



1

Identificación de correos electrónicos fraudulentos (phishing):



Los correos phishing **son mensajes falsos** que buscan obtener información confidencial de los destinatarios. Es importante que los usuarios detecten señales como errores de ortografía o **direcciones de correo electrónico sospechosas**.

2

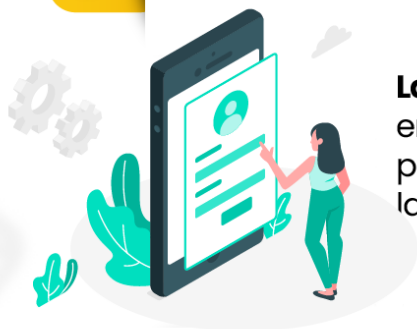
Uso de correos electrónicos corporativos seguros:



Se recomienda el **uso de correos electrónicos corporativos** proporcionados por la organización en lugar de correos personales. Esto asegura el cumplimiento de las políticas de seguridad.

3

Capacitación y concienciación usuario:



La **capacitación sobre seguridad** en el correo electrónico es esencial para educar a los usuarios sobre las **mejores prácticas de seguridad**.

4

Uso de contraseñas seguras:



Los correos electrónicos pueden contener **enlaces o archivos adjuntos peligrosos** que pueden comprometer la seguridad de los datos si se hace clic en ellos. Es importante usar **contraseñas fuertes y únicas**.



Secretaría
de las Tic