

Recomendaciones



Equipo corporativo

- **Sigue las directrices de tu organización** y utiliza tu equipo únicamente para tareas relacionadas con tu actividad profesional.
- Utiliza **contraseñas robustas** y **no las compartas**.
- Manténlo **actualizado**.
- Procura **no dejarlo desatendido** y en ese caso bloquéalo.
- Ten **cuidado con los dispositivos** que conectas.



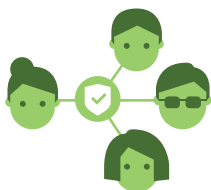
Correo electrónico

- **Sé precavido** con los correos. Desconfía si solicitan datos personales.
- **Revisa la dirección** del remitente para confirmar que es quien dice ser.
- Antes de acceder a un enlace **fíjate en la dirección** a la que apunta.
- **Desconfía** si el correo insta a tomar una decisión urgente.
- **No ejecutes ficheros** adjuntos de remitentes desconocidos.



Dispositivos Móviles

- Protege tu dispositivo móvil configurando una pantalla de bloqueo y utilizando una **contraseña, un pin o biometría** para desbloquearla.
- **Mantén actualizado** el dispositivo y realiza copias de seguridad periódicamente.
- **No utilices** redes **Wifi públicas**.
- **Deshabilita funcionalidades** como Wifi y Bluetooth cuando no las utilices.
- Instala únicamente aquellas aplicaciones que vayas a utilizar y **siempre de fuentes oficiales**.



Redes Sociales

- Utiliza contraseñas robustas y habilita la **verificación en 2 pasos**.
- **No utilices las mismas contraseñas** en tu entorno corporativo y personal.
- Configura adecuadamente las **opciones de privacidad**.
- Antes de publicar **valora las consecuencias** de dicha publicación.



Compartir información

- Utiliza únicamente los **medios establecidos por tu organización** para compartir la información. No utilices servicios como Wetransfer, Dropbox, Mega, Drive, etc.
- **No abandones documentos** en impresoras o escáneres.

La ciberseguridad es responsabilidad de todos