

# RANSOMWARE: AMENAZA #1 A TU SEGURIDAD



## ¿Cuánto se puede perder por ransomware?

Un ciberataque de ransomware tiene un costo promedio de remediación de **\$761 106 USD**, para organizaciones que no pagan el rescate, y de **\$1,448,458 USD** para organizaciones que sí pagan.



## Una amenaza que afecta a TODOS

El **51%** de las organizaciones fueron **afectadas** por ransomware en el último año. Los delincuentes **lograron cifrar los datos en el 73%** de estos ataques.

?

- El ataque se lanza a través de un correo electrónico infectado, que una vez abierto **se reenvía a todos los contactos**.
- En 24 horas cifra datos en **30 millones de dispositivos** en todo el mundo.



- Se recomienda **capacitar a los empleados**, ellos pueden convertirse en una línea de defensa contra el ransomware.
- Tener un indicio de archivos corruptos o cifrados ayudará a **reducir el alcance de la amenaza**.

!



## Respaldo de datos como Mantra

- **Prevención ante todo:** Mantener los sistemas operativos actualizados y realizar copias de seguridad de forma periódica.
- Una copia de seguridad **puede evitar la pérdida de material y datos sensibles** en caso de robo y problemas técnicos.
- Si se presenta un ciberataque en donde haya secuestro de datos, la compañía puede **evitar pagar por el rescate**.



## Protección actualizada en todos los dispositivos

Una **defensa exhaustiva en todos los puntos de control** incluye:

- Correo electrónico.
- Soluciones web gateway.
- Protección del DNS
- Tener actualizado el antivirus de tu equipo.
- IPS (sistema de prevención de intrusiones) que pueda aplicarse para evitar la instalación o ejecución de archivos maliciosos en el sistema.

## Algunos tipos de ransomware

- **Malware criptográfico:** Cifra los archivos. Te permite iniciar sesión, pero no te deja abrir tus archivos, WannaCry es un ejemplo de este tipo de ransomware.
- **Bloqueador:** Impide por completo el acceso al equipo, Petya es un ejemplo de este tipo de ransomware
- **Doxware:** Descarga una copia de los archivos confidenciales de su víctima y amenaza con hacerlos públicos si no se paga el rescate. El ransomware Ransoc utiliza este método.



PARA MÁS INFORMACIÓN ENTRA A:

[www.smartekh.com](http://www.smartekh.com)

