SOFTWARE BÁSICO DE SEGURIDAD

10 ideas para estar mas seguro

SERVICIOS INFORMÁTICOS UCM

1 TU SISTEMA OPERATIVO ACTUALIZADO

Los sistemas operativos sufren pequeños cambios y ofrecen fantásticas herramientas como Windows update que permiten tener el equipo actualizado de forma automática.

Así disfrutarás de todas las novedades que se integran en el sistema operativo y corregirás las vulnerabilidades usadas por los virus para propagar el software malicioso.

2 UTILIZA ANTIVIRUS Y APLICACIONES ANTI-MALWARE

Un antivirus es imprescindible para tener un mínimo de seguridad.
En la UCM se utiliza SEP (Symantec Endpoint Protection)como antivirus corporativo. Fuera de la UCM dispones de antivirus gratuitos y de pago.

Es recomendable que utilices programas para localizar malware como "Spybot Search and Destroy" y "MalwareBytes"que buscarán y eliminarán sw malintencionado

3 UTILIZA SW DE CREACIÓN DE CONTRASEÑAS SEGURAS

La misma contraseña de años para todos los servicios a los que estás suscrito es realmente un riesgo, pues si te descubren una; descubren todo.

Olvidate de "recordar contraseña" en sitios públicos y usa un sw de gestión y creación de contraseñas seguras. La mayor parte de las intrusiones se producen por una contraseña fácil de adivinar.
Por ejemplo keepass es una opción gratuita multiplataforma.

4 ACTIVA EL FIREWALL DE TU SISTEMA

Todos los Sistemas Operativos actuales incorporan firewalls que te permiten seleccionar qué trafico dejarás que entre en tu equipo, previniendo cierto tipos de arranque de red.

Conviene utilizarlo y activarlo en una configuración lo más cerrada posible para evitar accesos no deseados a tu equipo.

Y SI NECESITAS AYUDA PARA ESTAR MAS SEGURO
CUENTA CON NOSOTROS

913944774 CENTRO DE ATENCIÓN A USUARIOS
HTTPS://HELPME.UCM.ES

Si quieres más accede a https://ssii.ucm.es

UTILIZA SW PARA EVITAR EL RAMSOMWARE

5

El Ramsomware es una de las amenazas que más impacto tiene al encriptar tus datos y ficheros personales para después pedirte un rescate.

Esto ocurrió con el conocido virus Wannacry.

Usa sw que previene el cifrado de los datos como Ransomfree que evita en tiempo real esta amenaza, de tal forma que aunque el ordenador sufra una infección por uno de estos virus se evitará el encriptado de los datos.

UTILIZA TECNOLOGÍAS SEGURAS Y SOFTWARE DE NAVEGACIÓN QUE PERMITA PRIVACIDAD

6

Hay navegadores, como Firefox, que te permiten, usando la modalidad de navegación privada, que un tercero no pueda explotar, contra ti, la información de tu navegación por internet.
Conviene, además, configurarla elimininación de datos de tus sesiones de navegación.
Si utilizas conexiones https, de esta forma tu tráfico estará cifrado y tu privacidad protegida.

UTILIZA SOFTWARE DE COPIAS DE SEGURIDAD

7

En el caso de darse una situación donde pierdes datos por falta de políticas de seguridad en tu ordenador, lo único que te salvará es haber realizado una copia de seguridad de los datos.

Los Sistemas Operativos suelen tener integrados software de backup automáticos. Además, hay un montón de programas gratuitos que te permitirán hacer todo tipo de backups a tu medida.

UTILIZA SOFTWARE VPN

8

Tener y utilizar un software VPN (redes privadas virtuales) te permite establecer conexiones seguras y cifradas con las instituciones con las que trabajas. De esta forma todo el trabajo remoto que realices quedará cifrado y evitarás que un tercero pueda verlo.

También, puedes contratar los servicios de un proveedor VPN externo de terceros para que toda tu navegación esté cifrada (no sólo el tráfico remoto hacia la red de la institución donde trabajas), teniendo en este caso una total privacidad.

HERRAMIENTAS DE CIFRADO DE USB Y DISPOSITIVOS EXTRAÍBLES

9

Es conveniente que tus sistemas de almacenamiento extraíbles como discos duros o memoria USB, estén cifrados con un software específico de cifrado.

Así, en caso de que caigan en manos de un tercero, no puedan acceder a su contenido. Una opción multiplataforma de código abierto y gratuita puede ser veracrypt.

DESINSTALA TODO EL SW QUE NO UTILICES Y EVITA INSTALAR SW PIRATA

10

Tener un ordenador sólo con el software que utilizamos minimiza las probabilidades de tener problemas, ya que el software no usado no se actualiza y acaba siendo fuente de vulnerabilidades y problemas.