COHESITY

RESILIENCE EVERYWHERE

RESILIENCIA CIBERNÉTICA EN LA ERA DEL RANSOMWARE

Cómo Cohesity ayuda a las organizaciones a resistir y recuperarse de los ciberataques mientras se alinean con el Marco de Ciberseguridad 2.0 del NIST.

CONTENIDO

DE LA RESILIENCIA DE LOS DATOS A LA RESILIENCIA CIBERNÉTICA

Los desastres naturales representan una gran amenaza para las operaciones comerciales. Un relámpago, un huracán, un tornado o una inundación pueden causar daños graves y detener el negocio. En estas situaciones, las estrategias de resiliencia de datos garantizan que los datos permanezcan intactos y accesibles incluso en caso de fallas de hardware, eliminaciones accidentales o desastres naturales.

Sin embargo, estos eventos no están dirigidos activamente a su negocio con ataques continuos e intencionales.

Compárelo con una amenaza cibernética. Los actores de amenazas nunca dejan de trabajar y emplear nuevas herramientas para tomar sus datos como rehenes y paralizar su negocio. Los vectores de ataque a menudo son multifacéticos y evasivos. Además, el riesgo de reinyectar vulnerabilidades, cuentas comprometidas y otros artefactos de ataque en su entorno es una amenaza generalizada. En comparación con los escenarios tradicionales de continuidad del negocio y recuperación ante desastres, donde la causa raíz suele ser obvia, responder a las amenazas cibernéticas requiere investigación para descubrir estas causas e impulsar medidas correctivas para evitar su recurrencia.

Además, en un ataque de ransomware, la infraestructura de seguridad y la evidencia clave pueden haber sido afectadas por el incidente, lo que puede afectar la capacidad de entregar productos y servicios.

Al desarrollar un negocio ciberresistente, los líderes de TI y seguridad necesitan procesos más sólidos, dinámicos y colaborativos en comparación con los procesos utilizados al responder a una interrupción estándar causada por desastres naturales o interrupciones técnicas. La resiliencia cibernética se basa en las prácticas de resiliencia de datos e incluye elementos como la preparación para la ciberseguridad, los planes de respuesta a incidentes, la capacitación de los empleados y la inteligencia sobre amenazas.

Las amenazas cibernéticas actuales necesitan soluciones modernas que promuevan la visibilidad global de los activos de datos protegidos y optimicen la colaboración entre los profesionales de TI y de seguridad.

En Cohesity, nuestras soluciones modernas de seguridad de datos impulsadas por IA permiten a las organizaciones fortalecer la preparación cibernética, acelerar la respuesta ante incidentes y lograr una recuperación rápida y segura.

CON COHESITY, USTED PUEDE:

- Proteger todos sus datos.
- Asegurarse de que sus datos siempre sean recuperables.
- Obtener visibilidad de las vulnerabilidades y amenazas en sus datos de copia de seguridad.
- Responder rápida y eficazmente a los ataques y buscar amenazas que evadan las defensas tradicionales.
- Recuperar sistemas y datos de manera rápida y segura.

El resultado es un negocio más resiliente, capaz de prepararse, resistir, responder y recuperarse de los ataques cibernéticos.

UNA PARADOJA DE CONFIANZA Y CAPACIDAD

El 78 % de las organizaciones confían en la estrategia de resiliencia cibernética de su empresa[1]. Esto es, por lo general, una buena señal, siempre que esta confianza esté respaldada por capacidades concretas. Pero los datos muestran una desconexión entre la intención estratégica y las capacidades reales.

El 98 % apunta a recuperar datos y restaurar procesos comerciales después de un ataque en el plazo de un día[2].

Pero solo el **2 %** pudo lograr esto[3].

Afortunadamente, Cohesity proporciona un manual comprobado con procesos y herramientas para ayudar a los clientes de todo el mundo a reanudar las operaciones rápidamente y mitigar los impactos de un ataque.

[1-3] Informe de resiliencia cibernética global de Cohesity 2024

6 CLAVES PARA CREAR UN NEGOCIO CON RESILIENCIA CIBERNÉTICA

Nuestras soluciones de seguridad de datos en Cohesity ayudan a las organizaciones a comprender, gestionar y reducir mejor los riesgos, y a fortalecer la resiliencia cibernética en consonancia con las funciones clave del Marco de Ciberseguridad del NIST: Gobernar, identificar, proteger, detectar, responder y recuperar.

GOBERNAR
- Clasificar los datos de respaldo para comprender los requisitos regulatorios.
- Apoyar el cumplimiento de los marcos de seguros cibernéticos y otras obligaciones contractuales relacionadas con datos de terceros.

IDENTIFICAR
- Escanear los sistemas frágiles en busca de vulnerabilidades sin impacto.
- Identificar los sistemas críticos que no están respaldados.
- Mejorar la respuesta a incidentes futuros y las actividades de BC/DR.
- Identificar áreas de mejora en los programas de resiliencia cibernética de las organizaciones.

PROTEGER
- Proteger los datos empresariales a escala.
- Proteger las copias de seguridad de los ataques.
- Probar copias de seguridad y restauraciones.

DETECTAR
- Detectar cifrado de ransomware, ataques wiper e infiltrados maliciosos.
- Buscar proactivamente indicadores de compromiso para ser inmune a las técnicas de evasión.
- Enviar detecciones de seguridad a herramientas de SOC para su correlación.
- Capturar más artefactos forenses y activar instantáneas incrementales basadas en señales EDR/XDR.
- Identificar malware en servidores NAS.

RESPONDER
- Involucrar al equipo de respuesta a eventos cibernéticos (Cyber Event Response Team, CERT) de Cohesity para acelerar la respuesta y asegurar la recuperación.
- Restaurar las herramientas de respuesta y AD a un estado confiable y proporcionar acceso rápido.
- Establecer rápidamente una sala limpia para la respuesta y la recuperación.
- Buscar pasivamente artefactos para identificar otros sistemas afectados.
- Hacer un análisis forense de los sistemas de archivos históricos.
- Comprender las vulnerabilidades históricas que se explotaron en el ataque.
- Ayudar a cumplir con las obligaciones regulatorias y de cumplimiento para notificar a los reguladores, socios y sujetos de datos afectados.

RECUPERAR
- Garantizar que la recuperación de sistemas y datos permita la mitigación de amenazas.

1.

Gobernar los datos de respaldo para comprender los requisitos regulatorios y abordar el riesgo.

El panorama de datos actual es vasto —como un garaje sobrecargado—, lo que hace que sea cada vez más difícil localizar datos confidenciales y garantizar que estén protegidos adecuadamente. Esta falta de visibilidad aumenta el riesgo de exposición de datos e incumplimiento normativo.

Para gestionar este riesgo, las organizaciones no solo deben cumplir con los requisitos legales y reglamentarios (como HIPAA, CCPA y GDPR), sino que también deben demostrar controles internos sólidos mediante una gobernanza de ciberseguridad eficaz. Cada vez más, estos controles no se tratan solo de cumplimiento, sino que se están volviendo esenciales para obtener un seguro de ciberseguridad.

Con la frecuencia y la gravedad de los ciberataques en aumento, el seguro cibernético se ha convertido en una estrategia crítica de transferencia de riesgos. Ayuda a cubrir pérdidas financieras como la recuperación de datos, los honorarios legales y otras consecuencias después de un incidente. Pero las aseguradoras exigen más a los clientes, y requieren pruebas de una sólida protección de datos y controles de seguridad antes de emitir o renovar pólizas.

Para anticiparnos a estos requisitos, ayudamos a las organizaciones a:

Descubrir y clasificar datos confidenciales. Utilice nuestras instantáneas de copia de seguridad ilimitadas e inmutables para descubrir y categorizar datos confidenciales en su entorno. Nuestro motor de clasificación de datos integrado utiliza cientos de clasificadores y algoritmos impulsados por IA para identificar y etiquetar información regulada y de alto riesgo, lo que le ayuda a inventariar activos digitales y aplicar políticas de seguridad adecuadas.

Apoyar el cumplimiento de los requisitos de seguros cibernéticos y otras obligaciones contractuales relacionadas con datos de terceros. Nuestra plataforma ayuda a cumplir con las crecientes expectativas de las aseguradoras y los reguladores mediante la implementación de controles de mejores prácticas:

- Entornos de respaldo aislados separados de la red de producción.
- Servicios de copia de seguridad en la nube dedicados.
- Cifrado en reposo y en tránsito.
- Instantáneas de copia de seguridad inmutables.
- Acceso basado en roles con credenciales separadas.
- Exigencia de MFA para acceso interno y externo.
- Pruebas de integridad de copias de seguridad antes de la restauración para garantizar que no tengan malware.

2.

Identificar los riesgos de resiliencia cibernética

La gestión efectiva del riesgo de ciberseguridad requiere una comprensión clara de las vulnerabilidades en su entorno de TI, incluidos los sistemas de copia de seguridad. También implica priorizar la protección de los activos de datos de acuerdo con su clasificación y mejorar continuamente a través de pruebas de seguridad, simulacros y lecciones aprendidas de esfuerzos pasados de respuesta ante incidentes y recuperación.

CyberScan
Powered by tenable

Escanear los sistemas frágiles en busca de vulnerabilidades sin impacto.

Utilice Cohesity CyberScan, con tecnología de Tenable, para realizar escaneos de vulnerabilidades en instantáneas de respaldo y evitar el impacto en los sistemas de producción.

Identificar los sistemas críticos que no están respaldados.

Integrar Cohesity con su proveedor preferido de gestión de la postura de seguridad de datos (Data Security Posture Management, DSPM) es una forma poderosa de descubrir riesgos ocultos de resiliencia cibernética. Las soluciones DSPM proporcionan visibilidad tanto de los repositorios de datos conocidos como de los olvidados en diversas plataformas en la nube, clasifican los datos para identificar información confidencial y determinan el riesgo de exposición.

Si bien es posible que gran parte de sus datos confidenciales ya estén protegidos por Cohesity Data Cloud y las políticas de copia de seguridad existentes, a menudo quedan brechas significativas. Ahí es donde entra en juego la integración con DSPM.

Al combinar las perspectivas de DSPM con Cohesity, puede identificar sistemas y datos críticos que no están respaldados y extender rápidamente las políticas de respaldo para cubrirlos, mejorando la seguridad y reduciendo el riesgo.

Otros beneficios operativos clave incluyen:

- Frecuencia optimizada de copias de seguridad y retención en función de la criticidad de los datos dentro de los almacenes de datos respaldados por Cohesity.
- Restauración priorizada de datos basada en la criticidad comercial de los datos.
- Respuesta a incidentes optimizada a través del análisis “justo a tiempo” de los datos afectados (se explora más en la función de respuesta).

Juntos, DSPM y la plataforma de seguridad de datos impulsada por IA de Cohesity ayudan a mejorar su postura de seguridad en entornos multinube.

2.

Identificar los riesgos de resiliencia cibernética

Identificar mejoras para la respuesta a incidentes futuros y las actividades de BC/DR.

Evalúe las capacidades actuales de respuesta y recuperación de su organización y trace un camino hacia las mejores prácticas de la industria con el **Modelo de Madurez de Resiliencia ante Ataque Cibernético Destructivo (Destructive Cyberattack Resilience Maturity Model, DCARMM).**

Desarrollado por Cohesity, este modelo se alinea con marcos líderes como el Proceso de Respuesta a Incidentes de 6 pasos de SANS, RE&CT, MITRE D3FEND y NIST SP 800-61, lo que permite a las organizaciones:

- Evaluar la preparación para ataques cibernéticos destructivos.
- Comparar la madurez de la resiliencia con los pares de la industria o los estándares regionales.
- Identificar las brechas y crear una hoja de ruta para la mejora continua.

Su organización puede usarlo como una herramienta estratégica para fortalecer su postura de resiliencia cibernética y guiar la inversión en personas, procesos y tecnología.

Identifique las áreas que necesitan mejorar en su programa de resiliencia cibernética invirtiendo en evaluaciones de terceros.

Los servicios de consultoría de resiliencia cibernética del equipo de respuesta a eventos cibernéticos (CERT) de Cohesity ofrecen interacciones proactivas dirigidas por expertos diseñadas para fortalecer su resiliencia cibernética antes de que ocurra el próximo incidente. Desde evaluaciones de resiliencia en profundidad basadas en el DCARMM hasta planes de acción personalizados, el CERT le ayuda a identificar brechas, reducir riesgos y construir defensas duraderas.

3.

Proteger los datos empresariales a escala

A medida que los entornos de datos se vuelven más complejos, impulsados por el tamaño y la diversidad de los activos de datos, también aumenta el riesgo de un impacto empresarial grave por un ciberataque o una interrupción de datos.

El uso de una plataforma única y segura para respaldar todas sus fuentes de datos en entornos locales, en la nube y SaaS le permite escalar la protección de datos y, al mismo tiempo, minimizar significativamente el impacto de los posibles ataques.

Reduzca su superficie de ataque

Muchos entornos están diseñados con soluciones puntuales fragmentadas. Por el contrario, Cohesity consolida todos los componentes de respaldo y recuperación en una única plataforma global. Incluye la eliminación de datos duplicados global de longitud variable en todas las fuentes de datos y compresión para reducir aún más las superficies de ataque.

Escale la protección de datos en todos los entornos de datos

Debido a que Cohesity Data Cloud está basada en una arquitectura de hiperescala, los administradores de TI pueden aumentar el tamaño de sus clústeres de Cohesity de manera ilimitada y almacenar instantáneas y clones ilimitados sin ningún impacto en el rendimiento. La eliminación de datos duplicados sin precedentes no solo garantiza que pueda almacenar más datos a un costo mucho menor, sino que también puede crear instantáneas en cualquier momento para respaldar investigaciones forenses.

3.

Proteger los datos empresariales a escala

Proteger las copias de seguridad de los ataques

Utilizando los principios de Zero Trust, Cohesity ha adoptado un enfoque de seguridad multicapa que minimiza el riesgo de ransomware dirigido a las copias de seguridad y el riesgo de eliminación de datos inadvertida o maliciosa.

- **Instantáneas de estado de solo lectura inmutables**
  Cohesity Data Cloud está diseñado específicamente para frustrar los ciberataques al almacenar instantáneas de copia de seguridad en un estado inmutable. Las instantáneas no están montadas para aplicaciones externas, y las modificaciones o eliminaciones de instantáneas de copia de seguridad inmutables están deshabilitadas sin aprobación.
- **Políticas de DataLock** – Nuestras capacidades de escribir una vez, leer muchas (write-once-read-many, WORM) para la copia de seguridad permiten que ciertos roles establezcan políticas de DataLock inalterables en trabajos seleccionados.
- **Autenticación multifactor (MFA)**
  Cualquier persona que acceda a una copia de seguridad de Cohesity debe autenticarse utilizando dos formas de verificación. Admitimos múltiples proveedores de autenticación, de modo que su organización pueda mantener una autenticación sólida incluso si el servidor principal se ve afectado por un incidente cibernético.
- **Cifrado de datos** – Cohesity cuenta con cifrado estándar AES-256 validado por FIPS, basado en software, para datos en tránsito y en reposo.
- **Control de acceso basado en roles y privilegio mínimo**
  Cohesity reduce el riesgo de acceso no autorizado al permitir que el personal de TI otorgue a cada persona un nivel mínimo de acceso a los datos necesarios para realizar un trabajo en particular.
- **Separación de funciones** – Con Cohesity Quorum, cualquier cambio crítico del sistema o de nivel raíz debe ser autorizado por dos o más personas para proteger los datos de amenazas internas y credenciales robadas.

Aislar datos empresariales críticos

Puede replicar automáticamente los datos en otro clúster de Cohesity inmutable en las instalaciones o en la nube pública para garantizar que siempre esté disponible una copia inmutable adicional de los datos.

Probar copias de seguridad y restauraciones

Mediante la **orquestación de recuperación cibernética**, puede generar plantillas personalizables que automaticen los flujos de trabajo de recuperación y permitan pruebas rigurosas en entornos no productivos. De esta manera, su organización puede prepararse mejor para los incidentes cibernéticos y optimizar la recuperación para reducir el tiempo de inactividad y la pérdida de datos.

4.

Detectar posibles ataques cibernéticos y compromisos

Los ciberdelincuentes no se detendrán ante nada para encontrar y explotar cualquier vulnerabilidad en su entorno de datos. La detección temprana de cambios anormales en los datos de respaldo o en el comportamiento del usuario es esencial para minimizar el impacto de un ataque.

Aquí es donde la IA juega un papel fundamental: identificar patrones sutiles de actividad de datos que pueden pasar desapercibidos para los seres humanos. Y al capturar automáticamente instantáneas de copia de seguridad de datos críticos al inicio de un ataque de ransomware –detectado por herramientas EDR/XDR–, puede reducir la pérdida de datos y acelerar la recuperación.

Detectar cifrado de ransomware, ataques wiper e infiltrados maliciosos.

Monitoree, modele y optimice proactivamente las operaciones utilizando análisis predictivos para evaluar tendencias. Nuestro algoritmo basado en IA establece patrones y escanea continuamente en busca de anomalías en los datos a través de las instantáneas a lo largo del tiempo.

La detección de anomalías acelera la corrección al enviar una notificación a sus administradores de TI, así como al equipo de soporte de Cohesity.

Esto proporciona a los equipos de seguridad información sobre el comportamiento que podría indicar un ataque de ransomware o de borrado, o incluso la presencia de un infiltrado malicioso.

Estas alertas también pueden compartirse con su Centro de Operaciones de Seguridad utilizando sus herramientas de correlación de eventos (p. ej., SIEM).

Busque proactivamente amenazas en los datos de respaldo.

El ransomware y otros ataques utilizan tácticas engañosas para ocultar el malware. La búsqueda de amenazas de Cohesity le ayuda a encontrar amenazas esquivas mediante la detección de amenazas impulsada por IA, que identifica las últimas variantes de ransomware y otros ciberataques.

Nuestra extensa biblioteca de patrones de comportamiento se actualiza con frecuencia con las últimas amenazas.

También admitimos fuentes comerciales de inteligencia de amenazas, como CrowdStrike Falcon Adversary Intelligence, e incorporamos cualquier IOC en formato YARA de otras fuentes de terceros.

4.

Detectar posibles ataques cibernéticos y compromisos

Envíe detecciones de seguridad a herramientas de SOC para su correlación.

Envíe las detecciones de seguridad críticas —como los IOC, las anomalías en los cambios en los datos de copia de seguridad y las alertas de datos confidenciales— a sus herramientas del SOC (p. ej., SIEM, SOAR) para permitir una detección y respuesta rápidas ante amenazas.

Cohesity se integra con plataformas líderes como CrowdStrike, Splunk y Microsoft para compartir telemetría sin problemas, de modo que su SOC pueda agregar, analizar y correlacionar la información de Cohesity con datos de registro de alto volumen de toda su infraestructura.

El resultado: una vista unificada en tiempo real que mejora la visibilidad y acelera la detección de posibles ataques de ransomware u otras amenazas cibernéticas.

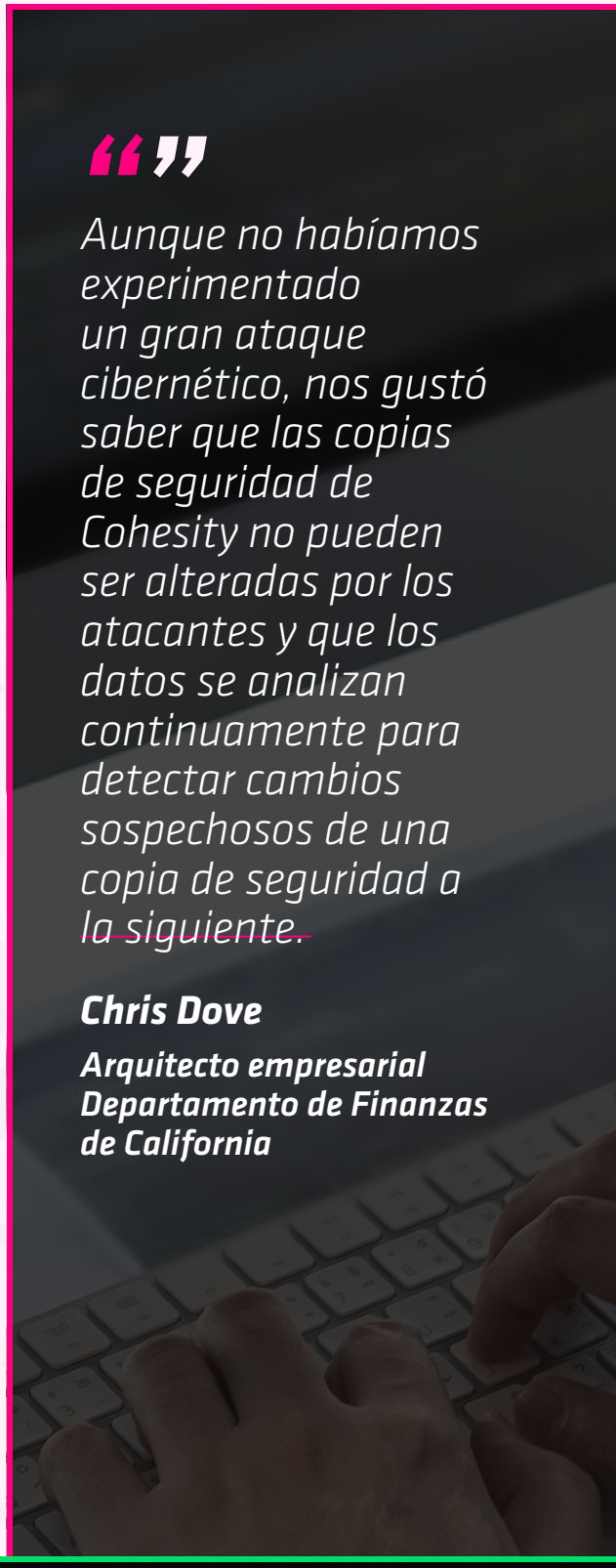
Capture más artefactos forenses y active instantáneas incrementales basadas en señales EDR/XDR.

La integración entre Cohesity Data Cloud y Cisco XDR le permite automatizar la copia de seguridad de datos críticos en el momento en que Cisco XDR detecta un ataque de ransomware, lo que reduce los objetivos de punto de recuperación (recovery point objectives, RPO) y minimiza la interrupción del negocio.

Estas instantáneas de copia de seguridad también proporcionan al personal de respuesta a incidentes un contexto más detallado de los cambios en el sistema de archivos, lo que hace que las investigaciones forenses sean más rápidas y eficaces.

Identificar malware en servidores NAS.

Además de monitorear las tasas de cambio de los datos de copia de seguridad para detectar posibles ataques de ransomware, Cohesity detecta y alerta de forma exclusiva sobre anomalías a nivel de archivo dentro de archivos no estructurados y datos de objetos.



> *"Aunque no habíamos experimentado un gran ataque cibernético, nos gustó saber que las copias de seguridad de Cohesity no pueden ser alteradas por los atacantes y que los datos se analizan continuamente para detectar cambios sospechosos de una copia de seguridad a la siguiente.*
>
> ***Chris Dove***
> ***Arquitecto empresarial***
> ***Departamento de Finanzas de California***

5.

Responder rápidamente a incidentes cibernéticos

Una vez detectado un incidente cibernético, la organización debe actuar rápidamente para contener el incidente, investigar su alcance y mitigar los riesgos para permitir una recuperación segura.

Los incidentes de alto impacto, como el ransomware y los ataques wiper, pueden interrumpir los sistemas necesarios para entregar productos y servicios a los clientes, y los sistemas internos de TI críticos para gestionarlos. Estos escenarios requieren un flujo de trabajo diferente y más estructurado que va más allá de los protocolos estándar de violación de datos.

Apresurar la recuperación sin investigar y mitigar la amenaza puede dejar las vulnerabilidades subyacentes sin resolver, lo que pone en riesgo la reinfección y un tiempo de inactividad prolongado.

La recuperación segura de dichos ataques requiere comprender cómo ocurrió el incidente y cómo remediar sus causas raíz. Este enfoque disciplinado es la esencia de todo marco de respuesta a incidentes de ciberseguridad basado en las mejores prácticas.

1. **Involucre al CERT de Cohesity** al principio del proceso de respuesta ante incidentes para obtener asistencia rápida y experta. Nuestro equipo ayuda a contener la amenaza, minimizar el tiempo de inactividad, asistir con el análisis forense de la infraestructura de respaldo, respaldar el cumplimiento normativo y los requisitos de notificación de violaciones de seguridad, y facilitar la recuperación segura a producción.

2. **Restaure las herramientas de respuesta a un estado confiable y proporcione acceso rápido.** Cuando un ciberataque golpea—y su negocio se interrumpe—no hay tiempo que perder. La respuesta rápida es fundamental y un **digital jump bag**™ le ayuda a actuar de inmediato.

   Idealmente preparada antes de un incidente, el kit digital de emergencia es un repositorio protegido y confiable que proporciona acceso rápido a las herramientas, software, archivos de configuración y documentación necesarios para iniciar una respuesta efectiva. Almacenado en una ubicación inmutable en una bóveda más allá del alcance de los adversarios, es la base de toda la solución Cohesity Clean Room, que apoya las etapas críticas de la respuesta a incidentes y permite una recuperación segura y con confianza.

3. **Restaure la infraestructura limpia de Active Directory (AD).** Pocos sistemas son más críticos para el negocio—o más atacados—que AD. Al comienzo de la respuesta a incidentes, es imperativo investigar y limpiar a fondo su entorno de AD antes de volver a poner otras herramientas de respuesta en línea y, ciertamente, antes de restaurar AD en producción. Omitir este paso deja la puerta abierta para que los atacantes vuelvan a entrar, socaven los esfuerzos de recuperación y prolonguen la interrupción del negocio.

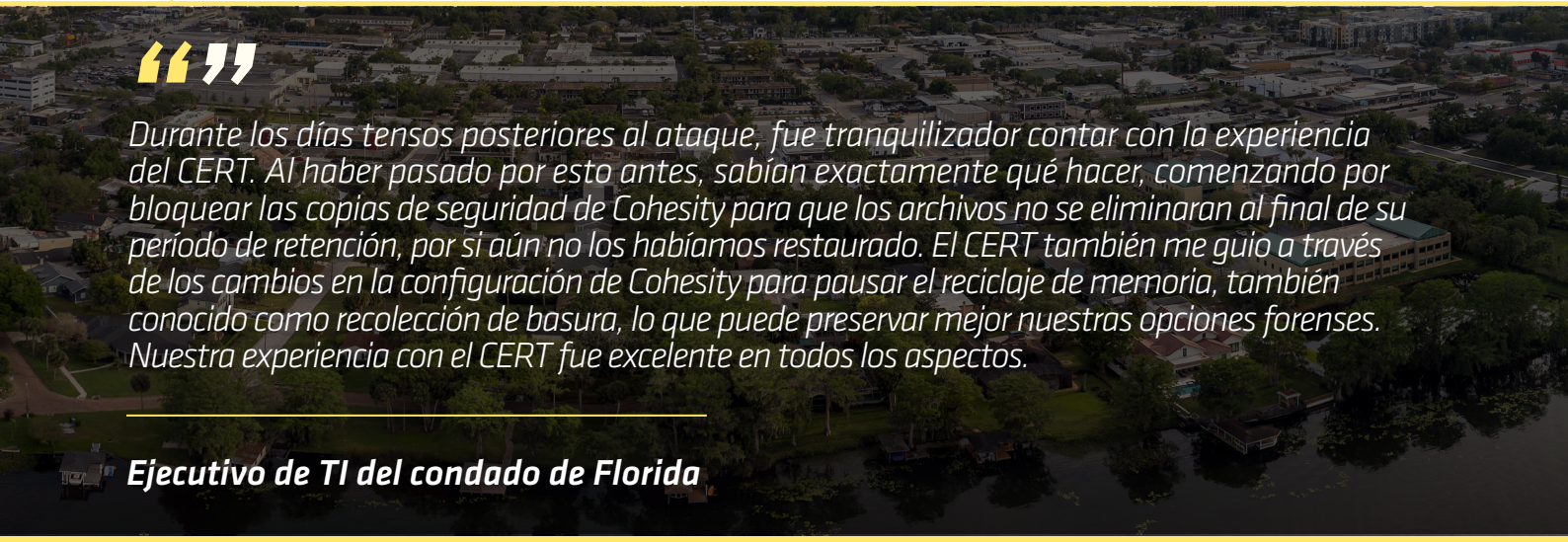
   Con **Cohesity Identity Resilience con tecnología de Semperis**, puede restaurar AD a un estado confiable hasta un 90 % más rápido.

5.

Responder rápidamente a incidentes cibernéticos

4. **Establecer rápidamente una sala limpia para la respuesta y la recuperación.** Se debe implementar una sala limpia como un entorno de confianza donde los analistas e investigadores realicen investigaciones forenses, comprendan las vulnerabilidades explotadas en el ataque y garanticen que los datos infectados no se vuelvan a introducir en entornos de producción.

5. **Buscar pasivamente artefactos para identificar otros sistemas afectados.** Nuestra capacidad de búsqueda de amenazas detecta los IOC en toda la infraestructura de su organización, incluso cuando los sistemas están aislados para su contención. Esta capacidad es resistente a las técnicas comunes de evasión de defensa que pueden cegar o retrasar la detección mediante herramientas tradicionales de seguridad de punto final.



> *"Durante los días tensos posteriores al ataque, fue tranquilizador contar con la experiencia del CERT. Al haber pasado por esto antes, sabían exactamente qué hacer, comenzando por bloquear las copias de seguridad de Cohesity para que los archivos no se eliminaran al final de su período de retención, por si aún no los habíamos restaurado. El CERT también me guio a través de los cambios en la configuración de Cohesity para pausar el reciclaje de memoria, también conocido como recolección de basura, lo que puede preservar mejor nuestras opciones forenses. Nuestra experiencia con el CERT fue excelente en todos los aspectos.*
>
> ***Ejecutivo de TI del condado de Florida***

6. **Hacer un análisis forense de los sistemas de archivos históricos.** Nuestra protección de datos permite el acceso a una serie completa de instantáneas inmutables a través de la interfaz de usuario y la API, para que los equipos de respuesta puedan realizar investigaciones forenses detalladas a nivel de archivo en los datos de copia de seguridad retenidos.

7. **Comprender las vulnerabilidades históricas que se explotaron en el ataque.** Con la solución Cohesity CyberScan, puede escanear instantáneas de copia de seguridad para detectar vulnerabilidades conocidas. Esto permite que los equipos de seguridad identifiquen vulnerabilidades durante un ataque, incluso si un sistema es inaccesible debido a la contención, ha sido borrado o si un adversario implementó parches después de una intrusión.

8. **Ayudar a cumplir con las obligaciones regulatorias y de cumplimiento para notificar a los reguladores, socios y titulares de datos afectados.** Nuestra clasificación de datos impulsada por IA escanea las copias de seguridad para identificar datos confidenciales y regulados, lo que ayuda a las organizaciones a cumplir con los requisitos normativos, incluso en ataques cibernéticos destructivos donde se cifran o eliminan los almacenes de datos críticos. También ayudamos a restaurar las capacidades de comunicación necesarias para la gestión de incidentes como parte de la solución Cohesity Clean Room. Las plantillas de comunicación para notificar a las partes interesadas se pueden guardar en el maletín digital de respuesta para un acceso rápido.

6.

Recuperar sistemas y datos de manera segura

La fase de recuperación de la respuesta a incidentes debe respaldar la erradicación exhaustiva de las amenazas, evitar la reinfección y reducir la probabilidad de ataques futuros similares.

La solución Cohesity Clean Room le brinda la flexibilidad de elegir su estrategia de recuperación preferida, ya sea recuperando y limpiando los sistemas existentes o reconstruyendo desde cero.

Admite una rápida recuperación de volúmenes, lo que permite recuperar todo un sistema de archivos antes de aplicar mitigaciones para erradicar amenazas. También permite reconstrucciones rápidas a partir de imágenes de software confiables y configuraciones conocidas.

Nuestra organización sufrió un ataque crítico de ransomware, lo que paralizó de manera efectiva toda nuestra infraestructura. Con Cohesity, hemos podido recuperar máquinas y recursos compartidos de archivos, verificar que estén limpios y volver a poner las aplicaciones en línea.

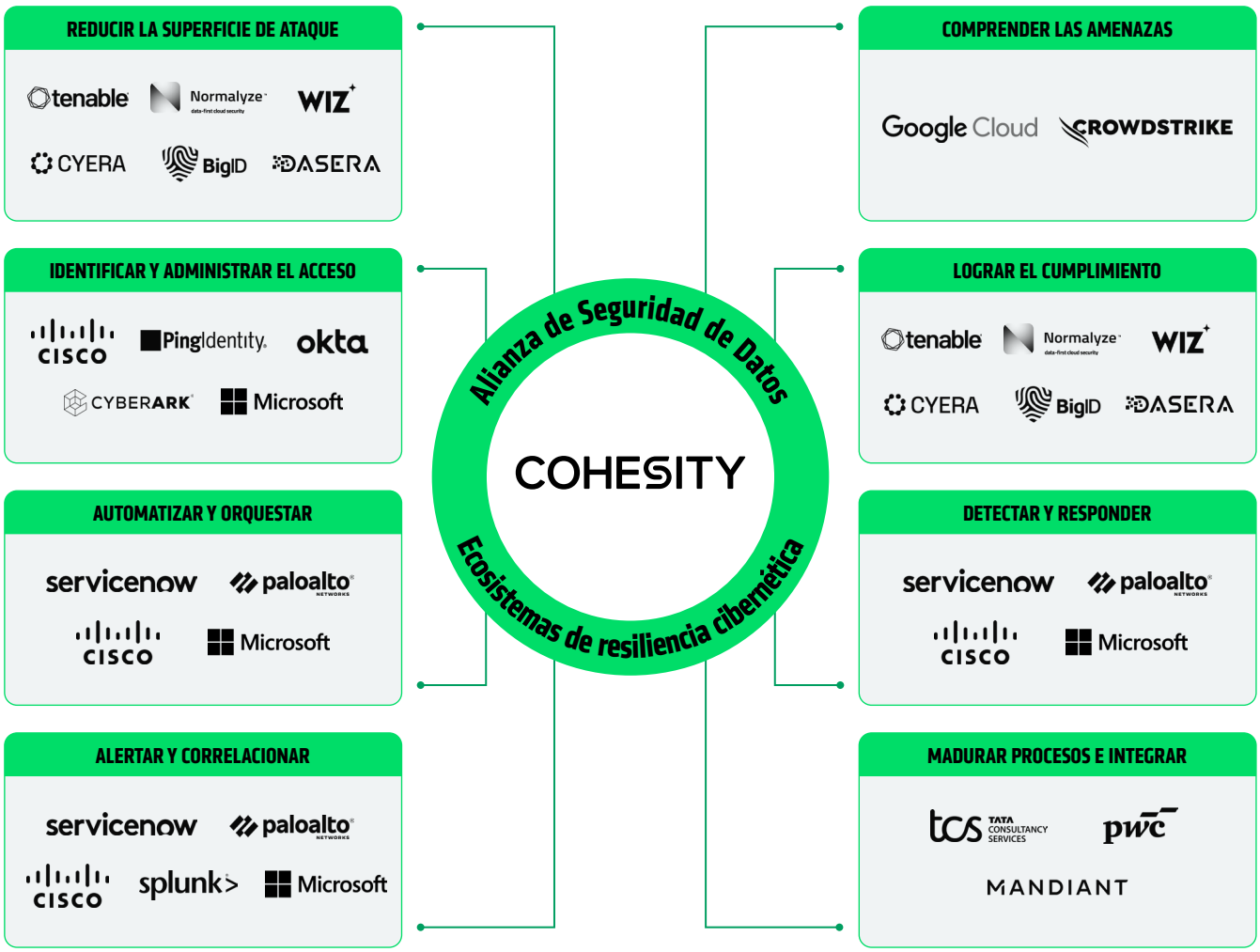
Cohesity nos ha ahorrado literalmente cientos de horas de trabajo, y diría que nos evitó tener que pagar realmente la nota de rescate. Todos todavía tenemos empleos y la comunidad tiene un hospital funcional porque hemos tenido mucho éxito con Cohesity.

Sam Stewart
Analista de sistemas de red de Sky Lakes Medical Center

FORTALECER LA RESILIENCIA CIBERNÉTICA A TRAVÉS DE ALIANZAS

La resiliencia cibernética es un deporte de equipo. Ninguna solución de un solo proveedor puede investigar y remediar un incidente en su totalidad.

Es por eso que establecimos la Data Security Alliance, un ecosistema de empresas líderes en seguridad y recuperación cibernética que le ayuda a reducir los riesgos de recuperación cibernética, aumentar la eficiencia de su Centro de Operaciones de Seguridad y proteger más de su entorno de datos utilizando herramientas que ya tiene.



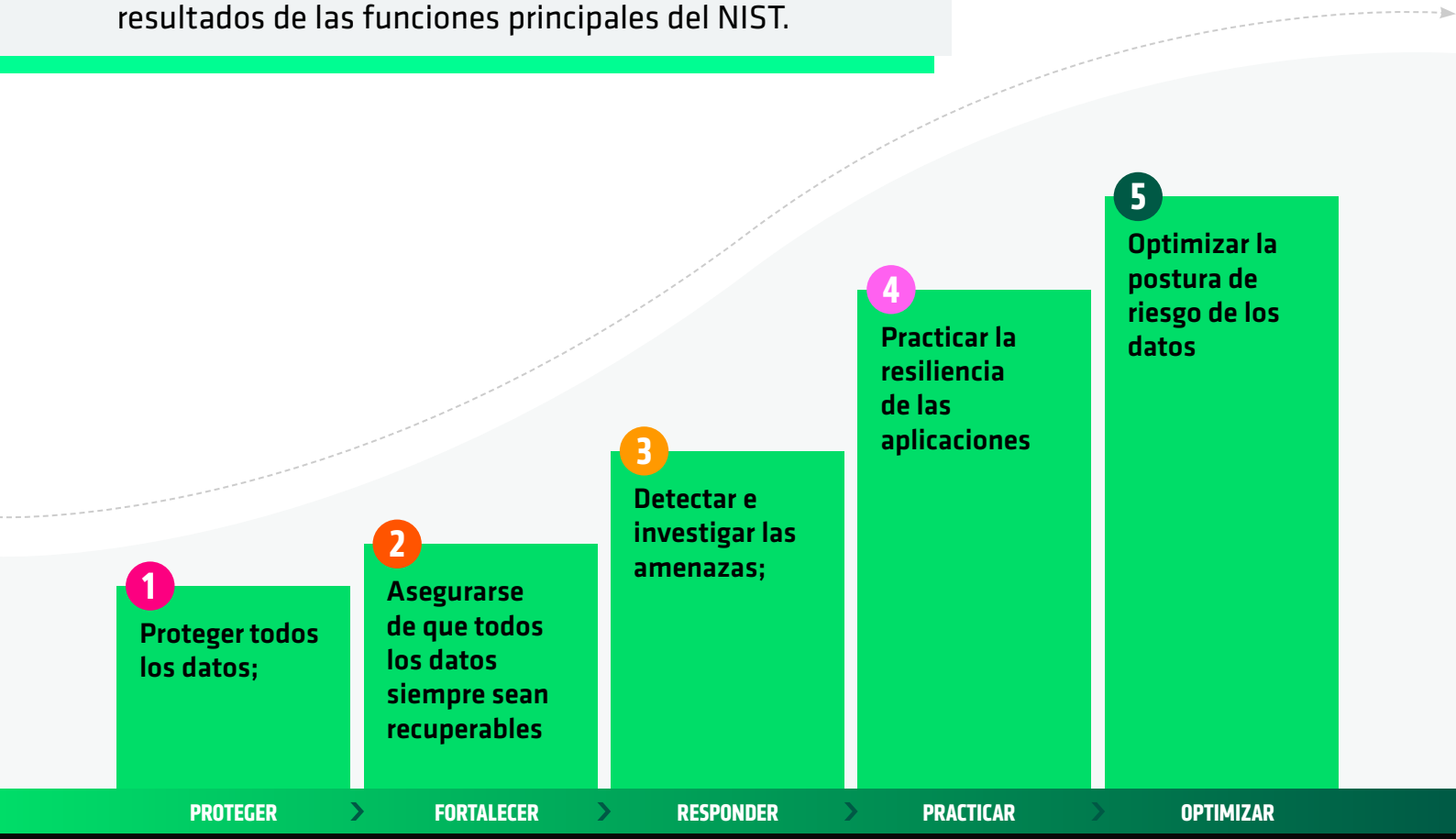
SIGUIENTES PASOS

PARA SU ORGANIZACIÓN...

Los 5 pasos de Cohesity hacia la resiliencia cibernética

Ha explorado las seis claves para construir un negocio con resiliencia cibernética y cómo apoyamos cada etapa del Marco de Ciberseguridad (Cybersecurity Framework, CSF) del NIST. Ahora es el momento de poner esas perspectivas en acción.

Para ayudarle a comenzar, hemos desarrollado un **manual de estrategias de resiliencia cibernética de cinco pasos** alineado con las mejores prácticas de la industria para la respuesta cibernética y la recuperación. Es una guía práctica que le muestra cómo implementar acciones concretas y repetibles utilizando la nube de datos y los servicios de Cohesity. Cada paso le ayuda a lograr los resultados de las funciones principales del NIST.



Los ***5 pasos*** de Cohesity hacia la resiliencia cibernética

1. PROTEGER TODOS LOS DATOS

Alineación con el CSF del NIST: ***Proteger***

Desarrolle resiliencia protegiendo los datos dondequiera que residan, a escala empresarial. Cohesity Data Cloud admite **más de 1000 fuentes de datos**, incluidas máquinas virtuales, aplicaciones SaaS, bases de datos y entornos NAS, a la vez que reduce el costo y el riesgo mediante la eliminación de datos duplicados y compresión globales.

Este enfoque reduce los costos de almacenamiento para TI y reduce la superficie de ataque para los equipos de seguridad: dos factores críticos para una función de protección más sólida.

2. ASEGÚRESE DE QUE LOS DATOS SEAN RECUPERABLES

Alineación con el CSF del NIST: ***Proteger y recuperar***

La protección es tan sólida como su capacidad para recuperar.

- **Refuerce su plataforma:** Habilite defensas como MFA, control de acceso basado en roles y Quorum para hacer cumplir la separación de funciones y minimizar el riesgo interno.
- **Aísle datos críticos:** Cree copias seguras y recuperables con la bóveda cibernética de Cohesity, disponible como una bóveda en la nube administrada por Cohesity o una solución autoadministrada.

Estos pasos garantizan que pueda restaurar copias confiables cuando más importa.

3. DETECTE E INVESTIGUE AMENAZAS

Alineación con el CSF del NIST: ***Identificar y detectar***

La resiliencia depende de la detección temprana. Con Cohesity, usted puede:

- **Identificar vulnerabilidades**, incluidas brechas en la protección de datos.
- **Escanear continuamente las copias de seguridad** para detectar indicadores de ransomware y malware.
- **Buscar amenazas específicas** en los datos de respaldo para ser inmune a las técnicas de evasión.
- **Enviar los hallazgos** a sus herramientas SIEM/SOAR para una rápida correlación y respuesta del SOC.

El resultado: Las amenazas se detectan antes y los equipos de respuesta actúan más rápido.

4. PRACTIQUE LA RESILIENCIA DE LAS APLICACIONES

Alineación con el CSF del NIST: ***Responder y recuperar***

Descubra el paso final >

No espere a que ocurra un ataque para probar su plan de recuperación.

- **Ensaye periódicamente:** Practique sus planes de recuperación como si estuviera bajo ataque para validar sus procesos de recuperación y su preparación.
- **Automatice la recuperación:** Utilice la orquestación de recuperación de nuestra plataforma para optimizar los flujos de trabajo y acelerar la restauración del sistema después de un incidente.

Este paso transforma la recuperación de un proceso manual y estresante a una guía repetible y bien practicada.

Los ***5 pasos*** de Cohesity hacia la resiliencia cibernética

5. OPTIMIZAR LA POSTURA DE RIESGO DE LOS DATOS

Alineación con el CSF del NIST: ***Gobernar, identificar y responder***

- **Fortalezca la gobernanza de la seguridad de los datos:** Utilice sus datos de Cohesity y nuestras capacidades de clasificación de datos para comprender qué datos tiene, evaluar su nivel de riesgo y aplicar los controles de seguridad adecuados.
- **Identifique los sistemas críticos que no están respaldados:** Identifique datos confidenciales en todo su entorno —incluidas las copias de seguridad— y asegúrese de que estén protegidos adecuadamente. Puede agilizar este proceso combinando las capacidades de su herramienta preferida de Gestión de la postura de seguridad de datos (DSPM) y nuestra plataforma.
- **Evalúe el impacto del incidente:** Si se produce una violación, y especialmente si sus almacenes de datos críticos son cifrados o borrados, puede usar sus copias de seguridad para evaluar rápidamente qué datos confidenciales y regulados pueden haber estado expuestos, para que pueda cumplir con las obligaciones regulatorias y de cumplimiento para notificar a los reguladores, socios y titulares de los datos afectados.

Vea la resiliencia cibernética en acción

Descubra cómo 7 organizaciones de todas las industrias se recuperaron de manera rápida y segura después de ataques de ransomware.

OBTENGA EL LIBRO ELECTRÓNICO

INTEGRARLO TODO

En conjunto, nuestro manual de estrategias de resiliencia cibernética de cinco pasos le brinda un camino claro y práctico para poner en funcionamiento el CSF del NIST.

Con la moderna plataforma de seguridad de datos de Cohesity, no solo puede proteger y recuperar, sino también optimizar continuamente su postura de resiliencia cibernética.

OBTENGA MÁS INFORMACIÓN SOBRE NUESTRAS SOLUCIONES DE RESILIENCIA CIBERNÉTICA

COHESITY
RESILIENCE EVERYWHERE

6100008-006-EN 11-2025