



Cápsulas tecnológicas



Cuidado con los ataques de Phishing

- Verifique que dispone de un software antivirus, debidamente instalado y funcionando en el equipo.
- Cerrar las secciones VPN establecidas con la institución cuando no necesite estar conectado a un recurso de la Universidad.
- Bloquear la computadora cada vez que sea dejada desatendida, aunque se encuentre en su casa.
- Cerrar las secciones de todas las aplicaciones y escritorios remotos cuando no estén en uso.
- No abrir ningún enlace sospechoso (sea por medio de correo electrónico o vía una página Web).
- Evitar instalar aplicaciones sospechosas o de fuentes no creíbles.
- Evitar el envío de información sensible (confidencial) de la Institución por medio de canales no oficiales (WhatsApp, Telegram, etc.). La Universidad utiliza WhatsApp Business en la gestión de servicios al usuario.
- Utilice el correo institucional si tiene que compartir información confidencial.