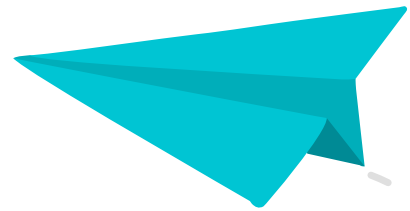
GUÍA DE USO DEL CORREO ELECTRÓNICO

netkia

pitma GRUPO



En las últimas semanas se están produciendo **ataques masivos a través del correo electrónico** que ponen en peligro la confidencialidad, integridad y disponibilidad de la información de la empresa, por eso os pedimos que antes de abrir un archivo adjunto o pinchar en un enlace os toméis un par de minutos para analizar el mensaje.

Hasta hace unas semanas la mayor parte de estas campañas simulaban venir de grandes empresas, ahora también **están llegando campañas de nuestros contactos de correo habituales**, y es importante aprender a diferenciar correctamente estos correos

Para ayudaros en esta tarea hemos preparado una pequeña guía que esperamos os sea de utilidad tanto **para la gestión del correo profesional** como el personal.

Si una vez analizado el mensaje aún tienes dudas de su autenticidad lo mejor es dejarlo aparcado y **preguntar al equipo de Netkia**, están ahí para ayudarte.

IDENTIFICA AL REMITENTE

No conocer al remitente debe ponernos en alerta máxima para no descargar ningún archivo adjunto ni pinchar en ningún enlace hasta estar completamente seguros de que no es un correo falso.

Las empresas **no suelen utilizar servicios gratuitos** para gestionar el correo electrónico. Desconfía de cuentas de correo profesionales con dominios como: *@google.es, @yahoo.com, @hotmail.com*, etc.

Si la empresa emisora del correo es de confianza **comprueba que la dirección del correo electrónico se corresponde** con la dirección de la empresa que supuestamente envía el mensaje. En la siguiente imagen se puede ver un correo que supuestamente viene de *CORREOS EXPRESS*, pero el dominio de la cuenta es *cartonell.es*, esto es una prueba suficiente para eliminar automáticamente el mensaje.

Asunto:DOCUMENTOS CORREOS
Fecha: Fri, 08 Nov 2019 03:10:59 +0000
De:CORREOS EXPRESS <rocio@cartonell.es>

Comprueba que **la dirección del correo del remitente coincide con la cuenta que ha enviado el mensaje**, en ocasiones puede ser una cuenta similar a la de alguna empresa con diferencias imperceptibles.

Netkia <info@netkla.es>
Netkia <info@nelkia.es>

ASUNTO Y CUERPO DEL MENSAJE

En muchas ocasiones el asunto de este tipo de mensajes suele **venir en mayúsculas** y en un tono que denota urgencia.

Asunto: SOLICITUD URGENTE DE COTIZACIÓN 00534-07.11.19

Desconfía de los saludos genéricos como pueden ser: *Estimado cliente, Buenos días señor, etc.* Si en el saludo no se incluye tu nombre es muy posible que no vaya dirigido a ti.

Hay que **prestar atención a la ortografía y gramática** del cuerpo del mensaje, en ocasiones los atacantes utilizan traductores automáticos que le dan un tono peculiar al mismo.

En caso de conocer al remitente, **comprobar que el estilo de redacción del mensaje** se corresponde con el utilizado por el mismo.

Desde ningún Banco, Entidad Oficial o Servicio (Google, Microsoft, Yahoo, etc.) **te van a solicitar nunca que envíes tus credenciales** o datos personales por correo electrónico.

ARCHIVOS ADJUNTOS

Presta mucha atención al **nombre completo del archivo adjunto**, nunca descargues ficheros cuya extensión sea: *.exe .com .bat*
En algunas ocasiones los ficheros adjuntos tienen nombres que tratan de ocultar su verdadera extensión:

No abras nunca ningún archivo directamente desde el cliente de correo electrónico o desde una web, **guarda el archivo en una carpeta en tu equipo**, el antivirus bloqueará el software malicioso antes de que este intente ejecutarse.

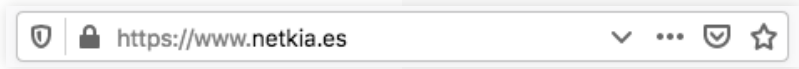
ENLACES

1

Antes de pinchar en un enlace **coloca el ratón encima del mismo para comprobar a donde apunta** la dirección real del enlace, si el texto del enlace no se corresponde con la dirección que muestra no pinches en el enlace.

2

Desconfía de cualquier sitio que no sea seguro, nunca introduzcas tus credenciales en una web no segura. Los sitios seguros comienzan siempre por *https://*



BUENAS PRÁCTICAS

Como usuarios podemos reforzar la seguridad de nuestro equipo con una serie de buenas prácticas:

- Mantener el **sistema operativo actualizado**.
- Mantener el **antivirus actualizado**.
- Realizar **copias de seguridad** periódicas.
- Utilizar **contraseñas sólidas** e intentar no utilizar la misma contraseña en diferentes servicios.