CINCO PASOS CRÍTICOS

PARA MEJORAR LA RESILIENCIA INFORMÁTICA DE SU ORGANIZACIÓN

COHESITY

RESILIENCIA EN TODAS PARTES

INTRODUCCIÓN

El aumento de los ataques de ransomware y sus impactos cada vez más graves revelan una verdad incómoda. Incluso con inversiones sustanciales en prevención, estas medidas por sí solas no son suficientes para contrarrestar las amenazas actuales.

Nos guste o no (y no nos gusta), los ciberataques no desaparecerán. Y nunca permanecerán iguales, ni en frecuencia, gravedad o escala.

Esas son las malas noticias.

Ahora, las buenas noticias. Existe un manual de estrategias comprobado para mejorar la resiliencia cibernética, y organizaciones como la suya lo están utilizando para repensar su enfoque y disfrutar de mejores resultados.

En este libro electrónico, presentamos este manual de estrategias como una progresión de cinco pasos hacia la resiliencia cibernética. Al tomar medidas concretas a lo largo de los cinco pasos, se alineará con las mejores prácticas en respuesta cibernética y recuperación. También verá beneficios sustanciales en materia de seguridad, ahorro de costos y menor riesgo.

ALGUNOS antecedentes rápidos

A pesar de una mayor conciencia de las amenazas cibernéticas como el ransomware, los ciberataques continúan causando enormes daños operativos, financieros y a la reputación. De hecho, son la principal amenaza para las empresas a nivel mundial.

El impacto financiero es real:

540 000 USD
que se pierden por cada hora de inactividad[1]

Más de 1000 000 000 USD
en pagos anuales de ransomware[2]

El estado del ransomware 2024 de Sophos[3] incluye estadísticas igualmente aleccionadoras:

Del 59 % de las organizaciones encuestadas que fueron afectadas por ransomware en el último año, el **94 % dijo que los atacantes apuntaron a sus copias de seguridad,** y el **57 % de esos intentos de comprometer copias de seguridad fueron exitosos.**

Además:

- **El 70 % de los ataques resultaron en el cifrado de datos**
- **Se exigieron 2 000 000 USD en promedio por rescate**
- **El 34 % de las organizaciones tardaron más de un mes en recuperarse**

Ahora es el momento de contar con estrategias, capacidades y soluciones nuevas y más efectivas.

[1] Splunk, Los costos ocultos del tiempo de inactividad: El problema de 400 mil millones de dólares que enfrentan las empresas Global 2000: https://www.splunk.com/en_us/pdfs/gated/ebooks/the-hidden-costs-of-downtime.pdf

[2] Chainalysis, Los pagos de ransomware superaron los 1000 000 000 USD en 2023, alcanzando un récord máximo después de la declinación de 2022, 7/2/24: https://www.chainalysis.com/blog/ransomware-2024/

[3] Sophos, El estado del ransomware 2024: https://www.sophos.com/en-us/content/state-of-ransomware

DOS RAZONES POR LAS QUE LA RESILIENCIA CIBERNÉTICA PUEDE SER ESPECIALMENTE DESAFIANTE:

1. La recuperación cibernética no es como la recuperación ante desastres.

Incluso si su organización cuenta con procesos sólidos de recuperación ante desastres, no puede confiar en estos mismos procesos para recuperarse de los ciberataques.

En un desastre, ya sea un incendio, una inundación, un corte de energía o incluso una mala configuración, usted puede hacer rápidamente un análisis de la causa fundamental para averiguar qué salió mal. En un ciberataque, pueden haber ocurrido cientos de cosas que requerirán una investigación y corrección exhaustivas; además, tiene a un adversario socavando activamente sus esfuerzos de recuperación y presionándolo para que pague el rescate.

2. Incluso las organizaciones y los expertos más experimentados pueden subestimar cuán destructivo podría ser un ataque de ransomware.

Puede suponer que los sistemas de confianza pueden ayudarlo a volver a estar en línea o contar con datos y evidencia para saber qué sucedió.

Pero en un ciberataque, los mismos sistemas en los que confía para investigar el incidente pueden estar caídos, o haber sido evadidos o estar comprometidos. Cuando los datos buenos se entremezclan con los malos, el camino hacia la recuperación será más largo y más difícil. Es por eso que vemos que muchas organizaciones inteligentes aún luchan por lograr una recuperación rápida, limpia y segura.

VEAMOS LOS **CINCO PASOS CRÍTICOS** PARA MEJORAR LA RESILIENCIA CIBERNÉTICA

Piense en esto como un plan práctico, donde cada paso que dé lo lleva más adelante en el progreso.

PASO UNO

PROTEJA TODOS LOS DATOS.

Puede sonar simple, pero muchas organizaciones aún no dan este primer paso crucial, y es probable que la expansión de datos sea la culpable.

El crecimiento orgánico de los datos ha llevado a la fragmentación y los silos, ampliando significativamente la superficie de ataque y dejando a las organizaciones más expuestas que nunca. Al mismo tiempo, la gestión y la seguridad de los datos a escala ejercen una creciente presión sobre la eficiencia operativa.

Esta combinación (más datos en más lugares, con menos capacidad para gestionarlos de manera eficiente) ha creado las condiciones perfectas para que los atacantes causen estragos.

BENEFICIOS NOTABLES DEL PASO UNO

- ☑ **Seguridad mejorada**
- ☑ **Menor riesgo**
- ☑ **Mejora del cumplimiento y la gobernanza**
- ☑ **Menores costos y mejor retorno de la inversión**
- ☑ **Mayor eficiencia de TI**

ACCIONES CLAVE PARA IMPLEMENTAR EL PASO UNO

1. **Adopte una plataforma de datos moderna que admita más de 1000 fuentes de datos, que incluya:**

- Máquinas virtuales (VM)
- Aplicaciones SaaS
- Bases de datos
- Entornos NAS (datos no estructurados)

2. **Asegúrese de que su plataforma funcione en entornos locales, en la nube y SaaS.**

Debido a que tiene datos por todas partes, su plataforma debe tener modelos de implementación flexibles unificados por una interfaz de usuario y API comunes.

3. **Simplifique las operaciones con una interfaz de usuario intuitiva.**

Cuando su interfaz de usuario es fácil de usar, puede tener un equipo relativamente pequeño que gestione una gran infraestructura. Y que lo haga bien. Nuestros clientes disfrutan de eficiencias operativas superiores con una sola interfaz de usuario y un conjunto de API para automatizar los flujos de trabajo en nuestra plataforma.

4. **Obtenga una compresión de almacenamiento fuerte.**

Querrá usar una plataforma con una compresión de datos fuerte. Esto producirá ahorros sustanciales cuando se ejecute a escala de petabytes. Tenemos un sistema de archivos único que es el estándar de la industria. Una compresión del almacenamiento realmente fuerte proporciona un TCO más bajo.

PASO DOS

ASEGÚRESE DE QUE LOS DATOS SIEMPRE SEAN RECUPERABLES.

Los atacantes apuntan a las copias de seguridad. Saben que si pueden afectar esta última línea de defensa, será mucho más probable que se pague el rescate, ya que su organización no tendrá otra salida.

Y si bien puede ser bueno suponer que una plataforma de datos moderna garantiza copias de seguridad recuperables listas para usar, esto no es del todo cierto.

Debe tomar varias medidas para que sea más difícil para los atacantes obtener acceso y para que su organización pueda recuperar copias de seguridad limpias si lo logran.

BENEFICIOS NOTABLES DEL PASO DOS

- ☑ **Recuperación más rápida y segura**
- ☑ **Mayor protección contra ataques**
- ☑ **Preparación para la auditoría**
- ☑ **Alineación de confianza cero**

ACCIONES CLAVE PARA IMPLEMENTAR EL PASO DOS

1. **Fortalezca su plataforma configurando funciones potentes como:**

- Autenticación multifactor (MFA)
- Inmutabilidad (para que los datos no se puedan alterar o eliminar)
- Control de acceso basado en roles (RBAC)
- Separación de tareas (dividir tareas críticas entre diferentes personas)

2. **Implemente una bóveda cibernética**

Con una copia aislada de sus datos más importantes y el cumplimiento de la **regla de copia de seguridad 3-2-1-1** (tres copias de datos, dos medios diferentes, uno fuera del sitio y uno inmutable), siempre tendrá una copia de sus datos disponible en caso de emergencia.

En Cohesity también proporcionamos un sistema avanzado de gestión de claves para que aún podamos dar a nuestros clientes acceso a sus datos en caso de un ataque.

Este acceso garantiza que las copias de seguridad sean siempre recuperables.

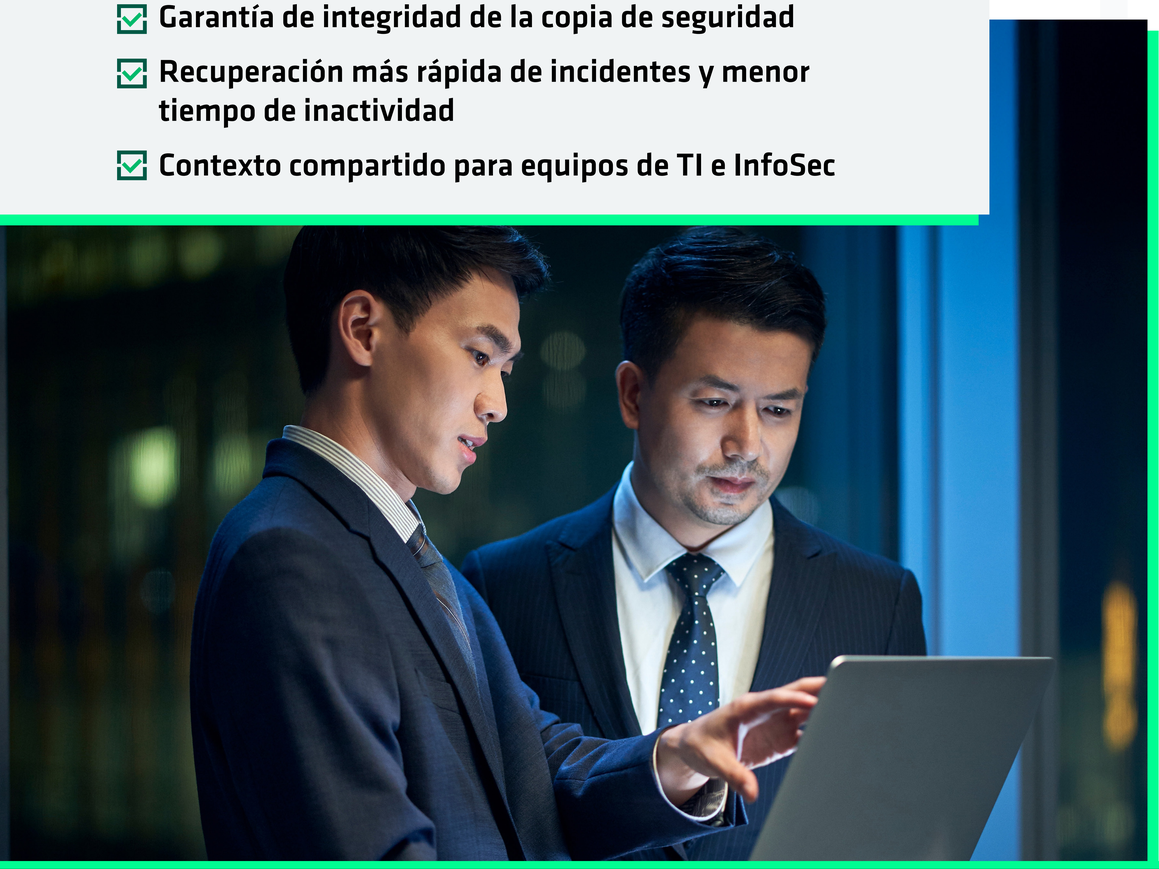
PASO TRES

DETECTE E INVESTIGUE LAS AMENAZAS.

Este paso se relaciona con el poder combinado del escaneo de amenazas y las capacidades de búsqueda de amenazas.

BENEFICIOS NOTABLES DEL PASO TRES

- **Detección y mitigación temprana de amenazas**
- **Garantía de integridad de la copia de seguridad**
- **Recuperación más rápida de incidentes y menor tiempo de inactividad**
- **Contexto compartido para equipos de TI e InfoSec**



ACCIONES CLAVE PARA IMPLEMENTAR EL PASO TRES

1. Sea proactivo escaneando regularmente las amenazas en sus copias de seguridad. Piense en este escaneo proactivo de **amenazas** como practicar una higiene constante. Le ayudará a:

- Eliminar cualquier cambio lo más rápido posible
- Identificar malware u otras vulnerabilidades

2. Inicie las capacidades de **búsqueda de amenazas** cuando busque amenazas específicas. Nuestras fuentes de amenazas seleccionadas e integraciones con los proveedores del ecosistema de seguridad en nuestra Alianza de Seguridad de Datos, incluidos CrowdStrike, Palo Alto Networks, Cisco y más, significan que usted obtiene el beneficio combinado de su sabiduría colectiva con los datos que podemos aportar a estos sistemas.

Sus equipos de InfoSec y TI también operarán con el mismo conjunto de información.

Habiendo ayudado a los clientes a recuperarse de los ciberataques a lo largo de los años, el escaneo de amenazas nativas y las capacidades de búsqueda de amenazas deben formar parte de su plataforma de datos.

¿Por qué? Porque otros sistemas de seguridad pueden estar desactivados o desconectados cuando se encuentra bajo ataque.

PASO CUATRO

PRACTICAR LA RESILIENCIA DE LAS APLICACIONES.

Cuando se trata de "practicar", ya está en buena forma si ha efectuado los pasos 1 a 3 anteriores. Ha puesto en pie su plataforma, la ha reforzado y ha ampliado su implementación con una bóveda cibernética.

También ha tenido una buena experiencia con el escaneo regular de amenazas y la búsqueda de amenazas. ¡Bien hecho!

En el paso cuatro, usted lleva la preparación al siguiente nivel al practicar sus procesos de respuesta y recuperación para la infraestructura, los datos y las aplicaciones. Después de todo, no querrá que la primera vez que haga esto sea durante un ataque real, cuando sus sistemas estén caídos y la presión esté sobre sus hombros.

Tal vez esté pensando: "Restaurar todo a su estado operativo es un proceso que lleva mucho tiempo. ¿Cómo puedo efectuar pruebas regularmente y aun así hacer mi trabajo diario?"

BENEFICIOS NOTABLES DEL PASO CUATRO

- ☑ **Recuperación más rápida y segura**
- ☑ **RTO mejorado**
- ☑ **Menor riesgo de reinfección**
- ☑ **Disrupción reducida y menor riesgo financiero**

Aquí es donde entra en juego la orquestación.

Con la orquestación, puede automatizar los flujos de trabajo de respuesta y recuperación y comenzar a "ensayar" volver a poner sus sistemas en línea después de un ataque. Estos ensayos lo ayudarán a mejorar la respuesta y la recuperación, y la orquestación puede ayudarlo a perfeccionar esas prácticas con menos esfuerzo manual.

Un ejemplo clave de automatización en el trabajo: Nuestra solución de sala limpia le permite crear un entorno separado donde puede llevar a cabo análisis forenses y profundizar en los bits de datos infectados, comprender lo que sucedió y luego erradicar el artefacto del ataque para que pueda estar seguro de que es seguro recuperar sus sistemas. Este enfoque ofrece una combinación única de velocidad, automatización y análisis forenses potentes para ayudar a los equipos de respuesta ante incidentes a colaborar con los equipos de TI. El resultado: una respuesta cibernética y recuperación más rápidas.

En este paso, también trabajará con Cohesity CERT (equipo de respuesta a eventos cibernéticos). Estos expertos lo ayudarán a responder y manejar incidentes, desde ransomware sofisticado y violaciones de datos hasta ataques dirigidos. Nunca tendrá que hacerlo solo.

ACCIONES CLAVE PARA IMPLEMENTAR EL PASO CUATRO

1. Practique con orquestación y ensayos
- Automatice sus procesos de respuesta y recuperación
- Lleve a cabo ensayos para refinar sus planes de respuesta, incluida la forma en que secuencia la recuperación de infraestructura, datos y aplicaciones

2. Use una sala limpia
- Cree un entorno separado y seguro para el análisis forense
- Identifique y erradique amenazas antes de restaurar infraestructura, fuentes de datos y aplicaciones

3. Obtenga apoyo experto
- Comuníquese con el CERT de Cohesity cuando esté bajo ataque

PASO CINCO

OPTIMIZAR LA POSTURA DE RIESGO DE LOS DATOS.

Además de que las bandas de ransomware son cada vez más peligrosas, ahora tiene más datos que administrar que nunca (en las instalaciones, SaaS, la nube, el borde). Todos siempre piensan: "Mmm, ¿qué tengo en ese bucket S3 sin asegurar que nadie conoce o está monitoreando?".

Además de los buckets S3 no asegurados, los riesgos ocultos también pueden incluir bases de datos huérfanas, credenciales expuestas y más.

Medidas proactivas como la gestión de la postura de seguridad de los datos (DSPM) y la clasificación de datos pueden ayudar a reducir estos riesgos.

BENEFICIOS NOTABLES DEL PASO CINCO

- ☑ **Visibilidad y clasificación de datos mejoradas**
- ☑ **Identificación y mitigación proactiva de riesgos**

ACCIONES CLAVE PARA IMPLEMENTAR EL PASO CINCO

1. **Averigüe dónde están los datos**

- Escanee su entorno y evalúe dónde están los datos y cuál es su nivel de protección. Toda la clase de herramientas con DSPM lo hace posible.
- Comprenda lo que puede haber en su patrimonio de respaldo y asegúrese de que esté protegido de la manera correcta con nuestras integraciones completas con algunos de los mejores proveedores de la industria, incluidos Cyera y BigID.

2. **Evalúe lo que puede haberse visto afectado en una violación o lo que puede haber sucedido en un caso de exfiltración de datos**

- Obtenga la cobertura adecuada que necesita y reduzca su riesgo con la clasificación de datos integrada de nuestros productos.
- Responda rápidamente cuando haya un incidente y los abogados pregunten: ¿Qué datos se han visto afectados? ¿Qué tan sensibles son? ¿Cuál es nuestro riesgo? ¿Cuántos clientes se han visto afectados? ¿Qué tipos de registros se han visto afectados?

CONCLUSIÓN

Ahora comprende los cinco pasos críticos para mejorar la resiliencia cibernética de su organización y cuenta con la información práctica necesaria para implementar estos pasos en su entorno.

En Cohesity estamos en una posición única para guiarlo a lo largo de esta progresión, de modo que pueda lograr la mayor resiliencia cibernética posible.

Para obtener más información sobre cómo recuperarse del ransomware de manera segura y rápida, recomendamos:

“CÓMO FORMULAR UNA RESPUESTA EN TIEMPOS DE GUERRA ANTE CIBERATAQUES DESTRUCTIVOS”.

COHESITY

RESILIENCIA EN TODAS PARTES

6100028-002-ES 6-2025