CIBERSEGURIDAD PARA ORGANIZACIONES MÁS PEQUEÑAS

LISTA DE VERIFICACIÓN DE RANSOMWARE

PREPARACIÓN FRENTE A RANSOMWARE

☐ **A medida que desarrolle un plan de prevención y protección frente a casos de ransomware, evalúe periódicamente lo siguiente:**

- ¿Su organización tiene copias de seguridad programadas con frecuencia?
- ¿Hay algún dispositivo no esencial conectado a la red de su organización?
- ¿Comprende su organización los riesgos normativos y jurídicos que conlleva el pago de un rescate?
- ¿Su organización actualiza periódicamente sus sistemas de software? ¿Están automatizadas estas actualizaciones?
- ¿Tiene su organización un plan para hacer frente a un ataque de ransomware y pérdida de datos?
- ¿Tiene su sistema una póliza de seguro cibernético? Si es así, ¿cómo cubre ese plan los ataques de ransomware?

PROTECCIÓN EN TIEMPO REAL

☐ **Invierta en sistemas de protección antimalware que se adapten a la nueva inteligencia de amenazas en tiempo real.**

☐ **Evalúe la seguridad de todos los dispositivos conectados a las redes que contienen información confidencial o esencial.**

- ☐ Conecte todos los sistemas no esenciales a una red independiente.
- ☐ Tenga en cuenta la seguridad de las configuraciones de trabajo a distancia. Asegúrese de que las herramientas de seguridad funcionen fuera de la red para supervisar todo el tráfico de la web.

☐ **Promueva la formación de los empleados en torno a los ataques de phishing y la necesidad de una protección de contraseñas sólida.**

☐ **Considere la posibilidad de aplicar la autenticación multifactorial en toda su organización, si es viable.**

☐ **Mantenga todos los programas y sistemas actualizados periódicamente.**

- ☐ Cambie la configuración para permitir actualizaciones automáticas si es posible.

☐ **Desarrolle un plan de respuesta a incidentes y de gestión de crisis sobre cómo hacer frente a un ataque de ransomware y a la pérdida de datos importantes.**

- ☐ Prepare un plan de comunicación externa en caso de un ataque de ransomware.

COPIAS DE SEGURIDAD DE DATOS

☐ **Invierta en sistemas de copia de seguridad que sean seguros y se actualicen periódicamente y que mantengan sus datos protegidos.**

- ☐ Si utiliza USB o discos duros, desconecte físicamente estos dispositivos de los equipos conectados en red después de que las copias de seguridad hayan terminado.
- ☐ Si utiliza el almacenamiento en la nube, equipe los servidores con encriptación de alto nivel y autenticación multifactorial.

☐ **Cree una copia de solo lectura del libro mayor para la recuperación de desastres en el peor de los casos.**

- ☐ **Desarrolle sistemas que permitan la recuperación y reparación automatizadas de datos.**
- ☐ **Elabore escenarios para evaluar el tiempo que se tardará en recuperar datos y servicios comerciales críticos.**

ENTORNO NORMATIVO

- ☐ **Evalúe las directrices normativas y legales pertinentes para el ransomware en su entorno operativo.**
  - ☐ Considere las directrices específicas para cada país.
  - ☐ Tenga en cuenta las directrices específicas para el sector financiero.
  - ☐ Considere los requisitos legales y normativos internacionales.
  - ☐ Prepare un plan para la evaluación periódica de las directrices cambiantes.
  - ☐ Valore los riesgos que conlleva el pago de un rescate.
  - ☐ Coordínese con las fuerzas del orden locales.
  - ☐ Establezca conexiones para compartir rápidamente la información en caso de un ataque.
  - ☐ Evalúe los beneficios y desventajas de las pólizas de seguro cibernético frente a ataques de ransomware.

CARNEGIE
ENDOWMENT FOR
INTERNATIONAL PEACE

CarnegieEndowment.org