



O acceso a aplicacións e información é cada vez máis sinxelo de realizar case dende calquera tipo de dispositivo. Os usuarios están xa moi familiarizados co feito de poder acceder as súas aplicacións en calquera momento e en calquera lugar, e isto leva a descoidar a seguridade.

No uso do PC podemos facer distinción en dous ámbitos, no que o PC é público ou compartido con outros e no que é dedicado para o usuario ou persoal.

No ámbito de **PC público**, debemos ser moi conscientes de que o seu uso pode supoñer grandes riscos, debido a que non se dispón do coñecemento de como ni por quen foi empregado anteriormente, de se ten medidas e ferramentas de seguridade aplicadas ou se está libre de virus. O usuario non ten control nestes equipos.

Este contexto de PCs públicos débese evitar. Pero se se emprega, seguir polo menos as seguintes recomendacións:

- Non realizar transaccións bancarias nin compras.
- No executar nin abrir arquivos presentes no PC do que non somos propietarios.
- Non deixar ficheiros nin información no PC ó finalizar o seu uso. Borralos.
- Non deixar só o ordenador con información confidencial ou privada na pantalla.
- Non deixar que o navegador garde credenciais de acceso cando o pregunte.
- Cerrar a sesión de todas as aplicacións que se empreguen ó finalizar.

No ámbito de **PC privado**, aínda dispoñendo do control para establecer as medidas de seguridade que se consideren necesarias, non exime da existencia de riscos. Algúns destes son:

- Roubo de información e/ou recursos do PC.
- Posibilidade de perda de información por borrado ou cifrado de datos que impida o acceso a estes.
- Secuestro ou suplantación de identidade.

Como facer un uso seguro do PC:

Instalación de software:

- Non descargar nin instalar software de fontes non fiables.

Perfil de usuario:

- Non empregar o usuario Administrador. Usar usuarios sen excesos de permisos.

Conectividade con redes non confiables:

- Contar con aplicacións de antivirus actualizadas.
- O seu uso debe ser excepcional e débese evitar o máximo posible o acceso a aplicacións ou servizos con información, persoal, confidencial ou privada.
- Empregar comunicacións seguras (canles SSL ou accesos por VPN).

Execución de arquivos:

- Non abrir nin executar ficheiros nin url de dubidosa procedencia e de títulos chamativos. Soen ser un gancho.

Actualización:

- Manter sempre actualizados os sistemas.

Servizos non seguros:

- Deshabilitar ou desinstalar aqueles servizos ou aplicacións que non se precisen: concepto de mínima superficie de exposición.

“NON SE CONFÍE. SEXA CAUTO E PROTÉXASE”

