CIBER SEGURIDAD

Castilla-La Mancha

# Píldoras Formativas de Ciberseguridad

## Como actuar ante un ataque de ransomware

15 Mayo 2026

Agencia de Transformación Digital de Castilla-La Mancha. 2026

Financiado por la Unión Europea NextGenerationEU

GOBIERNO DE ESPAÑA
MINISTERIO PARA LA TRANSFORMACIÓN DIGITAL Y DE LA FUNCIÓN PÚBLICA
SECRETARÍA DE ESTADO DE TELECOMUNICACIONES E INFRAESTRUCTURAS DIGITALES

Plan de Recuperación, Transformación y Resiliencia

incibe_ INSTITUTO NACIONAL DE CIBERSEGURIDAD

Castilla-La Mancha

# Cómo actuar ante un ataque de ransomware

El **ransomware** es un **tipo de malware** que bloquea o cifra los sistemas y los archivos de un equipo, haciendo imposible el acceso a la información hasta que se realiza un pago para su recuperación. Este tipo de ataque puede provocar **pérdidas de datos críticos, interrupciones en la actividad, daños económicos y afectación a la reputación**, tanto a nivel personal como empresarial.

Por ello, resulta fundamental comprender en qué consiste esta amenaza y cómo actuar ante su aparición, así como aplicar buenas prácticas de ciberseguridad que permitan **reducir los riesgos y proteger tanto la información personal como los activos de la organización**.

## No apagar el sistema

Evita **apagar o reiniciar el equipo** sin indicaciones del personal técnico, ya que podrías perder información relevante para el análisis del incidente o su recuperación.

## Aislar el equipo

**Desconecta** inmediatamente el dispositivo afectado de la red (WiFi, cable o VPN) para evitar que el **ransomware se propague** a otros equipos o sistemas de la organización.

## No pagar el rescate

No se recomienda realizar el pago, ya que **no garantiza la recuperación de los datos** y además contribuye a financiar la actividad de los ciberdelincuentes.

## Notificar de inmediato

Comunica inmediatamente el incidente al **equipo de seguridad** y, si procede, a las **autoridades competentes** según la gravedad del ransomware.

## Identificar el ataque

Intenta determinar qué información, archivos o sistemas han sido **afectados**, con el objetivo de **evaluar el impacto** y priorizar la recuperación.

## Recuperar desde copias

**Restaura los sistemas** y los datos únicamente desde copias de seguridad verificadas y seguras mediante herramientas de recuperación, asegurando que **no estén comprometidas por el ataque.**

**Agencia de Transformación Digital de Castilla-La Mancha. 2026**

Financiado por la Unión Europea NextGenerationEU

GOBIERNO DE ESPAÑA · MINISTERIO PARA LA TRANSFORMACIÓN DIGITAL Y DE LA FUNCIÓN PÚBLICA · SECRETARÍA DE ESTADO DE TELECOMUNICACIONES E INFRAESTRUCTURAS DIGITALES

Plan de Recuperación, Transformación y Resiliencia

incibe_ INSTITUTO NACIONAL DE CIBERSEGURIDAD

Castilla-La Mancha