eBOOK

Guía de Preparación para la Ciberrecuperación

CONOCE CÓMO MANTENER LA RESILIENCIA FRENTE A LOS DESAFÍOS.

Commvault®

CONTENIDO

Muchas organizaciones han considerado que la ciberrecuperación y la recuperación ante desastres son lo mismo. Sin embargo, la ciberrecuperación a partir de incidentes recientes ha revelado algunos desafíos únicos en comparación con la recuperación ante desastres habituales. La variabilidad en las tácticas, técnicas y procedimientos de los atacantes ha demostrado que los planes de ciberrecuperación deben considerar:

- **Imprevisibilidad y amenazas en evolución:** a diferencia de un desastre natural, los ciberataques son maliciosos y los atacantes han tomado medidas extremas para ocultar sus acciones y movimientos. Debido a esto, puede ser difícil determinar exactamente cuándo comenzó el ataque, qué sistemas están afectados o el alcance total del daño.
- **Ataques secundarios:** se ha observado que los atacantes implantan código para lanzar ataques secundarios durante el proceso de recuperación o crean puertas traseras persistentes que se abren automáticamente al realizar una restauración.
- **Copias de seguridad comprometidas:** en algunos casos, los atacantes han dirigido sus esfuerzos específicamente hacia las copias de seguridad para asegurarse de que los esfuerzos de recuperación sean ineficaces. Esto hace que la necesidad de pagar un rescate para recuperar los datos de producción sea más real.
- **Restricciones de tiempo:** las empresas a menudo se enfrentan a una presión enorme para volver a estar operativas rápidamente después de un ciberataque. Se ha demostrado que el tiempo de inactividad puede costar a una empresa hasta $14.056 por minuto. Y lo peor es que apresurar la recuperación puede llevar a restaurar sistemas ya comprometidos, lo que amplifica aún más el daño.
- **Drenaje de recursos:** la ciberrecuperación puede ser un proceso intensivo en recursos, que requiere la experiencia de equipos de TI, seguridad, legal y, potencialmente, incluso de las fuerzas del orden. Esto puede agotar los recursos ya escasos de una empresa y distraer a los equipos de seguridad y operaciones de otras posibles amenazas cibernéticas.

Al comprender estos desafíos, las organizaciones pueden utilizar algunos elementos fundamentales de la recuperación ante desastres para construir un plan de ciberrecuperación que anticipe estas dificultades y les ayude a reponerse de un ataque de manera más efectiva.

Esta guía te ayudará a sentar las bases para la preparación de la ciberrecuperación de tu organización, proporcionándote los conceptos, ideas y procesos necesarios para establecer tu propio programa, todo mientras te alineas con algunos marcos comúnmente observados.

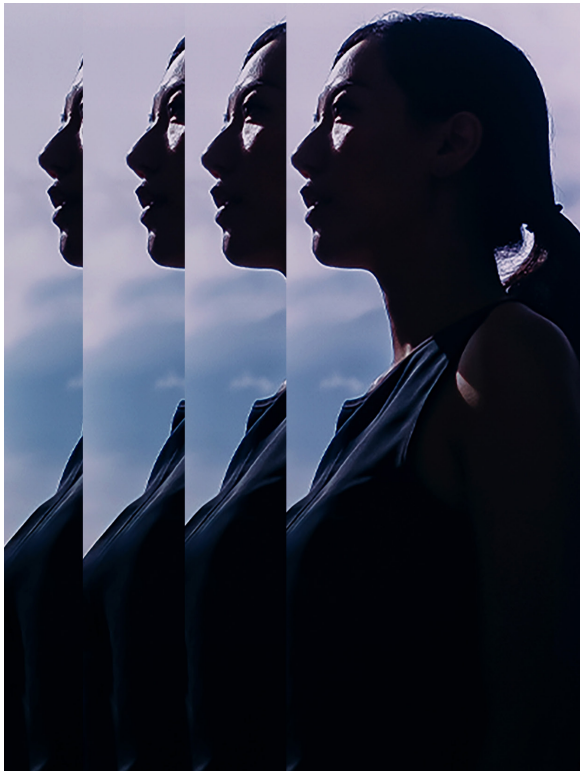
[1] Enterprise Management Associates, "IT outages: 2024 costs and containment," Valerie O'Connell, Research Director, April 2024.

MARCO DE CIBERSEGURIDAD NIST COMO GUÍA

El Marco de Ciberseguridad del Instituto Nacional de Estándares y Tecnología (NIST CSF) ha sido durante mucho tiempo una guía esencial para los equipos de seguridad a la hora de construir y alinear sus programas de seguridad y defenderse contra nuevas y evolutivas amenazas cibernéticas.

Utiliza el marco Identify, Detect, Protect, Respond y Recover para explicar cómo fortalecer cada uno de estos aspectos para una ciberrecuperación exitosa.

1. **Identificar (Identify).** Comprende tus datos, incluyendo los datos sensibles o críticos, dónde se encuentran y quién es responsable de ellos.
2. **Detectar (Detect).** Utiliza controles de seguridad y tecnología para observar lo que está sucediendo en tu entorno y con tus datos.
3. **Proteger (Protect).** Implementa mecanismos para bloquear tus datos sensibles o críticos y prepáralos para la recuperación.
4. **Responder (Respond)**. Elimina al atacante de tu entorno y borra o aísla el vector de ataque utilizado para infiltrarse en tu organización. Si esto no se puede hacer rápidamente, prepara un nuevo espacio de trabajo limpio y no comprometido para restaurar y utilizar con el fin de continuar con las operaciones.
5. **Recuperar (Recover)**. Reconstruye una versión no comprometida de todo tu entorno, incluyendo los datos, aplicaciones e infraestructura.



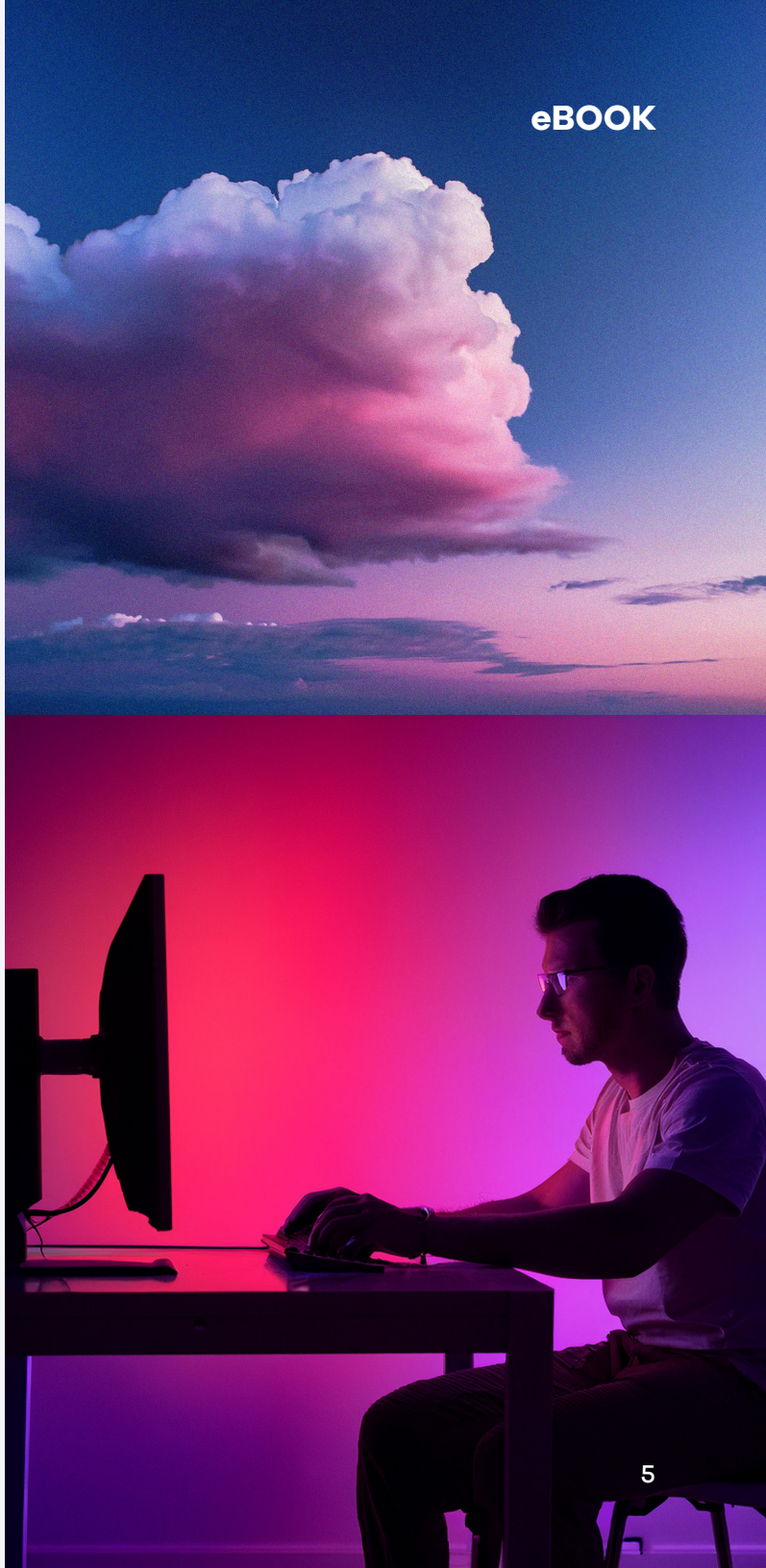
PREPARÁNDOTE PARA LO INESPERADO

Por su propia naturaleza, los incidentes cibernéticos son a menudo ataques encubiertos orquestados durante días o semanas antes de que se produzca la destrucción o el caos. Estudios han demostrado que el tiempo promedio de residencia (dwell time).

> ## 194 días, o más de seis meses
> **es el tiempo que un atacante ha estado realmente dentro de una organización durante un ataque**[1]

Las organizaciones han realizado pruebas de penetración durante mucho tiempo para destacar las áreas en las que sus defensas son débiles y han ejecutado ejercicios para probar la recuperación ante desastres. Sin embargo, dada la variabilidad de los ciberataques, la práctica debe tener en cuenta que, en un escenario real de ciberrecuperación, no se puede confiar implícitamente en casi nada.

Las copias de seguridad deben ser escaneadas en busca de malware persistente. La infraestructura debe ser limpiada para confirmar que solo están presentes los usuarios autorizados. Y las aplicaciones y los datos deben ser verificados para detectar puertas traseras y restaurados a un estado previo al ataque (o a la infiltración).



[1] Cost of a Data Breach Report 2024, IBM.

VIABILIDAD MÍNIMA: EL PRIMER PASO HACIA LA CIBERRECUPERACIÓN

Una vez que tu empresa ha sido golpeada por un ciberataque, estás bajo una presión inmensa para volver a la normalidad lo antes posible. ¿La mejor manera de reanudar las operaciones rápidamente? Restaura hasta la viabilidad mínima —los activos más críticos que necesitas para mantener la continuidad de las operaciones. De esta manera, puedes seguir llevando a cabo los aspectos más vitales de tu organización mientras se realiza una restauración completa.

Una vez que identifiques tus sistemas, procesos y datos más críticos que te permitirán volver a la viabilidad mínima, necesitarás elaborar un plan para restaurarlos en caso de un incidente. Es fundamental que comprendas el impacto del tiempo de inactividad y que pruebes y actualices tu plan según sea necesario.

Lee la guía definitiva sobre viabilidad mínima para conocer más sobre los pasos para restaurar tus operaciones de negocio y nuestras prácticas recomendadas..

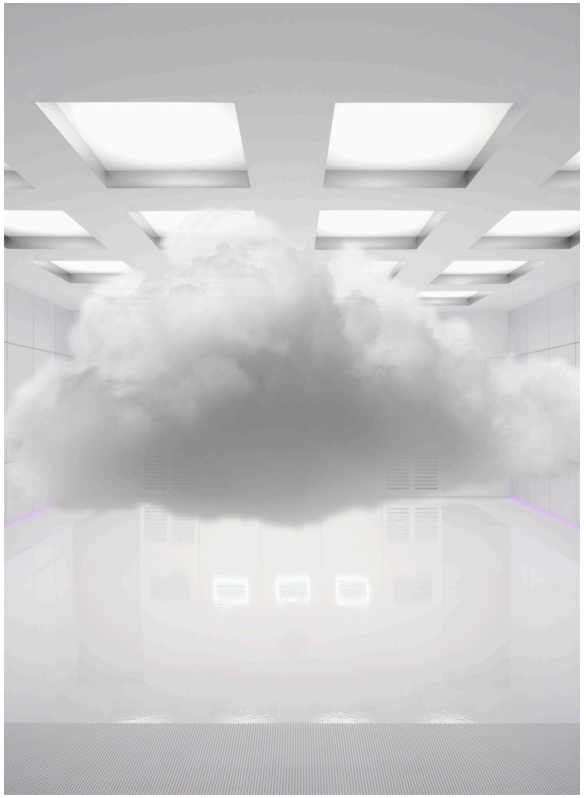
LA CIBERRECUPERACIÓN MÁS RÁPIDA Y COMPLETA

Commvault ofrece soluciones para proteger, probar y recuperar tsus datos, aplicaciones y cargas de trabajo, brindando proporcionando una recuperación integral y una verdadera ciberresiliencia.

Commvault® Cloud Cleanroom™ Recovery te permite probar y recuperar en un entorno seguro, a demanda, basado en la nube. Puedes recuperar fácilmente aplicaciones y datos, y realizar análisis forenses después de un evento. Contarás con un entorno de recuperación aislado para la continuidad del negocio en caso de un ataque.

Commvault Cloud Rewind™ permite una recuperación casi instantánea y escribe automáticamente el código necesario para recuperar datos y reconstruir aplicaciones, lo que te permite volver a operar en minutos después de una brecha, sin necesidad de intervención manual.

Commvault Cloud for Active Directory Enterprise Edition ofrece una recuperación rápida para entornos de AD y Entra ID. Ayuda a automatizar y orquestar la recuperación de ADs a nivel de bosque después de un incidente, lo que te permite volver a un estado de viabilidad mínima rápidamente.



eBOOK

Una certeza en la ciberseguridad: los actores malintencionados seguirán innovando para encontrar vulnerabilidades. Mantente un paso adelante con un plan y estrategia de ciberrecuperación bien pensados para proteger tus activos y mantener la continuidad del negocio frente a amenazas.

Conoce más: **www.commvault.com/minimum-viability**

commvault.com | 888.746.3849 | get-info@commvault.com

Commvault®