10 medidas básicas para la seguridad de la información

CSIRT-CV
Centre Seguretat TIC de la Comunitat Valenciana

GENERALITAT VALENCIANA

Unión Europea
Fondo Europeo de Desarrollo Regional
Una manera de hacer Europa

1 Utiliza un antivirus

Como todos sabemos, los antivirus sirven para detectar y eliminar virus informáticos. Instalar uno debe de ser la primera medida de seguridad que todos deberíamos hacer. Aunque la mayoría de antivirus analizan automáticamente cualquier fichero antes de abrirlo, es recomendable que los configuremos para que periódicamente analicen todo el equipo en busca de ficheros sospechosos. También deberemos asegurarnos de que periódicamente se actualice para detectar los nuevos virus que surgen cada día.

Existen multitud de antivirus en el mercado, por lo que para ayudar a decidir, hemos publicado una selección de los más conocidos.

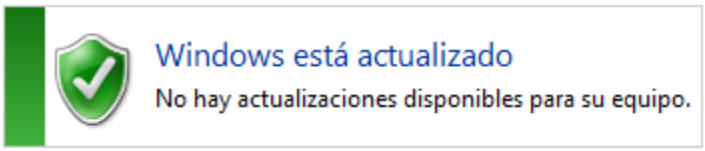
Recordemos que **un antivirus no ofrece una protección absoluta**, por lo que debe combinarse con el resto de medidas de seguridad de esta guía.

2. Actualiza el sistema

Cada día se descubren numerosos fallos y errores en aplicaciones informáticas, algunos de los cuales pueden poner en peligro la seguridad del sistema. Para corregirlos, los desarrolladores de los programas publican periódicamente actualizaciones o "parches de seguridad", los cuales arreglan los posibles puntos débiles descubiertos.

Algunas aplicaciones instalan estas actualizaciones automáticamente, pero de no hacerlo, debemos ser nosotros quien las busquemos manualmente. Generalmente las actualizaciones se encuentran en la sección de "*Ayuda*", o "*Acerca de*".

Las principales actualizaciones a las que debemos atender son las del propio sistema operativo, las del navegador y programa de correo electrónico, antivirus, y aplicaciones de terceros como Java, Adobe Reader, o Flash.



3. Utiliza solo software fiable

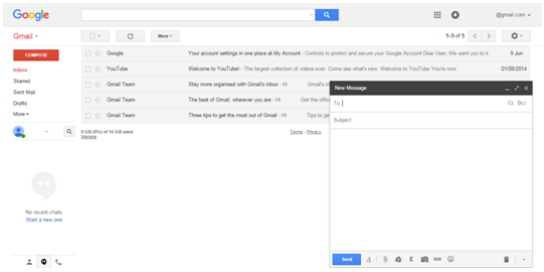
Cualquier programa que instalemos en nuestro equipo, debe venir de una fuente fiable. Generalmente las fuentes fiables son los propios CD o DVD originales, descargas desde la página web del fabricante, o incluso enlaces desde sitios web con buena reputación.

Debemos evitar a toda costa instalar software descargado de los conocidos como "sitios pirata", ya sean páginas web o programas de descarga, ya que no nos ofrecen ninguna garantía de que no han sido modificados para añadir virus o malware.

10 medidas básicas para la seguridad de la información

Evitaremos también el uso de software que, aunque sea gratis, prometa hacer cosas de dudosa legalidad, ya sea espiar a otros usuarios, “hackear wifis”, robar el usuarios de Facebook, etc, ya que es muy probable que se trate de una estafa y realmente estemos descargando un virus.

4. Evita estafas por correo electrónico



El correo electrónico sigue siendo una de las principales vías de infección de ordenadores así como la forma más habitual para intentar estafar a los internautas.

Nuestro sentido común será nuestro mejor aliado para evitar peligros al utilizar correo electrónico.

Desconfiemos de correos con ficheros adjuntos, especialmente si vienen de desconocidos, o si tenemos sospechas de que pueden ser fraudulentos.

¿Tiene sentido que un contacto con quien no hablamos en años nos envíe un correo con un fichero? ¿Y qué nos llegue una factura de alguien a quien no hemos comprado nada? ¿Un correo de un familiar escrito en otro idioma? Ante la duda, desconfiemos, y evidentemente nunca enviemos nuestras contraseñas ni datos personales sensibles aunque nos los soliciten.

Disponéis de una guía para ayudar a detectar este tipo de engaños en nuestra web.

5. Que las redes sociales no supongan un peligro

Las redes sociales son una gran herramienta para el ocio, y utilizarlas nunca debería suponer un peligro para nosotros ni los nuestros.

Debemos configurar las opciones de privacidad para adecuarla al uso que le vayamos a dar: si no vamos a publicar nada personal podemos dejar el perfil abierto, pero en caso contrario debemos tomar algunas medidas:

- No debemos aceptar a desconocidos
- Restringiremos la visibilidad solo a nuestros contactos
- No publicaremos fotos de otros sin su consentimiento, especialmente menores
- No demos información acerca de cuándo vamos a dejar nuestra casa vacía, por ejemplo en vacaciones
- No publicaremos datos personales o información que pueda revelar donde vivimos o la rutina que seguimos todos los días

10 medidas básicas para la seguridad de la información

CSIRT-CV
Centre Seguretat TIC de la Comunitat Valenciana

GENERALITAT VALENCIANA

Unión Europea
Fondo Europeo de Desarrollo Regional
Una manera de hacer Europa

6. Utiliza contraseñas seguras

Las contraseñas son la llave que protege nuestra información por lo que debemos utilizarlas adecuadamente. Elijamos siempre contraseñas fáciles de recordar, pero que contengan números, letras mayúsculas y minúsculas, caracteres especiales (¡!*$%&/) y de al menos 8 dígitos de longitud.

Estos son algunos ejemplos de contraseñas seguras y fáciles de recordar:

- Con3CafesSoyFeliz:)
- MeComo1YCuento20?
- 2Tostadas+1Cafe

Tampoco debemos utilizar la misma contraseña para todo, por lo que utilizar un gestor de contraseñas es muy recomendable.

7. Haz copias de seguridad

A pesar de que existen multitud de salvaguardas para proteger nuestra información, como último recurso siempre debemos tener copias de seguridad. Tengamos en cuenta que las copias no solo protegen contra virus y robos de información, sino que también nos ayudarán en caso de que el equipo se rompa, pierda, lo roben o incluso cuando seamos nosotros mismos quienes borremos información accidentalmente.

Existen muchos programas para hacer copias de seguridad aunque, según las necesidades de cada uno, puede bastar con hacer una copia periódica en un USB o disco duro externo (nunca en el propio equipo).

8. Utiliza solo equipos y redes seguras, especialmente Wifi

Al navegar por Internet, la seguridad de la red a la que nos conectemos, ya sea mediante un cable o por Wifi, es tan importante como la seguridad de nuestro propio equipo.

Configuremos **la red Wifi de casa** para que sea segura: debemos cambiar el nombre de la red y la contraseña que trae por defecto, debemos utilizar una contraseña segura, cambiarla periódicamente, y utilizar cifrado WPA2.

Al viajar o salir de casa, si no es imprescindible evitemos conectarnos a redes de hoteles, aeropuertos o restaurantes, especialmente si son Wifi y no tienen contraseña, ya que cualquiera que esté cerca podría interceptar nuestra información o incluso atacar nuestro dispositivo.

Por último, evitemos a toda costa **introducir nuestras contraseñas en equipos públicos** como pueden ser de bibliotecas, locutorios o centros de estudio, ya que pueden haber sido infectados y comprometer nuestras contraseñas.

10 medidas básicas para la seguridad de la información

CSIRT-CV
Centre Seguretat TIC de la Comunitat Valenciana

GENERALITAT VALENCIANA

Unión Europea
Fondo Europeo de Desarrollo Regional
Una manera de hacer Europa

9. Tu móvil es un pequeño ordenador: protégelo

Cada vez utilizamos más el móvil o tablet como sustituto del ordenador tradicional, por lo que debemos protegerlo como si de un ordenador se tratase:

- Hagamos copias de seguridad.
- Pongámosle una contraseña o patrón de acceso
- Manténganos actualizado el sistema y las aplicaciones
- No instalemos nada que provenga de fuentes no fiables
- Atentos a estafas o aplicaciones que prometan funcionalidades sospechosas
- Utilicemos solo redes seguras

10. Ayuda a otros a protegerse

La velocidad a la que la tecnología se ha extendido en nuestra vida cotidiana ha hecho que no todo el mundo sea consciente de los riesgos que suponen algunas malas prácticas, las cuales entrañan riesgos reales para nuestra información, vida social, amistades o trabajo.

Es deber de todos fomentar el buen uso de la tecnología, ya sea ayudando a los demás a configurar de forma segura sus nuevos dispositivos, enseñándoles buenas prácticas, o corrigiéndoles gentilmente cuando cometan errores.

Seamos especialmente pacientes con personas mayores que no acaban de entender cómo funcionan las cosas, pongamos freno a las ansias de los más pequeños a la hora de probarlo todo, y no dudemos en corregir a amigos y familiares en grupos de WhatsApp o publicaciones de Facebook cuando compartan cadenas, publiquen falsas alarmas, o suban contenido que debería ser privado.

Datos de contacto

CSIRT-CV Centro de Seguridad TIC de la Comunitat Valenciana

http://www.csirtcv.gva.es/

https://www.facebook.com/csirtcv

https://twitter.com/csirtcv

Licencia de uso