

SEGURIDAD

PROTEGE TUS DISPOSITIVOS

Medidas para reforzar la protección del ordenador, móvil/tablet.

Ordenador

- Periódicamente instala actualizaciones para todos los programas que utilices. Desde los sistemas operativos, como son Windows, Mac OS, Linux... además de mantener actualizados también los programas antivirus y antiespía y los navegadores de internet como son Internet Explorer, Google Chrome, Mozilla Firefox, Safari, Opera, etc.
- Nunca utilices programas, servicios ni navegues por sitios de internet que no sean conocidos y de confianza.
- Ten cuidado al descargar ficheros o abrir documentos adjuntos en correos electrónicos y en hacer clic en vínculos que contengan dichos correos, aunque su origen parezca conocido, no los abras si no estás totalmente seguro de su procedencia o confírmalo con el remitente antes de abrirlo.
- Desactiva las opciones de guardar contraseñas y autocompletar que disponen los navegadores de internet.
- Evita aceptar advertencias o ventanas emergentes inesperadas de sitios web que no sean de confianza.
- No conectes unidades flash (memorias USB) desconocidas en tu ordenador para evitar el posible contagio de virus o malware.
- Protege tus datos personales, de contacto y financieras. Las contraseñas más seguras incluyen una combinación de letras, números y símbolos.
- No utilices la misma contraseña en todos los sitios. Si te la roban, quedaría en peligro toda la información que esta protege.
- No compartas las contraseñas con nadie.
- No dejes desatendido el ordenador mientras se sigue conectado.
- Cuando se utilicen ordenadores compartidos con terceras personas, cerrar siempre las sesiones y eliminar la memoria cache de los navegadores de internet.
- No facilites datos en sitios web que no dispongan de un certificado de sitio web seguro (SSL) o que no tengan su identidad verificada (símbolo de un candado en el navegador).
- No guardes las copias de seguridad en el mismo lugar donde tengamos el ordenador.

Móvil y tablet

Además de tener en cuenta algunas de las medidas de protección que hemos mencionado anteriormente para tu ordenador, también serían aplicables las siguientes medidas más específicas para tus dispositivos móviles:

- Procura instalar aplicaciones conocidas desde las tiendas oficiales o "markets" correspondientes al sistema operativo de tu dispositivo (Google Play, App Store...). Son tiendas que se revisan continuamente por lo que es más difícil que haya programas dañinos. Es aconsejable también, leer los comentarios que la gente hace acerca de esas aplicaciones en las propias tiendas, así nos aseguramos que es la aplicación que buscamos.

- Instala un antivirus para tu móvil o tableta.
- Utiliza un código o un patrón gestual para bloquear el móvil cuando no lo utilices.
- No almacenes información comprometida en el móvil, por ejemplo, guardar números de PIN y contraseñas en el móvil no son prácticas seguras.
- No respondas a mensajes de texto SMS que te pidan información financiera desde el móvil.
- Activa la función de borrado remoto en el teléfono por si se te pierde el teléfono o te lo roban. Algunos móviles de Android, iPhone o Windows Phone disponen de funciones que facilitan la localización del móvil en caso de pérdida y la posibilidad de borrar o bloquear su contenido si fuera necesario de forma remota.
- Mantén las aplicaciones y el sistema operativo del teléfono actualizados y al día.
- De forma periódica, realiza copias de seguridad del contenido de tu móvil o tableta, contactos, calendarios, programas, etc.
- Cierra las sesiones, una vez que termines de utilizar las aplicaciones.
- Utiliza preferiblemente las redes móviles (3G y 4G) o redes WiFi que no sean de acceso público y no dejes tu dispositivo con el WiFi ni el Bluetooth activado continuamente.

