

EMPLEADOS

# Uso del correo electrónico

básico



## Normativa de uso de correo electrónico.

Dispones de una normativa referente al uso del correo electrónico que el empleado aceptará al incorporarse a su puesto de trabajo.



## Antimalware y antispam.

Instalas y activas aplicaciones antimalware y filtros antispam tanto en el servidor como en los clientes de correo.



## Ofuscar las direcciones de correo electrónico.

No publicas las direcciones de correo corporativas en páginas web ni en redes sociales sin utilizar técnicas de ofuscación.



## Uso apropiado del correo corporativo.

Nunca usas el correo corporativo con fines personales y el contenido cumple las normas marcadas por la empresa.



## Contraseña segura.

Usas una contraseña segura para acceder al correo electrónico.



## Correos sospechosos.

Sospechas de la autenticidad del correo cuando el mensaje: presenta cambios de aspecto, contiene una «llamada a la acción» que nos urge, invita o solicita hacer algo no habitual o solicita credenciales de acceso a una web o aplicación (cuenta bancaria, ERP, etc.).



## Identificación del remitente.

Identificas los remitentes antes de abrir un correo electrónico. Si sospechas que ha sido suplantado contactas con el remitente por otro medio para confirmarlo.



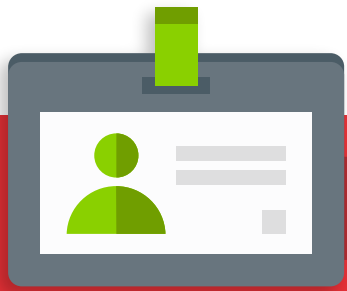
## Análisis de adjuntos.

Analizas cuidadosamente los adjuntos de correos de remitentes desconocidos antes de abrirlos. Si sospechas de su autenticidad, no lo descargas ni lo abres.



## Inspección de enlaces.

Examinas atentamente los enlaces incluidos en los correos antes de acceder a ellos.



EMPLEADOS

# Uso del correo electrónico

básico



**No responder al spam (correo basura).**

Nunca respondes al correo basura. Lo agregas a la lista de spam y lo eliminas.



**Utilizar la copia oculta (BCC o CCO).**

Utilizas la copia oculta cuando envías correos a múltiples direcciones.



**Reenvío de correos.**

En caso de necesitar el reenvío de algún correo corporativo a una cuenta personal lo solicitas previamente a la dirección.



**Evitar las redes públicas.**

No consultas el correo corporativo si estás conectado a redes públicas como wifis de hoteles o aeropuertos.

avanzado



**Cifrado y firma digital.**

Instalas una tecnología de cifrado y firma digital que se pueda usar con el correo electrónico para proteger la información confidencial y asegurar la autenticidad de la empresa como remitente.



**Desactivar el formato HTML, la ejecución de macros y la descarga de imágenes en los clientes de correo electrónico.**

Desactivas el formato HTML, la ejecución de macros y la descarga de imágenes para una protección adicional de las cuentas de correo electrónico.