RECOMENDACIÓNS DE SEGURIDADE INFORMÁTICA NO TELETRABALLO PARA O PERSOAL DA UNIVERSIDADE DA CORUÑA

Cando se traballe desde un ordenador que non estea xestionado polo Servizo de Informática e Comunicacións (SIC), como é o caso dos ordenadores que poidamos ter no noso domicilio, cómpre ter en conta unha serie de medidas de seguridade específicas para **minimizar os riscos de sufrir un incidente de seguridade**, como perdas de datos ou o roubo do noso contrasinal.

Ademais das seguintes recomendacións é importante coñecer a normativa específica que a UDC aprobou para o uso dos servizos de acceso remoto, que pode consultarse en Regulamento xeral e normativa de uso dos recursos TIC.

1. Configuración segura do ordenador persoal

O ordenador desde o que traballemos debe cumprir as seguintes medidas de seguridade:

- Ter o sistema operativo actualizado, aplicando sempre os parches de seguridade que se publiquen.
- Contar cun antivirus actualizado.
- Ter actualizadas as aplicación. Son de especial relevancia, por ser fonte habitual de incidentes de seguridade:
    - Navegadores web,
    - Java,
    - Adobe Flash.

Debe evitarse traballar desde un ordenador que non cumpra estes requisitos e, especialmente, en ordenadores de uso público.

2. Separación do contornos persoal e profesional

Deben seguirse estas medidas de seguridade orientadas a non mesturar a información persoal coa profesional.

- Non se deben memorizar as nosas credenciais (identificador de usuario e contrasinal), no navegador, cando accedamos a servizos TIC ou aplicacións da UDC.
- É aconsellable almacenar a información do ámbito profesional nos recursos que a UDC pon á nosa disposición, como os espazos de almacenamento en Office365 ou as unidades en rede accesibles desde o terminal VDI.
- Na medida do posible, limitarase a descarga de información no disco duro do ordenador persoal, eliminándoa cando deixe de ser necesaria.
- É aconsellable bloquear o equipo cando estea desatendido.
- Unha vez finalizada a sesión de teletraballo deberá realizarse unha desconexión dos servizos que se utilizaran: Office365, Escritorio virtual (VDI), acceso remoto seguro (VPN-SSL), etc.

3. Permanecer alerta ante posibles enganos

É probable que os ciberdelincuentes aproveiten para difundir mensaxes falsos relacionados coa COVID-19, ou outras cuestións de actualidade, coa intención de infectar equipos, roubar contrasinais ou cometer estafas.

Cómpre permanecer alerta e seguir as recomendacións xerais fronte este tipo de accións:

- Non abra arquivos anexos nin prema en ligazóns de remitentes descoñecidos ou de mensaxes non esperados. En caso de dúbida, se coñece o remitente, contacte con el para verificar a lexitimidade da mensaxe.
- Se ten dúbida sobre a procedencia dunha ligazón incluída nunha mensaxe de correo, en lugar de premer nel, abra o navegador e teclee directamente o enderezo do provedor.
- Mantéñase alerta sobre as mensaxes fraudulentas que empregan os ciberdelincuentes para apropiarse dos nosos datos persoais, suplantar a nosa identidade ou mesmo cometer fraudes económicos.
- Non publique o seu enderezo de correo electrónico corporativo nas redes sociais, foros ou sitios web públicos. Se evitamos a súa publicidade, dificultaremos que aos ciberdelincuentes intenten enviarnos correos fraudulentos.
- Peche sempre a sesión de correo electrónico cando termine de traballar con ela.
- Nunca facilite os seus datos persoais por correo electrónico ou a través de formularios dos que dubide da súa lexitimidade.

Pode atopar máis consellos relacionados coa ciberseguridade na web corporativa de Seguridade da Información: https://udc.es/gl/seguridade-da-informacion/consellos/