

# RIESGOS PARA EMPRESAS

Con esta guía pretendemos ayudarte para que no caigas en las trampas de los delincuentes.

**MANTENTE INFORMADO  
SOBRE  
CIBERSEGURIDAD  
EN ESTAS PÁGINAS**

<https://www.incibe.es>  
<https://www.osi.es>

- Comprueba dos veces la dirección de internet de la página a la que te estás conectando (una única letra puede llevarnos a ser estafados).
- Utiliza contraseñas complejas y sistemas de doble verificación.
- No visites páginas inseguras, comprueba si la dirección comienza por el protocolo seguro **HTTPS**.
- No hagas "click" en los enlaces, ni descargues adjuntos de correos electrónicos o mensajes no solicitados.
- Utiliza programas originales.
- Si recibes un mensaje o llamada diciendo que tu ordenador tiene problemas y te ayudan a solucionarlo, no facilites datos personales, descargues programas de control remoto o hagas "click" sobre enlaces sospechosos.
- Si has sido perseguido desconecta inmediatamente de la red el dispositivo, no pagues el rescate solicitado y ponte en manos de un técnico para solucionar el problema.

- Estafas en las compras o ventas en Internet.
- Robo de datos personales.
- "Secuestro" de los datos de nuestro ordenador mediante programas maliciosos.



# RECONOCELOS PARA ENTENDERLOS

- Ofertas de productos a precios excesivamente bajos.
- Recibir mensajes o correos electrónicos de organismos oficiales, entidades bancarias o publicidad en redes sociales, donde nos piden que introduzcamos claves personales, o números de tarjetas bancarias.
- Enlaces a páginas web para descarga de programas sin licencia aparentemente gratuitos.

## RECOMENDACIONES



- En las compras por internet no utilizar redes wifi públicas, comprar en comercios conocidos y seguros, no comprar cuando el anuncio del producto nos llegue de una página desconocida o correo electrónico no solicitado.
- No pagar a través de empresas de envío de dinero, usa métodos de pago seguros.
- Descarta de mensajes sobre premios de concursos donde no has participado.

## RECOMENDACIONES

- **Mantener actualizados** los sistemas informáticos (antivirus, sistemas operativos, aplicaciones).
- **No utilizar** redes públicas para el envío de nuestros datos.
- **Usar** aplicaciones que cifren los datos de extremo a extremo para el envío de correos electrónicos o documentos.
- **Realizar** copias de seguridad frecuentes y redundantes.
- **Formar a los empleados** para reconocer posibles engaños.
- **Prestar especial atención** a las operaciones de carácter económico, implantar la doble firma para transacciones económicas.
- **Utilizar** contraseñas complejas y con sistemas de doble verificación.
- **No tener a la vista** de terceros contraseñas o datos de acceso, guardarlas en un lugar seguro.
- **A demás** sigue las recomendaciones para un usuario particular.

# RIESGOS

- Estafas en el proceso de pago de facturas pendientes con proveedores habituales.
- "Secuestro" de los datos de nuestro ordenador mediante programas maliciosos.
- Accesos a las redes wifi propias para la captación de información o datos de la empresa.
- Obtención de contraseñas o datos de acceso que se encuentran a la vista.

# RECONOCERLOS PARA ENTENDERLOS



## RECOMENDACIONES



## RECOMENDACIONES

GUARDIA CIVIL  
ZONA DE ARAGÓN



# RIESGOS PARA AYUNTAMIENTOS Y ENTIDADES PÚBLICAS

## RIESGOS

- Bloqueos de los sistemas de la entidad pidiendo una cantidad de dinero en bitcoins (moneda virtual) para liberarlos.
- Robo de datos privados de los ciudadanos o integrantes de la Institución.
- Acceso remoto a los sistemas, bien usando aplicaciones escondidas en páginas web, aplicaciones gratuitas, o como adjuntos en correos electrónicos. También pueden llamar suplantando a técnicos del sistema operativo.
- Obtención de contraseñas o datos de acceso que se encuentran a la vista de terceros.



## RECONOCERLOS PARA EVITARLOS

- Recepción de llamadas telefónicas de servicios técnicos o mantenimiento por supuestos fallos en el sistema cuando no han sido solicitados o no existe tal fallo.
- Solicitud por parte de esos "supuestos técnicos" de contraseñas o datos de acceso a los sistemas para subsanar los supuestos fallos.
- Adernas de los indicados para las empresas.

## RECOMENDACIONES

- Mantener actualizados los sistemas (antivirus, sispemas operativos, aplicaciones).
- Realizar copias de seguridad diarias y en varios dispositivos de almacenamiento.
- No tener a la vista las contraseñas o datos de acceso, guárdalas en un lugar seguro.
- Evitar el uso de dispositivos de almacenamiento USB usados fuera de la entidad.
- Conciliar a los empleados de la Institución en la navegación segura por Internet, así como en evitar la instalación de aplicaciones no seguras en los equipos públicos.
- Seguir también las recomendaciones para empresas y particulares.



# RECUERDA

## PROTÉGETE CONTRA LOS CIBERATAQUES



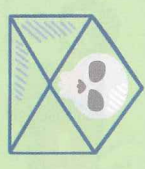
USA ANTIVIRUS



VERIFICA LA CONFIGURACIÓN DE PRIVACIDAD DEL NAVEGADOR



UTILIZA PÁGINAS SEGURAS



EVITA CORREOS MALICIOSOS



MANTÉN PRIVADA TU INFORMACIÓN PERSONAL



USA CONTRASEÑAS COMPLEJAS

SI HAS SIDO VÍCTIMA DE ALGÚN TIPO DE DELITO TELEMÁTICO PONLO EN CONOCIMIENTO DE LA GUARDIA CIVIL, LLAMA AL

062

GUARDIA CIVIL ZONA DE ARAGÓN

OFICINA PERIFÉRICA DE COMUNICACIÓN DE LA Bª ZONA DE LA GUARDIA CIVIL 04/2021



@guardia062 f www.guardia062.com/la-guardia062/ Guardia Civil Zaragoza

# GUÍA DE PREVENCIÓN DE LA CIBERDELINCUENCIA

CAMPAÑA DE PREVENCIÓN DE LOS DELITOS TECNOLÓGICOS



GUARDIA CIVIL ZONA DE ARAGÓN

062

