

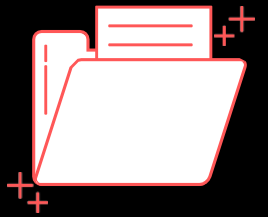
PROTÉGETE CONTRA LA INGENIERÍA SOCIAL

No te fíes de mensajes:

- Emitidos por direcciones desconocidas o sospechosas.
- No esperados.
- Redactados con fallos ortográficos y saludos impersonales.
- Que pidan actuar con urgencia, en secreto o a cambio de un beneficio.



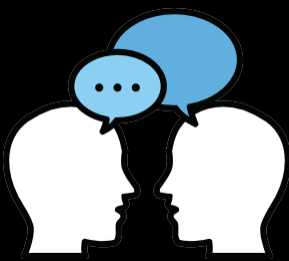
No accedas o descargues archivos adjuntos en emails o **mensajes sospechosos o inesperados.**



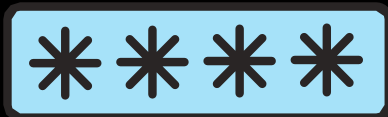
Instala un antivirus en cualquier equipo que utilices, incluyendo teléfonos móviles.



Contacta por medios alternativos al emisor de un mensaje sospechoso, para **comprobar su legitimidad.**



No remitas credenciales, datos personales o económicos en emails, mensajes o llamadas sospechosos o inesperados.



No accedas a enlaces adjuntos en emails o mensajes. Si necesitas acceder, **escribe la dirección del enlace en un buscador de Internet.** Vigila que comience con los dígitos **https://** y que se muestre en el buscador junto a un candado.



No introduzcas en tus equipos dispositivos de memoria extraíble cuya procedencia y contenido no conozcas de forma **segura.**



No permitas el acceso a tu oficina o edificio a personas cuya autorización para acceder no conozcas o no puedas comprobar.

