amger:pro

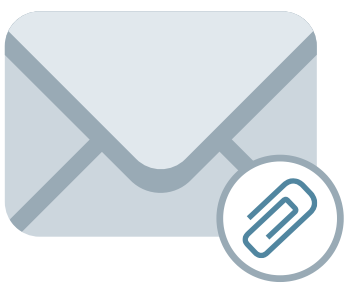
CIBERATAQUES EN ÉPOCA DE #CORONAVIRUS

RECOMENDACIONES PARA PROTEGER TUS EQUIPOS Y DISPOSITIVOS MÓVILES

CORREOS ELECTRÓNICOS

Extremar la atención en **correos electrónicos** de **procedencia desconocida o no solicitados**, tanto en la cuenta personal como profesional, especialmente los relacionados con el coronavirus u otros temas vinculados a la situación de alerta sanitaria actual (ayudas del Gobierno para empresas y autónomos, medidas sanitarias, donaciones, recomendaciones, etc.).

FICHEROS ADJUNTOS

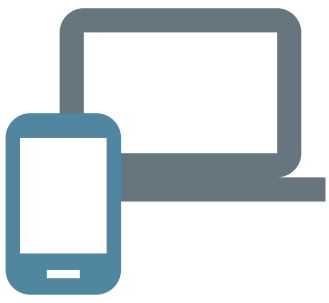


No abrir los **ficheros adjuntos** que vengan de direcciones de correo sospechosas o desconocidas.

ENLACES DESCONOCIDOS

No clicar en **enlaces desconocidos** a servicios no solicitados ni mensajes recibidos a través de **redes sociales** o **aplicaciones de mensajería.**

EQUIPOS CORPORATIVOS



Utilizar, siempre que sea posible, **equipos corporativos gestionados y configurados** por el servicio informático de tu empresa y seguir sus recomendaciones.

WI-FI DE CONFIANZA

Utilizar siempre **conexiones wi-fi de confianza**, evitando las gratuitas o no autenticadas, que pueden ser una puerta de entrada de fácil acceso para los ciberdelincuentes.

PÁGINAS WEB OFICIALES

Acudir a **fuentes de información oficiales** y **páginas web confiables** para seguir las noticias, evitando acceder a páginas con URLs extrañas o sospechosas, a pesar de que te lleguen a través de un contacto conocido.

LLAMADAS SOPORTE TÉCNICO

No atender **llamadas telefónicas** de supuestos servicios de **soporte técnico**, si no has solicitado el servicio o detectas algo extraño (idioma extranjero, tipo de servicio, solicitud de datos bancarios o personales o credenciales,...), puesto que probablemente sea un engaño.

SOLICITA TU AUDITORIA DE SEGURIDAD EN ONLINE@AMGERPRO.COM
WWW.AMGERPRO.COM