funcionalidad siguiendo las indicaciones del fabricante:

- <http://support.microsoft.com/kb/967715/es>

2.2.7. Móviles

Actualmente casi todo el mundo dispone de un teléfono móvil, que permite: llamar, enviar mensajes, hacer fotos, consultar la agenda, etc. Ya que es un dispositivo muy personal y con mucha información privada, es un buen motivo para mantenerlo seguro.

Proteger tu móvil

Al igual que se usan pautas de sentido común cuando se utiliza el ordenador, no se deben olvidar cuando se utiliza el móvil. Sobre todo se debe tener en cuenta el tipo de información que se guarda en él: las fotos personales, los mensajes que se reciben, agenda de teléfonos, etc. Toda esta información privada y personal es muy importante ya que contiene datos personales y los de contactos.



Para mantener seguro el móvil hay que asegurarse de proteger:

- La tarjeta de memoria. Normalmente guarda los datos personales: fotos, música, calendario de eventos, etc. Esta tarjeta se puede extraer, se debe guardar si no se va a utilizar el teléfono y se deben hacer copias de seguridad regularmente.
- La tarjeta de la operadora (SIM), que permite realizar las llamadas. Se debe proteger con una contraseña (PIN). En caso de robo, contactar con el operador para bloquearla. Realizar copias de seguridad de los datos periódicamente.
- El teléfono. Evitar dejarlo en lugares en los que lo puedan robar. En caso de pérdida o robo, denunciarlo a la policía, y comunicarlo al operador. Se debe apuntar el número identificativo del teléfono (IMEI) para indicárselo al operador en estos casos. Proteger el móvil con una contraseña, y hacer que se bloquee automáticamente cuando se deje de usar un tiempo determinado. Apagarlo cuando no se vaya a utilizar.
- Se debe mantener el software del móvil actualizado.

¿Si el teléfono móvil es un smartphone?

Los dispositivos móviles inteligentes, más conocidos como smartphones, son una fusión (y evolución) de los ordenadores actuales y, por tanto, son muchos los riesgos que también les afectan. Además, el uso cada vez más generalizado de estos dispositivos, hace que los atacantes lo incluyan dentro de sus objetivos preferidos.

Bluetooth

La mayoría de los móviles, disponen de un mecanismo para comunicarse con otros dispositivos mediante Bluetooth. Esto no es más que una forma de que dos dispositivos cercanos se entiendan para intercambiar información, bien con otro móvil, ordenador, impresora, etc.

Por ello recomendamos que se sigan las siguientes recomendaciones en relación al Bluetooth:

- No aceptar conexiones de dispositivos desconocidos

- Apagar el Bluetooth cuando no se utilice.
- Cuando se active. Hacerlo en modo "invisible", para que cualquier persona desconocida no pueda saber que está conectado

Contraseñas en el móvil

El móvil alberga gran cantidad de datos personales que se deben proteger con contraseñas seguras. La primera que se debe activar es el PIN, o número de identificación personal, ya que impedirá en caso de robo que otras personas puedan activar el móvil para realizar llamadas, consultar tu agenda, etc.

No se debe guardar el código personal, PIN, con el número de desbloqueo PUK, que proporciona el operador.

Activar la contraseña que bloquea el teclado del móvil, así cuando no se este utilizando protegerá el dispositivo si se deja olvidado o lo roban.

Fraude

La mayoría de los fraudes a través del móvil vienen derivados de incitar al usuario a llamar a números de tarificación especial, 800, 77x, 905... publicidad engañosa a través del envío de mensajes fraudulentos para ganar «regalos increíbles», puestos de trabajo, línea eróticas, consultorios sentimentales o de tarot. Se debe evitar contestar a estos mensajes basado en la ingeniería social.

Amenazas móviles

El móvil puede ser vulnerable si no se protege, ya que está expuesto a las mismas amenazas que los ordenadores: virus, spam, phishing, fraude, privacidad, etc. Al fin y al cabo es un miniordenador de mano.

Por ello se deben seguir las recomendaciones de seguridad básicas, igualmente que se hace para el ordenador personal:

- Navegación
- Correo electrónico
- Redes sociales
- Trámites en línea
- Juegos en línea

Si se va a conectar con el móvil a una red wifi, se debe asegurar que es una red segura, y no una red desconocida que pueda poner en peligro la información personal y el móvil.

2.2.8. Antes de que sea demasiado tarde...

Por último, en caso de tener un incidente –tener presente que no existe la seguridad al 100%- también se puede recurrir a la funcionalidad de restauración del sistema y a las copias de seguridad.

Restauración del sistema

Ante un incidente que afecte al adecuado funcionamiento del equipo, se puede utilizar la funcionalidad de restaurar el sistema, para volver a un estado previo en el que el PC funcionaba correctamente.

Diferentes motivos pueden traer consigo el mal funcionamiento del sistema operativo y por extensión del ordenador en general.

- La infección de un virus, que además de comprometer la seguridad del sistema puede afectar a su rendimiento.
- Los sucesivos ciclos instalación/desinstalación. Y en ocasiones, la instalación de ciertos ficheros –archivos de sistema, actualizaciones, controladores- .

Para minimizar el impacto que tiene este mal funcionamiento existe la posibilidad de restaurar el sistema. Restaurar sistema supervisa los cambios realizados en el PC y crea periódicamente puntos de restauración que pueden identificarse fácilmente en un calendario.

Ante un incidente, se puede navegar por el calendario para restaurar el sistema a un estado previo, que resuelva el problema.

Elegir un punto de restauración previo, en el que el PC funcionara correctamente, para que todo vuelva a la normalidad

Qué recupera exactamente la restauración del sistema

En ocasiones existe confusión respecto a los ficheros que recupera esta funcionalidad.

- La restauración del sistema únicamente recupera ficheros del sistema, configuraciones del sistema operativo, archivos del registro y la mayoría de los programas instalados.
- No se trata de una copia de seguridad de todos los archivos del equipo, solo restaura los archivos indispensables para su correcto funcionamiento.
- Por el motivo anterior, al restaurar el equipo a un estado previo, no recuperara los archivos personales -documentos de texto, imágenes, hojas de calculo, etc.-, pero tampoco perderá los ya existentes, que permanecerán en el equipo.

Para estar preparado ante un imprevisto

Para entender más en profundidad la funcionalidad de Restaurar Sistema, como configurarla y como utilizarla consulte en el punto 3.3. “Restauración del sistema en Windows XP“ para ver como se configura en Windows XP.

Para más información puede consultar las guías del fabricante:

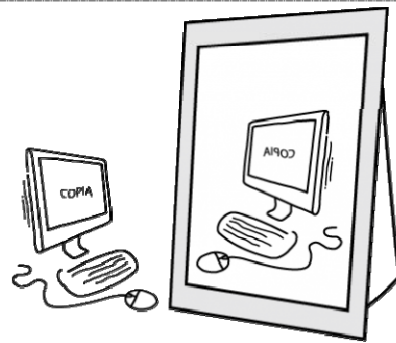
- Cómo restaurar el sistema operativo Windows 7:
<http://windows.microsoft.com/es-XL/windows7/products/features/system-restore>
- Cómo restaurar el sistema operativo en Windows XP a un estado anterior:
<http://support.microsoft.com/kb/306084/es>

Copias de seguridad

Por la acción de un virus, de usuarios malintencionados, por fallos en el hardware, o simplemente por accidente o descuido la información contenida el equipo puede resultar dañada o incluso desaparecer.

Las Copias de Seguridad (en inglés, 'backup') son réplicas de datos que permiten recuperar la información original en caso de ser necesario; virus, fallo eléctrico, borrado accidental, etc.

Existen diferentes métodos para realizar las copias de seguridad; manualmente o con un programa específico como se verá más adelante.



Consideraciones previas

Antes de realizar una copia de seguridad se debe tener en cuenta una serie de aspectos:

- Decidir qué guardar en función de los archivos que se consideren más importantes e irremplazables. Un programa se puede recuperar con el CD original o descargarlo de la página del fabricante.
- Calcular cuánto espacio de almacenamiento se necesita. Si la cantidad de datos que va a copiar es muy grande, quizá se necesite repartir la copia.
- Una vez calculado el espacio. Decidir cómo se va a distribuir los datos entre las diferentes opciones que se dispone. Un DVD, varios CDs, un disco duro externo,...
- Establecer un criterio temporal y planificado para realizar la siguiente copia. Marcar estos criterios como rutinarios para mantener esta buena práctica.
- Independientemente del método que se elija, es recomendable guardar al menos una copia de seguridad fuera del ordenador.
- Guardar las copias en un buen lugar, para asegurarse que ante un incidente se puede recurrir a ellas fácilmente. Valorar quien puede acceder a ellas para asegurar su confidencialidad.

Tipos de copias

Estas pueden ser:

- **Completa:** copia todos los ficheros indicados. La primera copia de seguridad que se haga, suele ser de este tipo, aunque después puede no ser necesario copiar todos los archivos, sino sólo aquellos que hayamos modificado o creado desde la última copia... Las copias completas, al realizar una copia de todos los ficheros, ocupan gran cantidad de memoria, por lo que no es práctico hacer siempre copias de seguridad completas, sino alternarlas con los otros dos tipos que se explican a continuación.
- **Diferencial o acumulativa:** sólo copia los ficheros que han sido modificados o creados desde la última copia completa. A modo de ejemplo, esto quiere decir que si el lunes se realiza una copia completa y el martes se crean tres nuevos archivos y se modifican dos de los que ya estaban en la copia completa, en la copia diferencial del martes, únicamente se guardarían estos cinco ficheros. Si el miércoles se hiciera otra copia diferencial, copiaría los archivos creados o modificados desde el lunes también, que es cuando fue la copia completa, independientemente que dichos ficheros fuesen nuevamente modificados el miércoles o no. Esto hace que las copias realizadas sean cada vez más grandes.

Si fuera necesario restaurar los datos, para tener lo mismo que se tenía anteriormente, se necesitaría la copia completa y la última copia diferencial.

- **Incremental:** en este caso, se copiarán los archivos creados o modificados desde la última copia, sea del tipo que sea. Siguiendo el ejemplo anterior de una copia completa el lunes, si se hace una copia incremental el martes, se grabarían los datos creados o actualizados desde el lunes y, si se realizara una copia incremental el miércoles, se copiarían los datos modificados o creados desde el martes. Por tanto el tamaño de las copias será menor que en el caso anterior.

Para restaurar los datos, necesitarías la última copia completa y todas las incrementales desde entonces.

Generalmente, se suele hacer una primera copia de seguridad completa y luego varias copias de seguridad incrementales o diferenciales según la criticidad que sea la información a almacenar. La frecuencia con la que se quiera hacer copias de seguridad, también depende de lo importante que sea la información a guardar; en grandes empresas que generan muchos datos todos los días, necesitarán realizar copias diarias, pero en ordenadores domésticos pueden ser semanales, quincenales o, como muy poco, mensuales.

También algunas herramientas permiten sincronizar los archivos indicados con los del dispositivo externo al realizar una copia de seguridad, de forma que si por ejemplo se ha eliminado un archivo, al hacer la copia de seguridad lo eliminaría también de allí, quedando una copia exacta cada vez de lo que se tiene en el ordenador.

Copias manuales

Basta con seleccionar los archivos que se desean salvaguardar, y copiarlos en el soporte que se escoja.

- En un CD o DVD.
- En otro ordenador, en un disco duro externo o memoria USB.
- En un segundo disco duro

Los siguientes soportes son los más básicos, se puede utilizar cualquier otro siempre que se este seguro de que se puede recuperar la información.

Copias con herramientas específicas del sistema operativo

Los sistemas operativos actuales, proporcionan programas que permiten realizar las copias de seguridad de una manera fácil y cómoda.

En el punto 3.4. “Copia de seguridad del equipo y restaurar el sistema en Windows XP” se puede ver cómo se pueden realizar copias de seguridad en Windows XP

Recuperar datos

En caso de ser necesario recuperar los datos, se debe utilizar el soporte en el que se realizó la copia: CD, DVD, disco duro externo, memorias USB, etc.

Para restaurar los datos se tendrá que utilizar el mismo método utilizado al realizar la copia de seguridad:

- **Manual:** restaurar los datos seleccionando el dispositivo donde se realizó la copia, y volviendo a trasladar todos los archivos al equipo.
- **Herramientas específicas:** Utilizar la misma herramienta con la que se creó la copia.

3. Recursos y utilidades

Para poder aplicar algunas de las indicaciones mencionadas en el apartado anterior, existen una serie de herramientas o utilidades que permiten mejorar la seguridad de los equipos. El sistema operativo de los equipos suele proporcionar algunas de esas herramientas que ayudan a proteger los equipos, sin necesidad de utilizar otros productos auxiliares, como pueden ser el cortafuegos o las herramientas de Windows para restauración de sistema o para realizar copias de seguridad de archivos, pero que por desconocimiento se recurre a otros productos que se han indicado o buscado.

En este apartado se señalará como se configuran y usan algunas de esas herramientas.

Las principales herramientas de protección según su categoría podrían ser:

Spyware

Espía, o spyware, es una aplicación con una función visible (una barra de tareas o un juego por ejemplo) y otra oculta. Recolecta sin consentimiento estadísticas de uso de la aplicación y de sitios visitados, y suele instalar nuevas aplicaciones sin autorización, que podrían ser dañinas para el equipo. Esta violación a la privacidad del usuario, y la apertura de una puerta digital que no tiene control, motivó la creación de software anti-spyware para eliminarlo.



Existen varias herramientas gratis, las versiones actuales de antivirus suelen incluir la detección de este tipo de malware, pero una herramienta específica de este tipo de detecciones es Spybot Search & Destroy que a diferencia de otros productos similares, aún no ha evolucionado a incluir antivirus.

- **Spybot Search & Destroy:** <http://www.safer-networking.org/>

Una vez instalada la aplicación, hay que actualizar su base de datos, ya que sólo detecta el spyware que conoce. Aunque puede funcionar en forma residente (es decir, analizando los datos que llegan al equipo), la primera vez hay que dejar que analice el equipo por completo buscando espías. Si encuentra alguno lo listará, y habrá que elegir si se anula (lo que puede hacer que otra aplicación deje de funcionar) o no. Se suelen listar aquí las cookies, archivos de seguimiento que dejan los sitios que se visitan. No son dañinas de por sí, pero muchos usuarios las consideran una violación a su privacidad, y por eso los programas ofrecen borrarlas. Hay que tener en cuenta, sin embargo, que hay servicios Web que se negarán a aceptar al usuario si éste no permite la carga de cookies en su computadora.

Antivirus

La otra aplicación que revisa los contenidos del disco del PC para verificar que está libre de infecciones es el antivirus: previene la instalación de virus, gusanos y troyanos en la computadora. Aunque antes los virus eran muy dañinos, formateando discos o borrando fotos, hoy suelen apuntar más que nada a su difusión masiva. No obstante, hay que evitar su instalación, sobre todo de los troyanos, que esconden tras

una fachada inocente (un juego en flash, un salvapantallas) la intención de permitir a un tercero la entrada en nuestro equipo para robar información almacenada en él, o usarlo para dirigir ataques a servidores de Internet.

Los antivirus también deben actualizarse como ya se indicó. Son capaces de revisar los archivos adjuntos que llegan en el e-mail, y deben usarse para analizar cualquier programa que se vaya a instalar en la PC, sobretodo si se descargó de un sitio Web o lo envió otra persona, por muy de confianza que sea. Entre los antivirus gratis podemos encontrar AVG, Avast!, Avira o Microsoft Security Essentials.

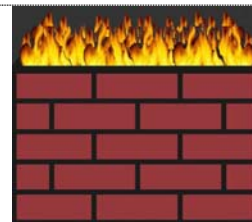
- Avast free: <http://www.avast.com/es-ww/index>
- AVG free: <http://free.avg.com/es-es/homepage>
- Avira free: <http://www.avira.com/es/avira-free-antivirus>
- Microsoft Security Essentials: <http://windows.microsoft.com/es-es/windows/security-essentials-download>

También hay alternativas comerciales, que en función de las versiones pueden incluir diferentes detecciones o utilidades en un mismo producto como puede ser antivirus, antyspyware, antispam y/o firewall. Entre algunos de los distintos fabricantes nos encontramos con ESET, Kaspersky, McAfee, Symantec, Norton, Panda y Trend Micro.

Cortafuegos

El tercer elemento para mantener seguro el PC es el firewall, o cortafuegos, que monitorea el intercambio de datos entre los programas e Internet, sólo si están autorizados para hacerlo, y evitando que un sitio con código malicioso ataque al equipo.

Dependiendo del desarrollador y de cómo esté configurado, el firewall será más o menos celoso a la hora de aprobar la conexión de una aplicación o proceso a Internet. Al ejecutarse la aplicación por primera vez (desde que se instaló el cortafuego) una ventana informará que intenta conectarse a la Red, y nos pedirá que se apruebe o deniegue este pedido. Es posible crear una regla para que no vuelva a pedir permiso.



Si no se reconoce el programa (porque el cortafuegos muestra sólo el nombre del archivo) es posible consultar sitios como www.processlibrary.com/es/, o www.ppedia.com, que dan información sobre los procesos que se ejecutan en el PC, para determinar si son peligrosos o no.

Windows XP y Vista incluyen un firewall, que se activa desde el Panel de Control. En el caso del XP, se debe instalar el Service Pack 2, que crea un centro de seguridad para gestionar el cortafuegos, el antivirus y las actualizaciones del sistema operativo. El de Vista es más sofisticado: controla las conexiones hacia afuera y las que vienen de Internet. Otros cortafuegos gratis son Comodo y Zone Alarm.

- Comodo: <http://www.personalfirewall.comodo.com>

- Zone Alarm: <http://www.zonealarm.com>

Mac OS X también tiene un firewall integrado; se configura en Preferencias del Sistema>Seguridad . Lo mismo ocurre con cualquier distribución de Linux. Algunas incluyen además la interfaz gráfica para configurarlo; si no, se puede probar con FireStarter (www.fs-security.com), que permite adecuar fácilmente el cortafuegos (llamado iptables) a las necesidades deseadas.

- FireStarter: <http://www.fs-security.com>

3.1. KeePass Password Safe

KeePass Password Safe es una herramienta que sirve para almacenar contraseñas de forma segura.

Permite recordar todas las contraseñas, claves de acceso y nombres de usuario que se necesiten para acceder a una cuenta o página de Internet. La información se almacena cifrada y sólo se puede acceder a ella a través de una contraseña maestra que se deberá memorizar.



KeePass
Password Safe

Introducción

Muchos de los servicios que presta Internet, exigen que se identifique y por eso, cada vez es más normal tener que acceder a sitios web como usuarios autenticados, ejemplo:

- Acceder al correo electrónico (gmail, yahoo mail, hotmail, etc...)
- Acceder a redes sociales (facebook, tuenti, etc...)
- Acceder a foros privados
- Editar webs en gestores de contenidos (MediaWiki, Joomla, Drupal,...)
- Subir videos o fotos (youtube, picasa, flickr, ...)
- Acceder a plataformas web de formación (Mentor, ISFTIC, Universidades, ...)
- Facturas electrónicas: compañías de luz, gas, teléfono, móvil, internet.

Para acceder a cualquiera de estos lugares, es necesario introducir el nombre de **usuario** y la **contraseña**, lo que exige acordarse de decenas de nombres de usuario y decenas de contraseñas, así como decenas de URLs para acceder a dichos sitios web.

Muchas personas para simplificar, deciden utilizar el **mismo nombre de usuario y la misma contraseña para todos los sitios**, lo cual es cómodo, pero supone un riesgo de seguridad importante ya que si algún usuario malintencionado consigue averiguar la



contraseña, podrá entrar en todos los sitios privados. Esto les ha pasado a algunos personajes públicos y les ha causado varios problemas

Muchos sitios web requieren autenticación

Otras veces se utilizan **contraseñas fáciles** como números sencillos, apellidos, fecha de nacimiento, teléfono, login del usuario, etc. A menudo, cuando se utilizan contraseñas un poco más raras, se suelen **anotar en un post-it**, lo cual es más inseguro que tener una contraseña sencilla.

Cada vez se hace más necesario tomar conciencia de la importancia de utilizar unas contraseñas seguras para evitar que nadie se **suplante la identidad** ocasionando graves problemas.

KeePass es una aplicación que facilitará enormemente la gestión de usuarios y contraseñas para acceder a sitios privados de Internet.

Características principales de KeePass

- Almacenar URL, nombre de usuario (login), contraseña (password) e información adicional que se desee.
- Función de Escritura Automática (acceder a los sitios automáticamente).
- Base de datos cifrada de forma segura y protegida con contraseña maestra y/o un archivo llave.
- Generador de complejas contraseñas.
- Traducido a varios idiomas (Español, Catalán, Gallego, etc...).
- Software libre (licencia GPL). Versiones para Windows, Linux y MAC. Código fuente disponible.



La contraseña maestra da acceso al resto de contraseñas

Utilizando KeePass

En sistemas Windows, KeePass se puede descargar desde el enlace: [KeePass download](#). Descargar en una carpeta temporal (ejemplo en C:/TEMP) la versión KeePass Portable. Una vez descargado el archivo zip con la versión portable de KeePass, se debe descomprimir utilizando algún descompresor como WinZip o 7zip y lo mejor es descomprimirlo en una memoria USB para utilizar KeePass en cualquier PC sin necesidad de instalación.

Para instalar KeePass en **Ubuntu** (solo disponible para las últimas versiones de Ubuntu), se pueden utilizar los repositorios de Ubuntu, por lo tanto, la instalación es tan sencilla como ejecutar el siguiente comando desde una consola: ***sudo apt-get install keepassx***

Idioma Español

Para ejecutar KeePass en **Windows**, se debe hacer doble clic en el archivo **KeePass.exe** que se encuentra en la carpeta donde se haya descomprimido KeePass Portable.

Inicialmente el programa está en Inglés, pero KeePass está traducido a varios idiomas entre los que se encuentran el Español, el Catalán y el Gallego. Para seleccionar el idioma Español, se necesita descargar el archivo de idioma desde el enlace: KeePass translations. Se debe descomprimir el archivo de idioma Spanish.lng en la carpeta donde se encuentre el programa. Después ejecutar KeePass.exe e ir a **View > Change Language > Spanish**. Para otros idiomas, habrá que repetir el mismo proceso.

Una vez seleccionado el idioma Español, reiniciar keepass. Se verá la pantalla inicial de KeePass:



Pantalla inicial de KeePass

La pantalla de KeePass inicialmente aparece vacía. Lo primero que se tiene que hacer es crear una nueva base de datos en la que almacenar las contraseñas. Para ello, ir a **Archivo > Nuevo**.

El programa pedirá una contraseña maestra (Master Password) para proteger la nueva base de datos. Esa contraseña es **la única contraseña que se debe recordar**. Con la contraseña

maestra se tendrá acceso a todas las URLs, usuarios y contraseñas almacenadas en la base de datos. Si se olvida o pierde la contraseña maestra, se perderá el acceso a la base de datos de KeePass ya que no se puede recuperar.

El programa pedirá que se introduzca de nuevo la contraseña maestra, para evitar errores al teclear y una vez comprobado que las dos contraseñas introducidas coinciden, aparecerá la ventana con la base de datos cargada.



Establecemos la contraseña maestra

En la siguiente captura se ve la pantalla que aparece nada más crear una base de datos.



Base de datos recién creada

Observar que aparece una carpeta llamada **General** desde la que cuelgan cinco carpetas que servirán para clasificar las contraseñas. Estas carpetas se pueden eliminar, cambiarlas de nombre o crear nuevas carpetas, así como personalizar los iconos.

Añadir entradas

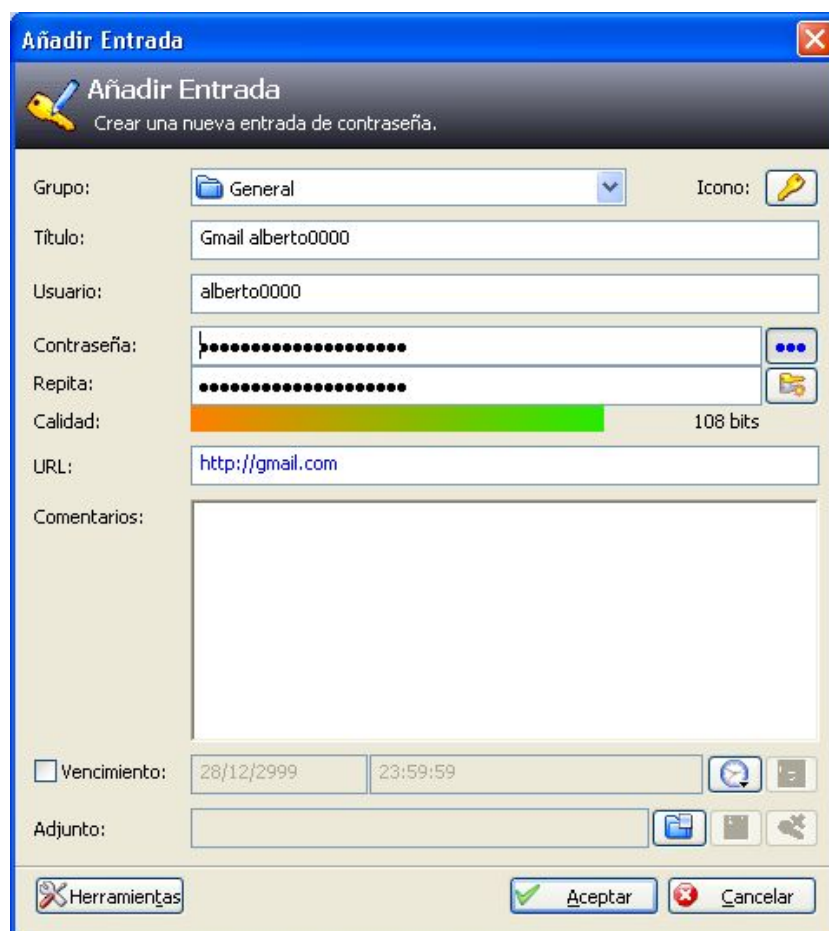
Para crear una entrada. Suponga que se quiere almacenar el usuario y la contraseña de nuestra cuenta de correo de Gmail. Los datos básicos que se van a almacenar son la URL, el nombre de usuario y la contraseña. Suponga que los datos son los siguientes:

URL: `http://gmail.com`

nombre de usuario: `alberto0000`

contraseña: `manzana`

Para añadir la nueva entrada ir a **Editar > Añadir Entrada**.



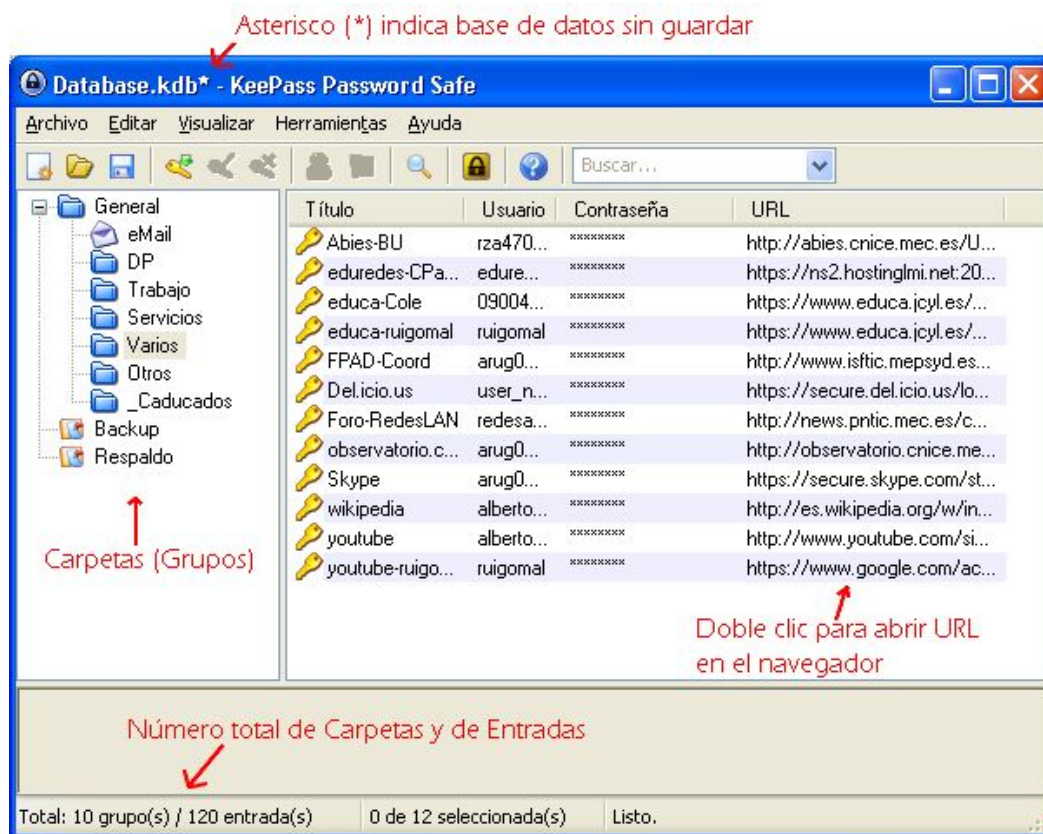
Añadir entrada

A continuación se explicaran brevemente los campos más significativos de la ventana anterior:

- **Grupo:** Carpeta en la que se almacenará la entrada
- **Título:** Título de la entrada. Se recomienda coincida con el título de la página
- **Usuario:** El login de usuario
- **Contraseña:** La contraseña del usuario. La barra -Calidad- (representa la seguridad de la misma)
- **URL:** La URL del sitio web
- **Comentarios:** Apartado para introducir información adicional, observaciones, etc...
- **Vencimiento:** Si el sitio web, por seguridad obliga a cambiar la contraseña cada cierto tiempo, se puede establecer esta alarma que indicara cuánto falta para que la contraseña caduque.

Si se hace clic en -Aceptar-, la entrada quedará creada y la base de datos ya no estará vacía, sino que dispondrá de una entrada. Al haber modificado la base de datos, en la barra del título de la ventana de KeePass aparece el nombre de la base de datos seguido de un asterisco que significa que la base de datos ha sido modificada pero no ha sido guardada. Al cerrar la aplicación preguntará si se desea guardar la base de datos. También se puede guardar en cualquier momento la base de datos haciendo clic en el icono del disquete de la barra de herramientas.

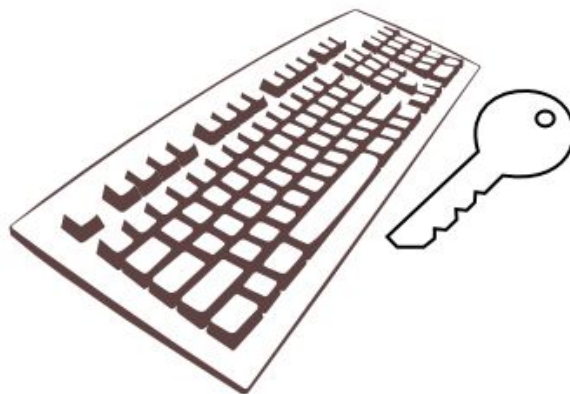
Se pueden crear tantas entradas como se quieran. En la siguiente captura de pantalla se ve una base de datos con varias entradas creadas:



Se pueden crear todas las entradas que se necesiten

Escritura Automática

La función de Escritura Automática (también conocida como función Auto-Tipéo o Auto-Type) es la característica más importante de KeePass ya que permite abrir la URL y autocompletar el nombre de usuario y la contraseña, de forma automática.



KeePass tecleará de forma automática

La escritura automática se realiza en dos pasos:

1. Abrir la URL: Haciendo doble clic sobre la URL de la entrada almacenada en KeePass, se abrirá el navegador de Internet y accederá a la URL

2. Realizar la escritura automática del nombre de usuario y la contraseña: Desde la ventana del navegador se debe teclear Ctrl + Alt + A que es la combinación de teclas de KeePass para disparar la Escritura Automática. Se recomienda que el título de la entrada coincida, al menos en parte, con el título de la página de entrada de los sitios web (página de login) para que KeePass pueda distinguir qué usuario y qué contraseña debe escribir.

Normalmente, la página de login, dispone de un formulario con dos cajas de texto, una para introducir el **nombre de usuario** y otra para introducir la **contraseña**. KeePass suele detectar correctamente el formulario de entrada y no tiene problemas para introducir el nombre de usuario y la contraseña automáticamente.

En algunos sitios web, la página de login no coincide con la página principal del sitio, en tal caso, la URL que hay que almacenar en KeePass es la URL de la página de login.

En otros casos, la página de login es muy compleja con varias cajas de texto que pueden confundir a KeePass y es necesario personalizar la secuencia de Escritura Automática, para ello, hay que editar la Entrada haciendo Clic derecho sobre ella > **Editar/Visualizar Entrada** > **Herramientas** > **Escritura Automática Personalizar Secuencia**. En la ventana comentarios aparecerá la secuencia por defecto de Auto-Type: {USERNAME}{TAB}{PASSWORD}{ENTER} que significa que KeePass escribirá el nombre de usuario, tecleará un tabulador, escribirá la contraseña y tecleará Intro de forma automática. Si la página de login tiene otro diseño y fuera necesario teclear tres veces el tabulador para escribir la contraseña, crearíamos la siguiente secuencia: {USERNAME}{TAB}{TAB}{TAB}{PASSWORD}{ENTER}. Si la página de login pide un código de verificación (como por ejemplo el correo web del ISFTIC), se tendría que teclear manualmente. En tal caso se debe modificar la secuencia para que se rellene el usuario y la contraseña, teclear un tabulador para posicionar el cursor en la casilla para introducir el código de verificación, y quitar {ENTER} para que no envíe el formulario: {USERNAME}{TAB}{PASSWORD}{TAB}

Las funcionalidades de KeePass se pueden incrementar instalando plugins. Uno de los plugins más interesantes es el plugin KeeForm que incrementa las funcionalidades de la escritura automática.

Seguridad en Escritura Automática

KeePass utiliza una doble técnica de envío de pulsaciones de teclas junto con la utilización del portapapeles, de forma que al realizar Escritura Automática, es capaz de despistar a casi todas las aplicaciones espías que suelen utilizar los hackers para capturar contraseñas. La gran mayoría de los troyanos que espían el teclado (KeyLoggers) y espían el portapapeles, son inútiles cuando se utiliza KeePass para identificarse en los sitios web, por eso, se convierte en una herramienta recomendable principalmente cuando utilizamos un PC que es utilizado por otras personas (PCs del centro educativo, cibercafés, etc...).

Generador de contraseñas

KeePass dispone de un Generador aleatorio de contraseñas que puede servir para elegir las contraseñas cuando se registre en los sitios web. Para utilizarlo ir a **Herramientas** > **Generador de contraseñas**, y se verá la siguiente pantalla:



Generador de contraseñas aleatorias

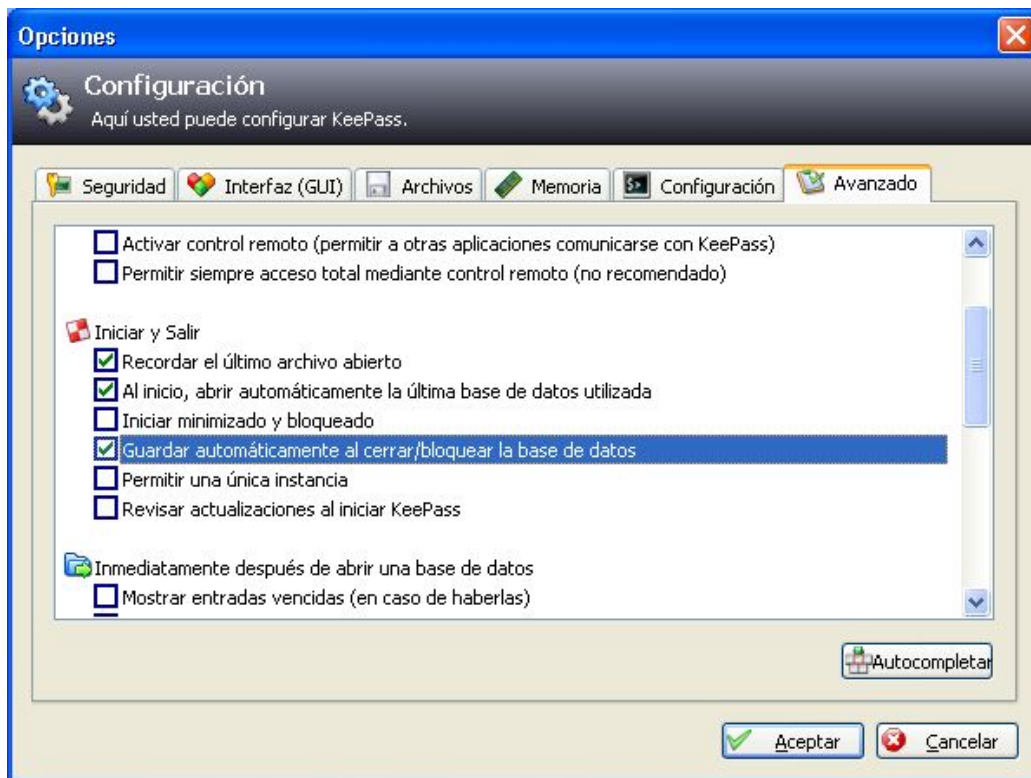
Se puede elegir los caracteres de los que se quiere se componga la contraseña (mayúsculas, minúsculas, números y otros símbolos). Se debe asegurar que la contraseña que se genere funcione en el sitio web donde se quiere establecer porque a veces no aceptan ciertos símbolos en la contraseña (espacios, comillas, barras, etc...)

Como ahora se dispone de KeePass, en lugar de utilizar contraseñas fáciles es mejor utilizar **contraseñas complejas**. Ejemplo, para el correo de Gmail, en lugar de utilizar como contraseña 'manzana', se puede utilizar 'z86O#?ik/+z9i4IQWqb' que es mucho más difícil de averiguar. La ventaja es que es muy improbable que alguien pueda averiguar la contraseña haciendo pruebas, aunque la desventaja es que se **depende de KeePass**, porque casi nadie podrá aprenderse de memoria una contraseña tan compleja, pero esto no es problema porque se puede tener el KeePass Portable en el pendrive USB u oculto en alguna URL dentro de una página web.

Opciones de KeePass

KeePass permite personalizar algunas opciones. Para ello, ir a **Herramientas > Opciones**.

Entre otras opciones, se puede por ejemplo ir a **Herramientas > Opciones > Avanzado** y establecer las opciones que se ven en la siguiente figura, para que al ejecutar KeePass.exe abra automáticamente la base de datos y al cerrar el programa guarde los posibles cambios que se hayan podido hacer.



Opciones de KeePass

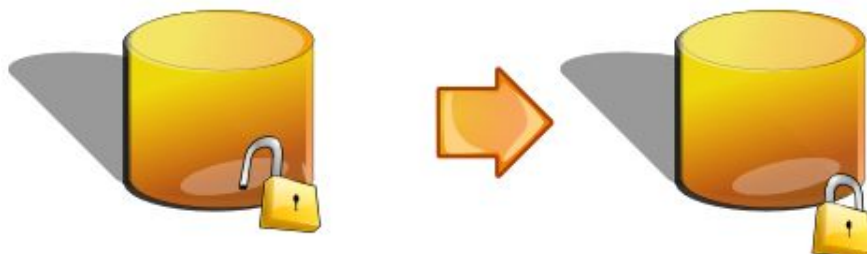
Otra opción interesante es la combinación de teclas para realizar la Escritura Automática que se puede personalizar desde **Herramientas > Opciones > Avanzado > Autocompletar**.

Seguridad de KeePass

KeePass guarda toda la información en la base de datos de KeePass, en un archivo que normalmente se llama **Database.kdb** aunque se puede darle otro nombre.

KeePass guarda en el archivo Database.kdb toda la información: URLs, nombres de usuario, contraseñas, información adicional, secuencias Auto-Type, etc... Para hacer copia de seguridad de KeePass, tan solo se debe salvaguardar el archivo Database.kdb.

El archivo Database.kdb se puede cifrar mediante el sistema **AES** o el **sistema Twofish**, reconocidos como dos de los mejores sistemas de cifrado. La **contraseña maestra no se almacena** en ningún lugar ni cifrada ni sin cifrar sino que es utilizada en el proceso de cifrado, lo que incrementa la seguridad.



La base de datos se guarda cifrada

Cada vez que se guarda el archivo Database.kdb en el disco duro, se aplica el algoritmo de cifrado un número elevado de veces consecutivas, **en torno a un millón**, para dar más fortaleza al cifrado. Si alguien consiguiera robarnos el archivo Database.kdb y quisiera tratar de descifrarlo por fuerza bruta probando todas las contraseñas posibles, debería aplicar el algoritmo de cifrado un millón de veces por cada clave, lo que tarda aproximadamente en torno a un segundo utilizando un PC rápido. Si se elige una contraseña maestra que tenga letras mayúsculas, minúsculas y números (60 caracteres distintos), de 6 caracteres de longitud ($60^6=46.656.000.000$ contraseñas posibles), harían falta unos mil quinientos años para que un PC pudiera probar todas las contraseñas posibles aplicando el algoritmo un millón de veces por contraseña ($46.656.000.000$ segundos = 1.500 años). Para elegir el algoritmo de cifrado y establecer el número de veces que se quiere que se aplique, ir al **Menú Archivo > Configuración de la base de datos**.

Para incrementar la seguridad, se puede además utilizar un **archivo llave** (Key File). El archivo llave es un archivo de 64 bytes de longitud que almacena una contraseña de 64 caracteres generada aleatoriamente. Sería como utilizar una contraseña de 64 caracteres y se puede utilizar como una seguridad extra además de la contraseña maestra. El inconveniente es que se debería guardar el archivo llave en el disco USB y si alguien lo roba, tendría la base de datos y el archivo llave.

Conclusiones

Si se quiere incrementar la seguridad de las contraseñas o manejar un número tan elevado de diferentes nombres de usuario y contraseña que cuesta recordar, KeePass es una herramienta excelente que facilitará el trabajo incrementando la seguridad. Se recomienda a todos aquellos que tengan dificultades para acordarse de sus contraseñas, que antes de utilizar una contraseña demasiado sencilla o tenerla anotada en un post-it en el monitor del PC, se animen a probar esta herramienta.

- KeePass Password Safe: <http://keepass.info/download.html>

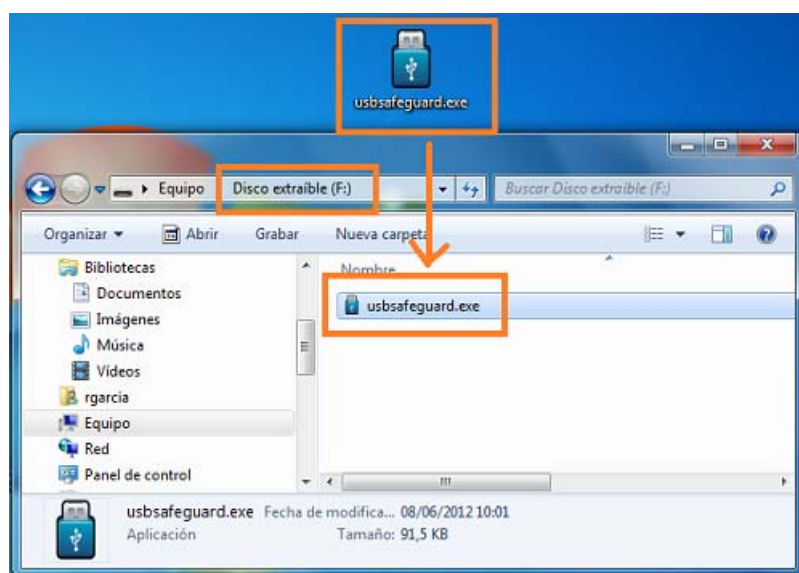
3.2. USB Safeguard

USB Safeguard es una herramienta que sirve para proteger el contenido almacenado en un pendrive (también conocido como memoria USB), cuando se accede desde un ordenador con sistema Windows.

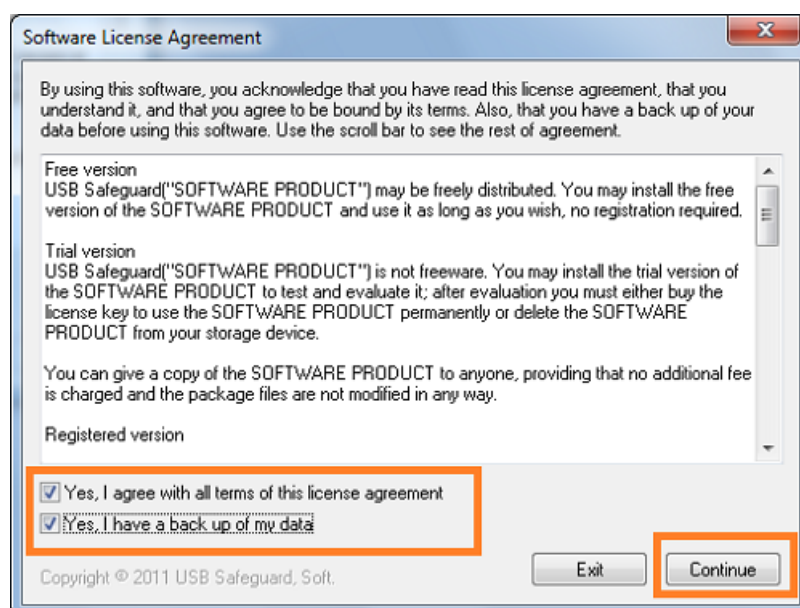
Evita que personas no autorizadas accedan a la información que almacena en él. Imagínese lo que podría pasar si se tiene almacenada información confidencial en el pendrive, se pierde o lo roban, y no estaba protegida esa información. Para evitar sustos y se recomienda utilizar USB Safeguard u otra herramienta similar.



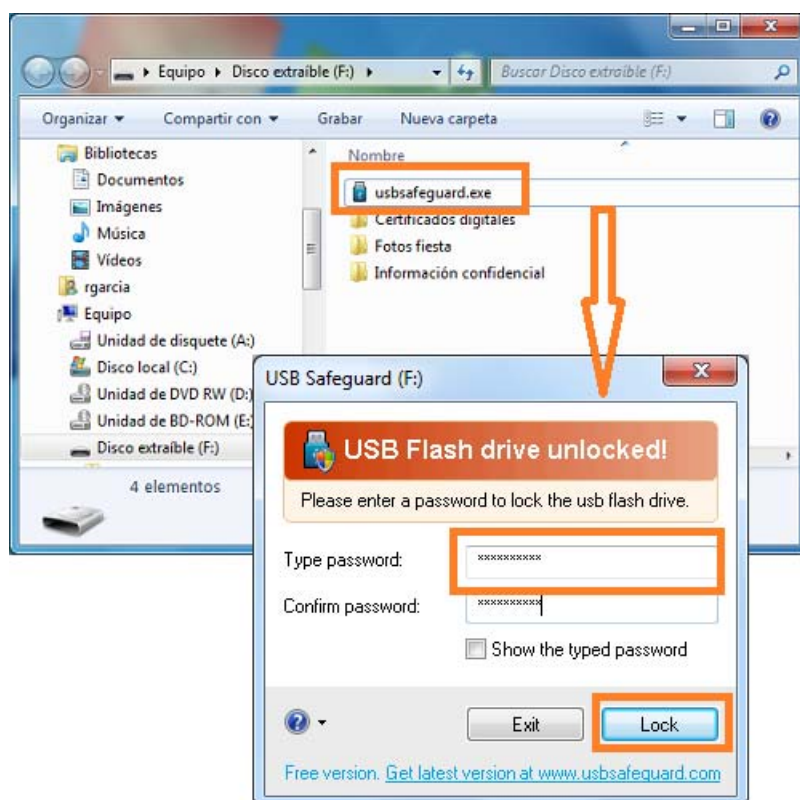
Su uso es muy sencillo, simplemente hay que descargar la herramienta ver enlace de descarga al final de este punto- y copiarla en el pendrive.



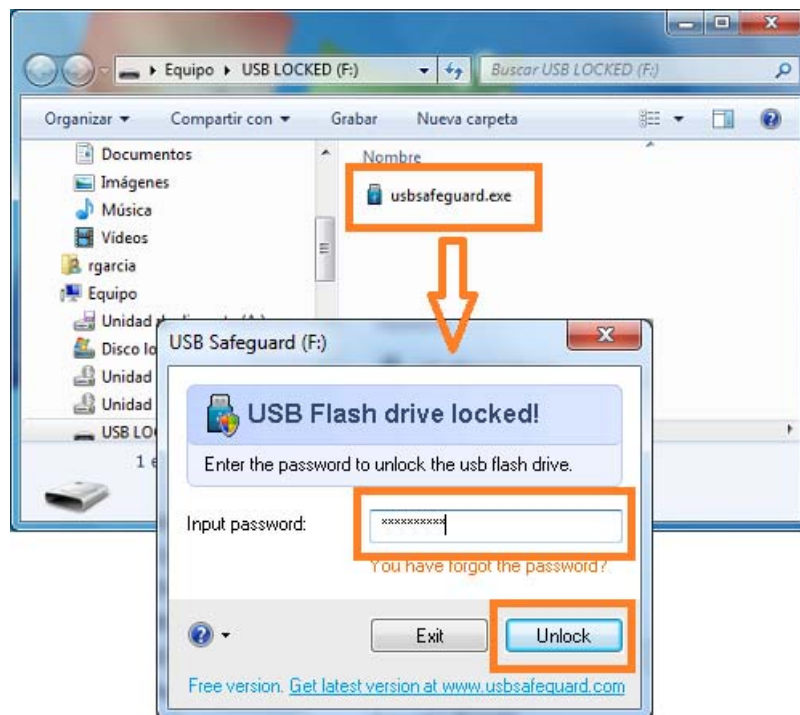
Antes de ejecutar por primera vez la herramienta, comprobar que el pendrive está vacío, ya que en este paso se borrará toda la información que contenga. En la instalación se solicitará la aceptación de los términos de licencia y, además, que se confirme que se tiene otra copia de los ficheros que pudiera tener el pendrive.



Instalada la herramienta, permite bloquear el acceso a los ficheros que se almacenen en el pendrive haciendo doble clic en el ejecutable, para introducir una contraseña que será la que proteja la información que se guardará en el pendrive. ¡Recuerde que la contraseña debe ser segura!



Cada vez que se bloquee el pendrive, se podrá utilizar una contraseña diferente. Una vez protegido el contenido del pendrive, sólo se verá el ejecutable de la herramienta. El proceso de desbloqueo también es muy sencillo, se deberá ejecutar el fichero e introducir la contraseña que se utilizó durante el proceso de bloqueo del mismo. Si ésta es correcta, se verá el contenido almacenado y se podrán incorporar ficheros o carpetas adicionales.



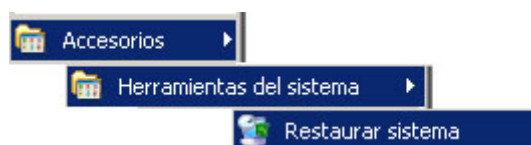
NOTA: La versión gratuita de la herramienta sólo funciona en pendrives de **2 Gigabytes de almacenamiento como máximo**.

- USB Safeguard: <http://www.usbsafeguard.com/download.html>

3.3. Restauración del sistema en Windows XP

Para acceder a la utilidad ir a:

Inicio > Todos los Programas > Accesorios > Herramientas de Sistema > Restaurar sistema.



Configuración Restaurar sistema

Si se va a:

Mi PC > Propiedades > Restaurar Sistema

Se podrá configurar las características de esta utilidad, desde desactivar esta opción en todas las unidades con solo marcar la casilla (muy útil cuando se va a desinfectar el ordenador de algún virus), hasta configurar cada unidad de manera independiente.



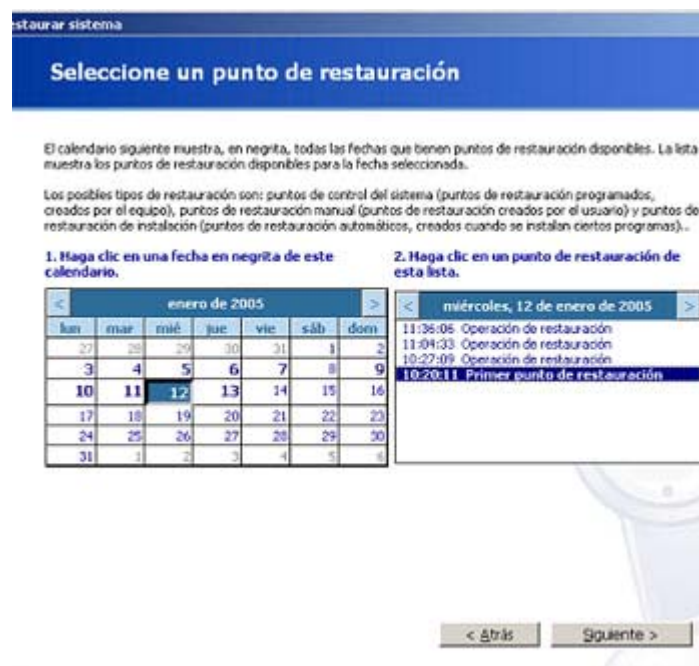
Cómo utilizar Restaurar sistema

En la primera pantalla escoger la opción deseada y avanzar con el botón siguiente.



Restaurar el equipo a un estado anterior

Aparecerá un calendario que muestra en negrita las fechas que tengan puntos de restauración disponibles.



Al seleccionar una fecha aparecerá una lista a la derecha con los distintos puntos de restauración disponibles en esa fecha. Se seleccionará el punto de restauración deseado y se pulsará **Siguiente**. Tras esto aparecerá una ventana con información sobre las tareas a realizar y solicitará confirmación. Pulsando en **Siguiente** se procederá a restaurar el sistema.

Crear punto de restauración

Se solicita un identificador para reconocerlo fácilmente cuando se quiera restaurar el sistema.



Tras introducir el identificador y pulsar en crear se habrá creado un punto de restauración que se almacenará con la fecha y la hora del sistema.

Deshacer la última restauración



Windows XP genera un punto de restauración automático cada vez que realiza una restauración. Esta opción permitirá deshacer los cambios realizados si estos no fueran satisfactorios. Aparecerá una ventana de confirmación informando de las tareas que Windows realizará para deshacer la última restauración.

Tras pulsar “siguiente” el sistema quedará tal y como se encontraba antes de realizar la última restauración.

3.4. Copia de seguridad del equipo y restaurar el sistema en Windows XP

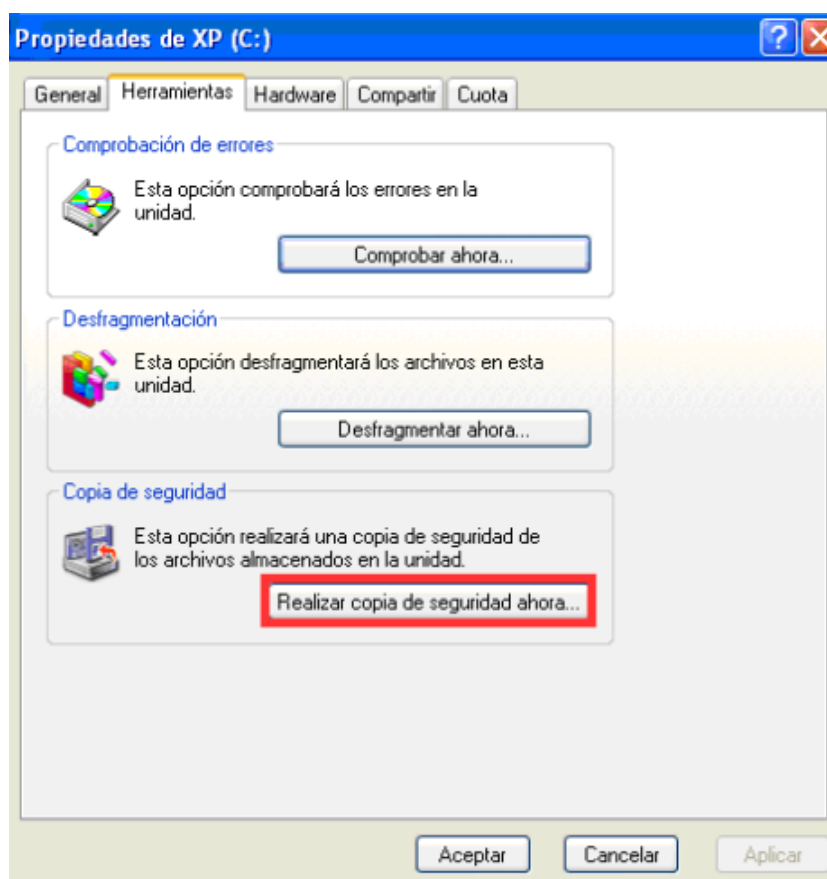
A partir de la versión XP, Windows incluye una herramienta bastante útil para hacer una copia de seguridad o “backup” del equipo, que es una copia exacta del contenido en una imagen para poder recuperar los datos en caso de accidente informático.

Hacer la copia

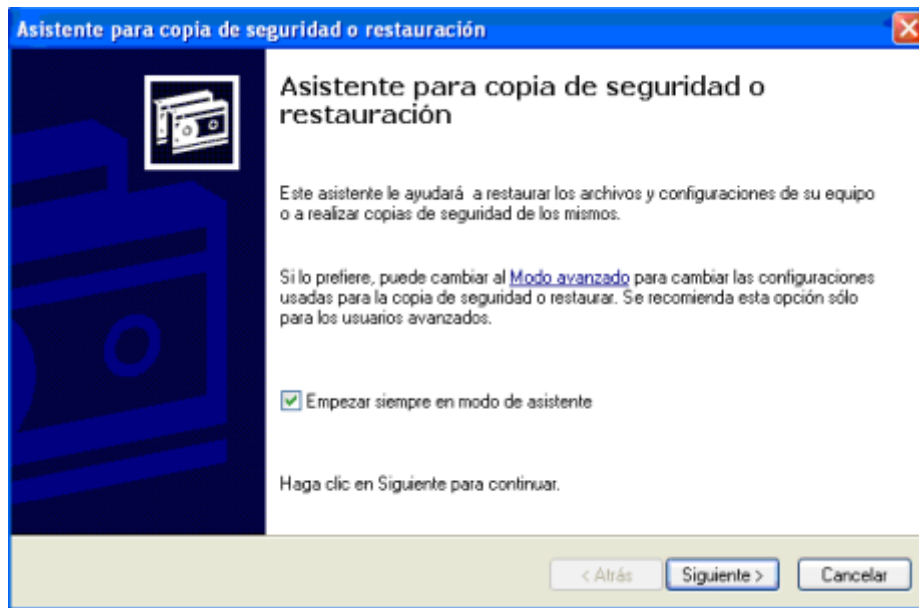
Ante todo se tiene que tener un disco duro a parte para hacer la copia de seguridad.



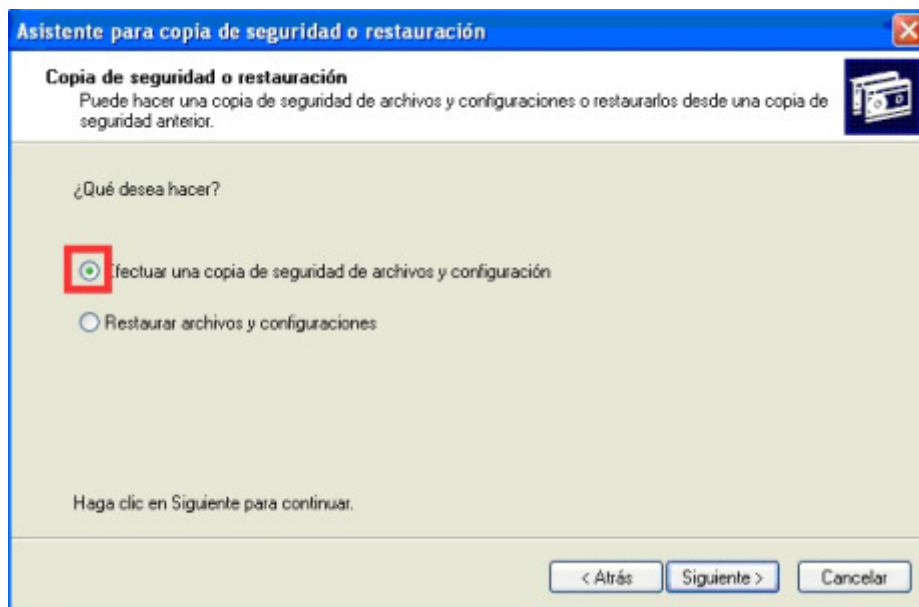
Se seleccionara el disco duro Origen (En este ejemplo se selecciono “XP (C:)”) con el botón derecho, y seleccionando **propiedades**, saldrán las propiedades del disco duro, donde sale el espacio libre en disco y lo que cabe, ir a la pestaña **Herramientas**, y como muestra en el dibujo, hay que ir a **Realizar copia de seguridad ahora...**



Ahora seguir los pasos que se indican, le damos a siguiente y comienza el asistente:

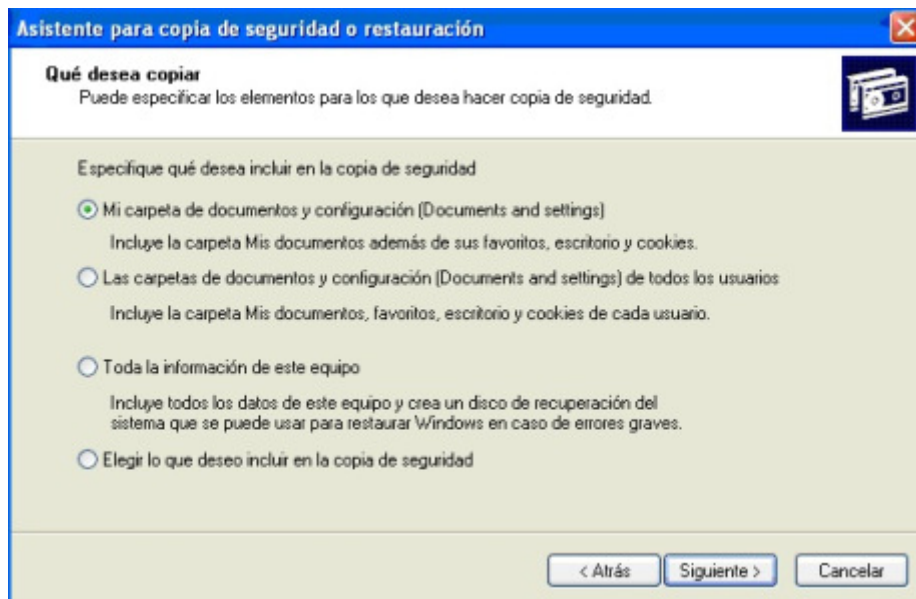


Seleccionar lo que se quiere hacer, si una copia de archivos y configuración o restaurarlo, lógicamente, en este caso se seleccionará la primera, la segunda opción será para cuando se tenga un desastre informático y se desee recuperar los datos.

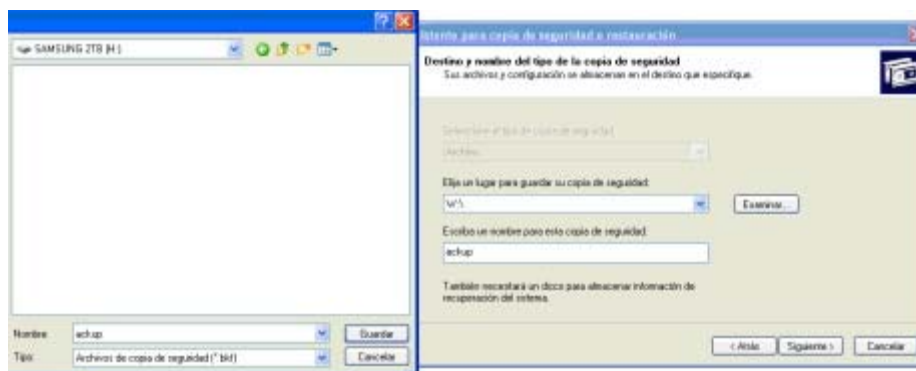


Elegir que se quiere copiar al disco aparte, la tercera opción va muy bien por ejemplo si se acaba de formatear el PC, ya que se tendrá una copia del disco en el estado actual, lo cual hace que si algún día se tiene un virus grave, restaurándolo, el PC vuelve a estar como el día que se hizo la copia de seguridad, aunque se puede seleccionar la opción que se quiera.

Si se tienen documentos importantes, se recomienda ir haciendo una copia de seguridad diaria o cada 2 días.



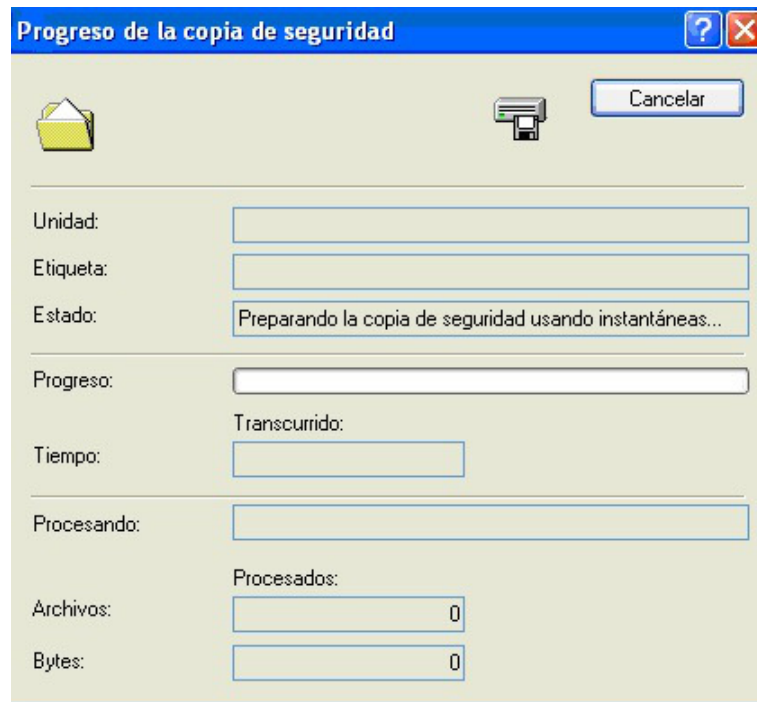
Seleccionar donde se quiere guardar y con que nombre, para ello pulsar a “**Examinar...**”, y se abrirá la ventana que se ve a la izquierda, ahí se buscara el disco duro externo, y se pulsará **Guardar**.



Pulsar el botón **Siguiente** y saldrá un resumen de lo que se va a ejecutar y si donde se pulsará **Finalizar** para comenzar el proceso:



Comenzará el proceso de la copia de seguridad, no hay que hacer nada, esperar unos minutos (dependiendo del tamaño del disco y velocidad del PC puede llegar a 1 hora o más, así que se puede seguir haciendo otras cosas), y como siempre paciencia la madre de la ciencia, las dos capturas siguientes son de lo que ocurrirá durante el proceso de copiado.



Progreso de la copia de seguridad

Unidad:

Etiqueta:

Estado: Preparando la copia de seguridad usando instantáneas...

Progreso:

Transcurrido:

Tiempo:


Procesando:

Procesados:

Archivos: 0

Bytes: 0

Cancelar



Progreso de la copia de seguridad

Unidad: C: XP

Etiqueta: BACKUP.bkf creado 03/03/2011 a las 19:53

Estado: Haciendo copia de seguridad de los archivos del equipo...

Progreso:

Transcurrido: 45 s. Restante estimado: 34 min., 57 s.

Tiempo:

Procesando: C:\...embles\Microsoft\Framework\v3.0\WindowsBase.dll

Procesados: 3.752 Estimados: 54.407

Archivos:

Bytes: 172.345.392 8.168.042.161

Cancelar

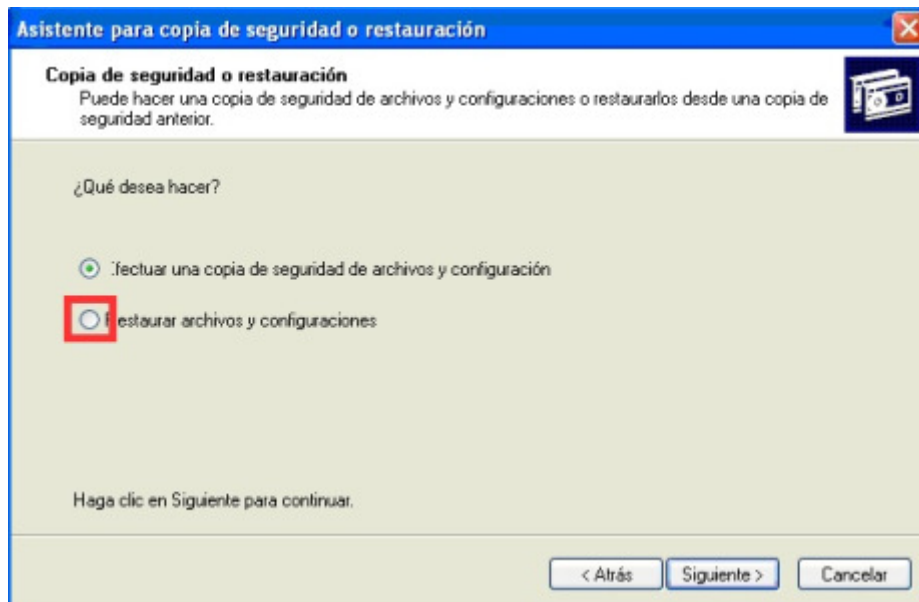
Si no hay un DVD vacío en la disquetera, saldrá este mensaje:



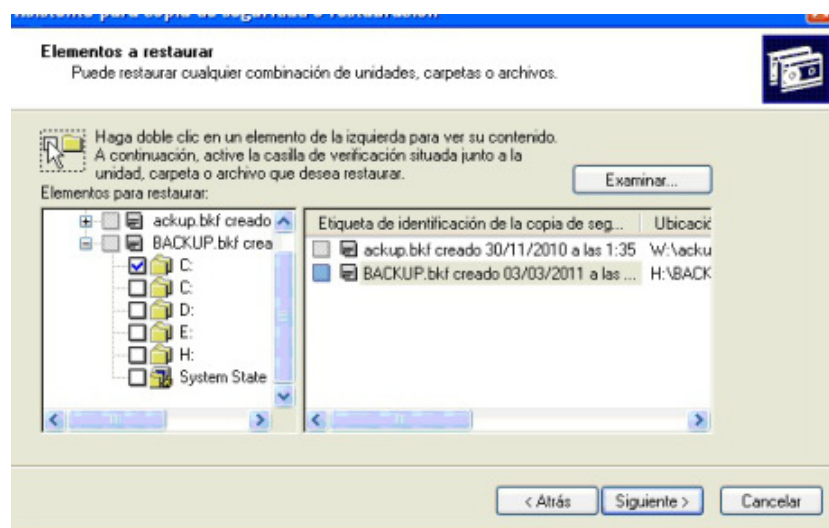
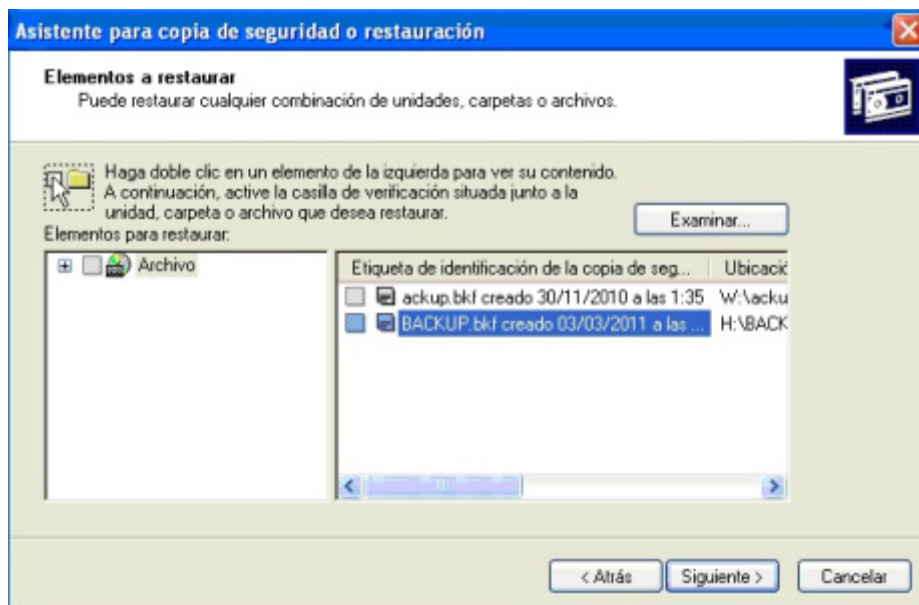
Restaurar la copia

Suponga que un virus ha dejado el Sistema Operativo dañado, en vez de formatear el disco duro, lo que haremos será restaurar el sistema, y volver a estar como en la última copia de seguridad. El proceso sería el siguiente:

Se tendrá que hacer como cuando se ha hecho la copia, **Mi PC, botón derecho > Propiedades**, ir a la pestaña **Herramientas** y seleccionar **“Realizar copia de seguridad ahora”** en el asistente le dar a **siguiente** e ir a parar en un punto que se ha mencionado antes, pero esta vez seleccionar **“Restaurar archivos y configuraciones”**.





Pulsar el botón **Siguiente**, y seleccionar la copia que se quiere recuperar (en este ejemplo hay dos, una del 30 de noviembre, y otra del 3 de marzo, por lo que se seleccionará la más reciente, y se recuperará la unidad C).




Pulsar el botón **Siguiente**, y después **Finalizar** para comenzar el proceso, entonces el PC se pondrá a restaurar:

Progreso de la restauración [?] [X]

Unidad:
Etiqueta:
Estado:

Progreso: 

Tiempo:

Transcurrido:	Restante estimado:
<input type="text" value="21 s."/>	<input type="text" value="2 min., 49 s."/>

Procesando:

Archivos:

Procesados:	Estimados:
<input type="text" value="0"/>	<input type="text" value="24.741"/>

Bytes:

<input type="text" value="8.832"/>	<input type="text" value="3.467.347.489"/>
------------------------------------	--

En pocos minutos se tendrá el PC restaurado y listo para volver a trabajar.

Bibliografía.

http://www.delitosinformaticos.info/consejos/sobre_seguridad_informatica.html

<http://recursostic.educacion.es/observatorio/web/ca/equipamiento-tecnologico/seguridad-y-mantenimiento>

http://www.inteco.es/Formacion/Amenazas/Vulnerabilidades/http://www.inteco.es/guias/educando_en_TI

<http://www.infoeme.com.ar/noticia.asp?id=8959>

<http://www.osi.es/es/protegete/protege-tu-ordenador>

<http://recursostic.educacion.es/observatorio/web/ca/equipamiento-tecnologico/seguridad-y-mantenimiento/707-keepass>

<http://www.informatica-hoy.com.ar/software-seguridad-virus-antivirus/Porque-instalar-un-antivirus.php>

<http://cajondesastres.wordpress.com/2007/06/12/proteger-datos-pendrive/>

<http://support.microsoft.com/kb/967715/es>