# Seguridad de la Información

# ~ RANSOMWARE ~

## Prevención y Recuperación

Seguir estos consejos puede reducir la probabilidad de que seas víctima de ransomware. El ransomware hace que tus datos o computadora queden inutilizables y te pide que hagas un pago para liberarlos.

## ¿Qué es el ransomware?

El ransomware es un software malicioso que te impide acceder a tu computadora (o a los datos almacenados en ella). Si tu computadora está infectada con ransomware, la computadora en sí puede bloquearse o los datos que contiene pueden ser robados, eliminados o encriptados.

Normalmente te piden que hagas un pago (el rescate), para "desbloquearla" o para acceder a tus datos. Sin embargo, incluso si pagas el rescate, no hay garantía de que obtengas acceso a tu computadora o a tus archivos. Esta es una de las razones por las que es importante tener siempre un respaldo reciente de tus archivos y datos más importantes.

### ¡No te dejes chantajear, mantén un respaldo!

*Si tienes un respaldo reciente de tus archivos más importantes, entonces no puedes ser chantajeado.*

Realiza respaldos periódicos de tus archivos más importantes (como fotos y documentos) y comprueba que sabes cómo restaurar los archivos desde el respaldo. Si no estás seguro de cómo hacerlo, puedes buscar en línea.

Asegúrate de que el dispositivo que contiene tu respaldo (como un disco duro externo o una memoria USB) no esté conectado permanentemente a tu computadora.

Activa el respaldo automático para que los datos de tu teléfono inteligente se copien automáticamente en la nube. Esto significa que podrás recuperar tus datos rápidamente si vuelves a iniciar sesión en tu cuenta desde otro dispositivo.

### Protección de tus datos y dispositivos

*Los siguientes pasos reducirán la probabilidad de que tus dispositivos se infecten con ransomware.*

Mantén actualizados tu sistema operativo y tus aplicaciones. Aplica actualizaciones de software de inmediato para ayudar a mantener tu dispositivo seguro. Esto incluye protección contra ransomware y otros tipos de virus. Configura las actualizaciones para que sucedan automáticamente, para que no se te olvide.

Asegúrate de que tu solución de antivirus esté encendido y actualizado. Windows y macOS tienen herramientas integradas de protección contra malware que son adecuadas para este propósito.

Evita descargar aplicaciones dudosas. Utiliza Únicamente las tiendas de aplicaciones oficiales (como Google Play o Apple App Store), que brindan protección contra virus.

### ¿Qué hacer si estás infectado?

*Si tu computadora ha sido infectada por ransomware (o cualquier tipo de malware), debes:*

Abre tu solución de antivirus (AV) y ejecuta un análisis completo. Sigue todas las instrucciones dadas. Si tu AV no puede limpiar tu dispositivo, deberás realizar una 'reinstalación limpia', que eliminará todos tus archivos personales, aplicaciones y configuraciones. Si no estás seguro de cómo hacerlo, puedes buscar en línea con otro dispositivo.

Restaura tus datos respaldados que has guardado en un dispositivo separado (como una memoria USB, un disco duro externo) o almacenamiento en la nube. No copies ningún dato de la computadora infectada.

Si recibes una llamada telefónica ofreciéndote ayuda para limpiar tu computadora, cuelgue inmediatamente (esta es una estafa común).

### ¿Debo pagar el rescate?

*Si pagas el rescate:*

- No hay garantía de que obtendrás acceso a tus datos o computadora.
- Tu computadora aún estará infectada.
- Estarás pagando a grupos criminales.
- Es más probable que seas objetivo en el futuro.

Fuente de información: www.ncsc.gov.uk/ransomware