Normas de uso del PC

Laboratorio de Seguridad de la Información

El acceso a aplicaciones e información es cada vez más sencillo de realizar casi desde cualquier tipo de dispositivo. Los usuarios están ya muy familiarizados con el hecho de poder acceder a sus aplicaciones en cualquier momento y en cualquier sitio, y esto lleva a descuidar la seguridad.

En el uso del PC podemos hacer distinción en dos ámbitos, en el que el PC es público o compartido con otros y en el que es dedicado para el usuario o personal.

En el ámbito de **PC público**, debemos ser muy conscientes de que su uso puede suponer grandes riesgos, debido a que no se dispone del conocimiento de cómo ni por quién fue empleado anteriormente, de si tiene medidas y herramientas de seguridad aplicadas o si está libre de virus. El usuario no tiene control en estos equipos.

Este contexto de PCs públicos se debe evitar. Pero si se utiliza, seguir al menos a las siguientes recomendaciones:

- No realizar transacciones bancarias ni compras.
- No ejecutar ni abrir archivos presentes en el PC del que no somos propietarios.
- No dejar ficheros ni información en el PC al finalizar su uso. Borrarlos.
- No dejar solo el ordenador con información confidencial o privada en la pantalla.
- No dejar que el navegador guarde credenciales de acceso cuando lo pregunte.
- Cerrar la sesión de todas las aplicaciones que se utilicen al terminar.

En el ámbito de **PC privado**, aún disponiendo del control para establecer las medidas de seguridad que se consideren necesarias, no exime de la existencia de riesgos. Algunos de estos son:

- Robo de información y/o recursos del PC
- Posibilidad de pérdida de información por borrado o cifrado de datos que impida el acceso a estos.
- Secuestro o suplantación de identidad.

Cómo hacer un uso seguro del PC:

Instalación de software:

- No descargar ni instalar software de fuentes no fiables.

Perfil de usuario:

- No utilizar el usuario Administrador. Utilizar usuarios sin excesos de permisos.

Conectividad con redes no confiables:

- Contar con aplicaciones de antivirus actualizadas.
- Su uso debe ser excepcional y se debe evitar lo máximo posible el acceso a aplicaciones o servicios con información, personal, confidencial o privada.
- Emplear comunicaciones seguras (canales SSL o accesos por VPN).

Ejecución de archivos:

- No abrir ni ejecutar ficheros ni url de dudosa procedencia y de títulos llamativos. Suelen ser un gancho.

Actualización:

- Mantener siempre actualizados los sistemas.

Servicios no seguros:

- Deshabilitar o desinstalar aquellos servicios o aplicaciones que no se necesiten: concepto de mínima superficie de exposición.

"NO SE CONFÍE. SEA CAUTO Y PROTÉJASE"

XUNTA DE GALICIA
CONSELLERÍA DE SANIDADE

SERVIZO GALEGO de SAÚDE

MINISTERIO DE ECONOMÍA Y COMPETITIVIDAD

UNIÓN EUROPEA
Fondo Europeo de Desarrollo Regional
Una manera de hacer Europa