

Pasos a seguir para proteger tu información del Ransomware

1.- Obtención y ejecución de un Antivirus XDR

Las plataformas XDR amplían la **cobertura para protegerse** contra tipos de ciberataques más sofisticados.

Integran funcionalidades de **detección, investigación y respuesta** en una gama más amplia de dominios, incluidos los puntos de conexión de una organización, las identidades híbridas, las aplicaciones y cargas de trabajo en la nube, el correo electrónico y los almacenes de datos.

¿Cómo funciona un XDR?

- 1.- Recopila y normaliza los datos
- 2.- Analiza y correlaciona datos
- 3.- Facilita la gestión de incidentes
- 4.- Ayuda a prevenir incidentes en el futuro

Principales ventajas de XDR

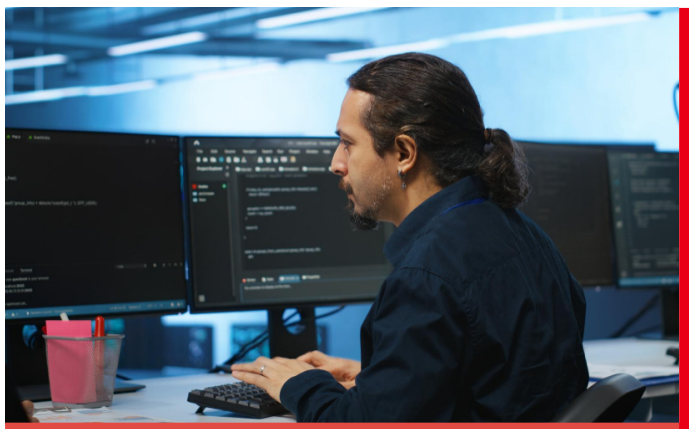
Con una plataforma XDR tendremos **grandes y excelente beneficios**, entre todos estos destacan:

- Detección y respuesta de amenazas aceleradas
- Priorización de incidentes mejorada
- Flujos de SecOps simplificados
- Conclusiones de SOC más rápidas



2.- Hardening: Endurecimiento de aplicaciones y dispositivos

El Hardening consiste en **asegurar un sistema reduciendo su cantidad de vulnerabilidades**. De esta manera, abarca un conjunto de herramientas, prácticas y métodos que buscan limitar la superficie de ataque de una infraestructura tecnológica.



Generalmente, este hardening se realiza **a través de CIS Benchmark**, que son un conjunto de mejores **prácticas y directrices técnicas** para una configuración segura de un sistema objetivo.

Estos proporcionan recomendaciones de **configuración específicas y controles de seguridad** para varios sistemas operativos, aplicaciones de software y dispositivos.

3.- Actualizaciones constantes: Defensa digital

El actualizar aplicaciones y dispositivos es clave para prevenir ataques de ransomware. Las actualizaciones **corrigen vulnerabilidades y refuerzan la seguridad**, protegiendo tus sistemas de posibles explotaciones.

Patch Tuesday

El Patch Tuesday se refiere al segundo martes de cada mes, que es el día, cuando la mayoría de plataformas **publican parches para mejorar la seguridad de su software**.

Exploit Wednesday

Se acuñó el término "Exploit Wednesday" (miércoles de exploits) por los muchos **eventos de explotación** que se observan poco después del lanzamiento de un parche; después del Patch Tuesday.

El análisis del parche ayuda a los **desarrolladores de exploits a aprovechar** de inmediato **la vulnerabilidad no revelada previamente**, que permanecerá en los sistemas sin parchear.

4.- Un adecuado y eficaz servicio de Backup

Para salvaguardar tus datos contra ataques de ransomware, es esencial contar con un **servicio de backups sólido y eficiente**.

La protección de la información no solo depende de la realización de copias de seguridad, sino también de **su correcta gestión y almacenamiento**.



3-2-1 Backup Rule

Se recomienda seguir la regla:

- Mantener **3 copias de tus datos**.
- Usar **2 tipos de medios distintos** para almacenarlas.
- Asegurar que **1 de las copias esté almacenada en una ubicación fuera del sitio**.

Esta estrategia reduce significativamente el riesgo de pérdida total y facilita la recuperación en caso de incidentes de ransomware.

3-2-1 Backup Rule.-



3 copias de la información



2 tipos de medios diferentes para almacenarlas



1 copia almacenada fuera del sitio

En **Najera Solutions**, te ofrecemos el **licenciamiento de Office 365**, una gran solución que resuelve las problemáticas de estas recomendaciones para la prevención de posibles ataques de Ransomware, ya que **incluye Windows Defender y Microsoft Intune**.

Contáctanos hoy mediante nuestra página web <https://www.najerasolutions.com.mx/> contamos con atención personalizada para cada proyecto.