

EMPLEADOS USO DEL CORREO ELECTRÓNICO



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. Importante mantenerlas actualizadas.



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.



Uso adecuado y racional.

Utilizas el correo electrónico corporativo solo para uso profesional, cumpliendo las reglas de buena fe y diligencia.



Cadenas de mensajes.

Evitas contestar a cadenas de mensajes innecesarias evitando la propagación de correo spam o malicioso.



Evitar usos indebidos.

Usas el correo electrónico de manera exclusiva para el ámbito profesional y no haces difusión de material ofensivo o ilegal.



Prestar atención al lenguaje empleado.

Haces uso de lenguaje riguroso, exento de faltas de ortografía.



Vigilar la inscripción en sitios web.

No utilizas el correo electrónico corporativo para registros en páginas web poco confiables o sospechosas.



Contraseña segura.

Usas una contraseña robusta para acceder al correo electrónico.

BÁSICO

EMPLEADOS USO DEL 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 tienes dudas o 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 abres ni lo descargas.



Inspección de enlaces.

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



No responder al spam (correo basura).

Nunca respondes al correo basura. Lo agregas a la lista de *spam* o correo no deseado y lo eliminas.



Utilizar la copia oculta (BCC o CCO).

Utilizas la copia oculta cuando envías correos a múltiples direcciones.



Evitar las redes públicas.

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



Reenvío de correos.

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



Acceso a correo electrónico a través de teléfonos móviles corporativos.

No accedes al correo corporativo desde teléfonos móviles que no estén aprobados y configurados por la empresa.

BÁSICO

EMPLEADOS USO DEL CORREO ELECTRÓNICO



BÁSICO



Acceso a correo electrónico a través de clientes web.

No accedes al correo corporativo a través de clientes web desde equipos públicos o compartidos.



Almacenamiento y eliminación del correo electrónico.

Evitas la acumulación innecesaria y no almacenas correos electrónicos corporativos indefinidamente.

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 gestores 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.