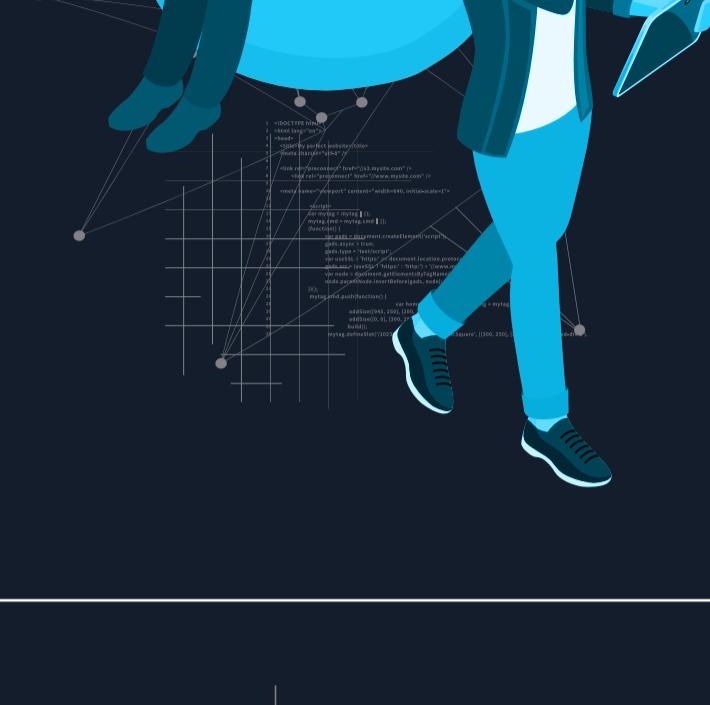


# CIBERCONSEJOS PARA PROTEGERSE DEL RANSOMWARE

El ransomware es considerado una de las amenazas ciberneticas más importantes del último tiempo, ya que genera significativas pérdidas económicas y de seguridad para las empresas. El objetivo de este tipo de malware es secuestrar los datos de una organización y/o persona para posteriormente pedir un rescate. Cómo protegerse y cómo actuar frente a este tipo de incidente, te contamos a continuación.

## ¿Qué es el Ransomware?



Tipo de malware diseñado para cifrar archivos en un dispositivo, impidiendo que una persona u organización accedan a la información y los sistemas. La infección puede ser por un phishing, publicidad en línea maliciosa o por sistemas y software no actualizados.

**Para recuperar los datos robados, el delincuente pide un rescate, por lo general, a través de criptomonedas.**

## Riesgos del Ransomware



- ① Secuestro y/o pérdida de datos y archivos de una persona u organización.
- ② Pérdida de confianza y datos de clientes y/o de la empresa.
- ③ Pérdidas económicas.
- ④ Posible exfiltración de datos privados.

## ¿Qué hacer si tengo un Ransomware?



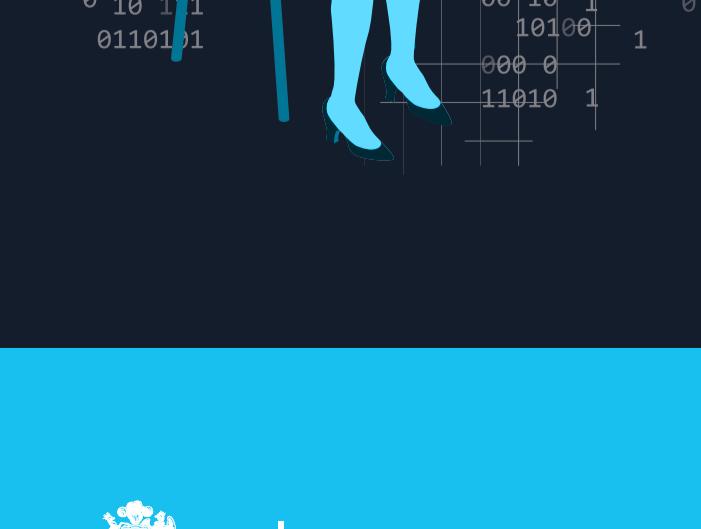
-  **NUNCA** pagar la recompensa solicitada.
-  **DESCONECTAR** el dispositivo de la red (Internet o WiFi) para no infectar otros equipos.
-  **DESCARGAR** un producto de seguridad para eliminar la infección y evitar su propagación.

## ¿Cómo prevenir?



- ① Contar con un programa de seguridad como antivirus y antispyware.
- ② Mantener actualizados todos los sistemas y software.
- ③ Crear copias de seguridad periódicamente, ya sea en la nube, unidades USB o discos externos y desconectarlos una vez hecha la copia.
- ④ Tener precaución con los correos electrónicos que invitan a descargar archivos adjuntos o ingresar a un link.

## Recomendaciones para empresas



- ① **REALIZAR** de forma rutinaria copias de seguridad y realizar pruebas de integridad de los datos y así asegurar su operatividad.
- ② **IMPLEMENTAR** sistemas antispyware para evitar recibir correos electrónicos maliciosos.
- ③ **APLICAR** los principios de mínimo privilegio y segmentación de red.