8. Consejos básicos

1. REMITENTE

¿Esperabas un email de esta persona/ entidad?

Comprueba que el email coincida con la persona o entidad remitente que dice ser o está suplantando a alguien.

2. ASUNTO

¿Capta tu atención el asunto del correo?

La mayoría de correos fraudulentos utilizan asuntos llamativos e impactantes para captar tu atención. Ten en cuenta esta consideración.

6. ADJUNTOS

¿Contiene un archivo adjunto que no estabas esperando o es sospechoso?

Analiza los adjuntos antes de abrirlos, puede tratarse de un malware. Los archivos y analizadores de ficheros te ayudarán a identificar si están infectados.

5. ENLACES

¿Los enlaces llevan a una página legítima?

Sitúa el cursor encima del enlace, o mantén presionado el enlace en dispositivos móviles, podrás ver la URL real a la que dirige. Si no coincide o es una web sin certificado de seguridad (https://) no hagas clic.

3. OBJETIVO DEL MENSAJE

¿Cuál es el objetivo del mensaje?

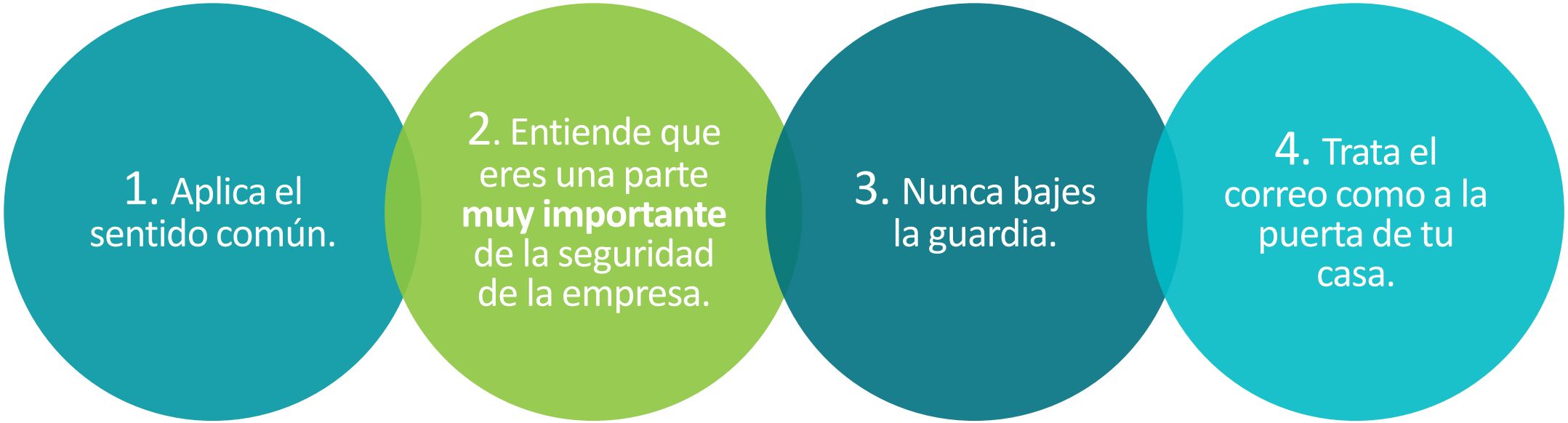
Una entidad de servicios como banco, suministros del hogar (agua, gas) u otros nunca te pedirá tus datos personales por correo. Además si es de carácter urgente, amenazante o con ofertas y promociones muy atractivas, es muy posible que sea un fraude.

4. REDACCIÓN

¿Tiene errores ortográficos o parece una mala traducción de otro idioma?

Revisa la redacción en busca de errores de ortografía o gramaticales. Además, si no está personalizado o parece una traducción automática sospecha.

Consejos básicos



Digital Security

Progress. Protected.