O'REILLY®
Report

La hora de la ciberresiliencia

Una nueva estrategia para sobrevivir ante el panorama de amenazas en la era de la IA agéntica

Govind Rangasamy

Commvault

Visit commvault.com

97 9 834 18 5 986 5

La hora de la ciberresiliencia

Una nueva estrategia para sobrevivir ante el panorama de amenazas en la era de la IA agéntica

Govind Rangasamy

O'REILLY®

La hora de la ciberresiliencia
por Govind Rangasamy

Publicado por O'Reilly Media, Inc., 141 Stony Circle, Suite 195, Santa Rosa, CA 95401.

Los libros de O'Reilly pueden adquirirse para uso educativo, comercial o promocional. También hay disponibles ediciones digitales para la mayoría de los títulos (https://oreilly.com). Para más información, comuníquese con nuestro departamento de ventas corporativas e institucionales: 800-998-9938 o corporate@oreilly.com.

Editora de adquisiciones: Simina Calin
Editor de desarrollo: Michele Cronin
Editor de producción: Jonathon Owen
Correctora de estilo: Paula L. Fleming
Diseño de portada: Susan Brown
Ilustración de portada: Ellie Volckhausen
Diseño de páginas: David Futato
Ilustración de páginas: Kate Dullea

Septiembre de 2025: Primera edición

Histórico de revisiones de la primera edición
2025-09-19: Primera edición

Este trabajo forma parte de una colaboración entre O'Reilly y Commvault. Consulte nuestra declaración de independencia editorial.

979-8-341-65986-5

[LSI]

Índice

Reconocimientos

Quisiera agradecer a Katherine Demacopoulos por su fantástico trabajo en todos los aspectos del libro, a Anna Griffin por reconocer su necesidad en el mercado y patrocinarlo, y a Chris DiRado por su experiencia y ayuda en materia de seguridad.

A mi esposa, Bhuvana, y a mis maravillosos hijos, Pranav y Sanjit: vosotros me recordáis cada día lo que de verdad importa. Vuestro amor, curiosidad, bromas y abrazos me han dado la alegría y la energía para seguir adelante.

CAPÍTULO 1

El ciberataque es inminente. ¿Podrás recuperarte con confianza?

El flujo vital de una organización corre a través de sus redes, aplicaciones y almacenes de datos. Estos sistemas vitales se enfrentan a amenazas crecientes a medida que los ciberataques se vuelven más frecuentes y sofisticados. Los ciberdelincuentes ya utilizan herramientas avanzadas potenciadas por IA, pero está surgiendo una amenaza aún más peligrosa: la IA agéntica (agentic AI), capaz de razonar, planificar y actuar de forma autónoma. Esta tecnología revolucionará las tácticas del cibercrimen, haciendo los ataques más escalables y eficientes.

A diferencia del ransomware tradicional, que basa su mecánica en guiones preprogramados, la IA de agentes puede adaptar su estrategia en tiempo real, aprendiendo de las respuestas defensivas y evolucionando sus ataques más rápido de lo que los defensores humanos pueden reaccionar.

Los incidentes de alto perfil demuestran que ningún sector ni región es inmune. Hemos visto ejemplos que van desde el envenenamiento de una planta de tratamiento de agua en Florida o el apagón durante 11 días del oleoducto de Colonial Pipeline hasta ataques de ransomware que paralizaron distritos escolares o el cifrado masivo de sistemas de hoteles y casinos.

Incluso las defensas perimetrales más sólidas y los programas más avanzados de inteligencia de amenazas —como el Financial Services Information Sharing and Analysis Center (FS-ISAC) o la US Cybersecurity & Infrastructure Security Agency (CISA)— son solo una parte del panorama. Los adversarios de hoy están bien financiados, son extremadamente pacientes y están enfocados en deshabilitar la capacidad de recuperación de sus objetivos.

Entendiendo el panorama de amenazas actual: la industrialización del cibercrimen

Hace apenas unos años, los ataques de ransomware estaban limitados a unos pocos grupos de hackers sofisticados. Hoy, las plataformas de ransomware como servicio (RaaS) están disponibles en la dark web para que cualquier criminal con habilidades moderadas las alquile. El modelo de negocio RaaS funciona como cualquier plataforma SaaS (Software as a Service) corporativa, ofreciendo suscripciones y esquemas de reparto de ingresos que hacen del cibercrimen algo accesible para cualquiera dispuesto a pagar.

Estas empresas criminales ofrecen acceso inmediato a marcos de extorsión listos para usar, con centros de llamadas de soporte a víctimas, asistencia para negociar rescates e incluso "garantías" de eliminación de datos si las víctimas se niegan a pagar. Este enfoque a escala industrial ha provocado una auténtica explosión de ataques. Los ciberdelincuentes ya no necesitan desarrollar su propio malware, simplemente tienen que elegir de un menú —LockBit, REvil, DarkSide, Conti, BlackCat y muchos más—.

Cada variante ofrece características específicas diseñadas para maximizar el daño y la ventaja. Las versiones modernas de ransomware exfiltran datos antes del cifrado para amenazar con la divulgación pública, apuntan sistemáticamente a destruir los sistemas de backup para eliminar opciones de recuperación y despliegan cargas útiles capaces de borrar redes o cuentas en la nube completas en minutos.

Ransomware con IA agéntica: cuando los ataques piensan, aprenden y se adaptan

La aparición de la IA agéntica marca un cambio fundamental respecto a las plataformas RaaS tradicionales. A diferencia de la IA generativa, que asiste en tareas específicas, la IA de agentes es proactiva y puede resolver problemas complejos y tomar decisiones de forma autónoma. Estos agentes de IA no se limitan a ejecutar ataques preprogramados; aprenden y adaptan sus estrategias según el entorno específico que encuentran.

Por ejemplo, en pruebas controladas, los investigadores de Unit 42 demostraron un ataque completo —desde la intrusión inicial hasta la exfiltración de datos— en solo 25 minutos. La diferencia de velocidad es abrumadora: mientras los atacantes humanos necesitaban una media de dos días para lograr la exfiltración, los ataques asistidos por IA lograron el mismo objetivo unas 100 veces más rápido.

Doble extorsión y más: ataques de alcance más profundo

El ransomware moderno suele seguir un guion de dos fases:

1. Exfiltrar datos sensibles.
2. Cifrar los sistemas críticos.

Incluso si la víctima cuenta con copias de seguridad externas o en otra región de la nube, la amenaza de que los datos sensibles se divulguen públicamente ejerce una enorme presión para pagar. A finales de 2024, la brecha de seguridad de LastPass expuso las copias cifradas de millones de usuarios, y aunque las contraseñas maestras permanecieron seguras, el simple hecho de que los atacantes tuvieran una copia de cada bóveda de datos generó una crisis de confianza.

Mientras tanto, los actores estatales utilizan el ransomware no con fines de lucro, sino con fines estratégicos, por ejemplo, paralizando operaciones clave en oleoductos, servicios públicos, sistemas de salud y servicios gubernamentales a gran escala, afectando directamente a infraestructuras críticas.

Un ejemplo perfecto es el ataque de WannaCry en 2017, que interrumpió gravemente los sistemas hospitalarios del Servicio Nacional de Salud del Reino Unido (NHS), provocando cancelación de cirugías y desvío de ambulancias. Este ataque demostró cómo los ciberataques pueden poner vidas en peligro cuando fallan las infraestructuras críticas.

Ubicuidad de los objetivos

La democratización de la IA agéntica a través de plataformas accesibles ha destruido cualquier ilusión de que ciertos sectores puedan ser inmunes. La IA de agentes puede planificar ataques y ejecutarlos de forma autónoma, haciendo los ataques más escalables y eficientes, mientras reduce la barrera de entrada para los ciberdelincuentes.

- *Educación:* en 2022, el grupo Vice Society retuvo los datos del Distrito Escolar de Los Ángeles, afectando a más de 1.000 escuelas y 600.000 estudiantes.

- *Energía:* ese mismo año, la canadiense Suncor Energy sufría un ataque de ransomware que inhabilitó las tarjetas Petro-Canada, dejando a conductores varados en gasolineras de todo el país.

- *Hostelería:* en 2024, BlackCat atacó a MGM Resorts, inutilizando máquinas tragaperras y sistemas de reservas en 30 establecimientos.

- *Retail y servicios:* en abril de 2025, Marks & Spencer tuvo que cerrar varias tiendas en Reino Unido cuando DragonForce cifró sus sistemas, mientras que Mailchimp y SendGrid sufrieron campañas globales de phishing.

La lección es clara: nuestros adversarios tienen tanto las herramientas como los incentivos para atacar en cualquier parte. A medida que la transformación digital acelera la conexión de más dispositivos, procesos y socios, la superficie de ataque crece. Los días en que TI podía aislar "sistemas críticos" detrás de un firewall tipo fortaleza han terminado. Cada endpoint, servicio o integración con terceros en la nube es un punto de entrada potencial.

Además, la interfaz humana en sí —ya sea a través de una llamada deepfake generada por IA o de un dispositivo personal comprometido que se usa para el trabajo— puede convertirse en una puerta de entrada eficaz para los atacantes.

Por qué las organizaciones aún se sorprenden cuando sufren un ataque

A pesar de esta creciente evidencia de vulnerabilidad frente a las ciberamenazas, muchas organizaciones siguen siendo tomadas por sorpresa. Esta vulnerabilidad persistente se debe al uso de supuestos profundamente arraigados sobre ciberseguridad que ya no reflejan la realidad actual. Tres puntos ciegos críticos —una mentalidad centrada solo en la prevención, equipos aislados con metodologías desconectadas y la creencia errónea en la resiliencia automática de la nube— dejan expuestas incluso a las organizaciones mejor defendidas.

Mentalidad centrada en la prevención: capas de falsa confianza

Históricamente, la ciberseguridad ha evolucionado en distintas etapas y, en cada una de ellas, los expertos creyeron haber dominado la protección de la información para sus organizaciones. La tabla 1-1 muestra en detalle esta evolución.

Tabla 1-1: Evolución de la seguridad informática en oleadas distintas

Era	Enfoque	Falsa promesa	Realidad
1990s	Defensa perimetral	Los firewalls y los routers perimetrales impedirían el acceso no autorizado.	Los ataques sortearon las barreras mediante phishing, ingeniería social y agentes internos.
2000s	Seguridad de correo electrónico	El escaneo eliminaría los mensajes maliciosos.	El malware se ocultó en flujos de tráfico legítimos y archivos adjuntos.
2005+	Seguridad de red	La monitorización detectaría anomalías.	Las amenazas sofisticadas parecían inofensivas hasta que provocaron brechas de seguridad.
2010+	Protección de endpoints	El antivirus bloquearía la ejecución.	El malware sin archivos y las vulnerabilidades de día cero eludieron la detección de firmas.
2015+	Seguridad de identidades	La arquitectura de confianza cero solo permitiría el acceso autenticado.	Tokens robados, claves API y permisos mal configurados crearon vulnerabilidades.
2020+	Seguridad en la nube	Los proveedores se encargarían de la seguridad.	Los ataques se dirigieron a permisos en la nube y registros de contenedores mal configurados.

Y es que, pese al aumento de las amenazas, muchas organizaciones siguen atrapadas en una mentalidad preventiva. Se invierte agresivamente en firewalls de nueva generación, sistemas de protección de endpoints (EDR), plataformas SIEM, inteligencia de amenazas y ejercicios de Red Team, pero al final queda claro que estos controles, aunque necesarios, son insuficientes.

Tan pronto como un atacante logra acceso —mediante robo de credenciales, exploits de día cero, phishing o compromiso de la cadena de suministro— la defensa perimetral colapsa. La imagen 1-1 ilustra la defensa en capas en que la industria de la ciberseguridad deposita su confianza.

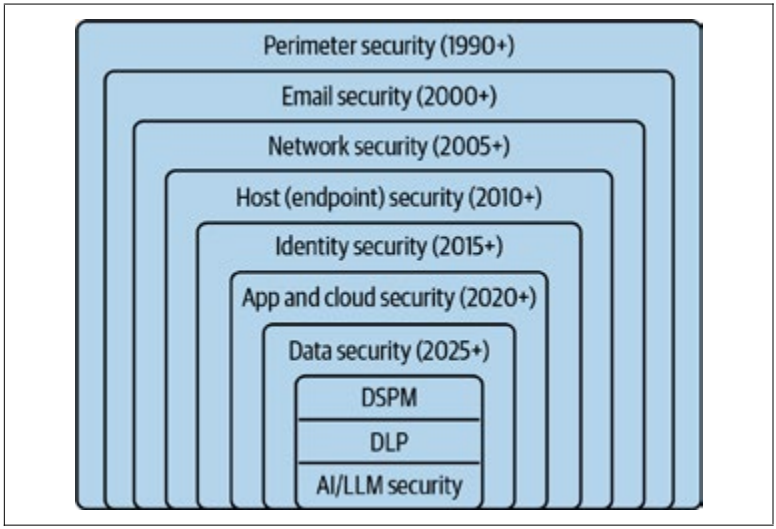

Figura 1-1. La defensa multinivel en el sector de la ciberseguridad

El resultado es una paradoja: al centrarse demasiado en la prevención, se invierte menos en recuperación y, especialmente, en pruebas de recuperación. Se tratan los backups como un simple requisito de cumplimiento, y las pruebas de recuperación se realizan como un ejercicio anual de DR (recuperación ante desastres), si es que se realizan.

Cuando suena la alarma, se intenta trabajar con manuales de operación (runbooks) improvisados, desactualizados, incompletos o no probados, y por tanto incompatibles con los entornos dinámicos actuales.

Equipos aislados y runbooks desconectados

Los equipos de ciberseguridad, operaciones en la nube, desarrollo, arquitectura y continuidad de negocio suelen trabajar en silos, cada uno con sus propios procesos, herramientas y prioridades.

El resultado: las políticas y runbooks se utilizan en presentaciones, documentos de Word o sistemas de tickets, pero rara vez —si es que se da el caso— se emplean en crisis reales. De hecho, es poco común que las dependencias entre aplicaciones, redes, sistemas de identidad, repositorios de código, contenedores, bases de datos y backups estén documentados.

El primer intento de reconstrucción es el peor momento para descubrir que falta una pieza.

Ilusiones sobre la resiliencia en la nube

Muchos CIOs, CTOs y CISOs creyeron en su momento que migrar a la nube bajo la bandera de la "transformación digital" solucionaría mágicamente el problema de recuperación. Los proveedores de nube e hyperscalers anuncian multizonas, regiones, snapshots, réplicas y herramientas nativas de backup que prometen reducir drásticamente los tiempos de recuperación. Pero, para lograr resiliencia real, los equipos deben utilizar múltiples herramientas y servicios.

Además, a medida que la infraestructura escala, el problema se agrava. Muchas grandes organizaciones no gestionan adecuadamente sus políticas de backup en todas sus cuentas en la nube. La cultura "shift left", que otorga a los desarrolladores mayor responsabilidad operativa, ha creado más riesgos de los que ha mitigado.

Los proveedores de nube siguen lanzando servicios para facilitar el modelo de autoservicio, pero en muchos casos este modelo ha desembocado en procesos rotos, dejando a las organizaciones aún más expuestas.

Estas lagunas se hacen aún más evidentes bajo presión. En un caso reciente, una empresa de servicios financieros intentó hacer failover a una segunda región tras una brecha simulada, pero descubrió que las claves de cifrado y los roles de identidad no se habían replicado. El script de failover falló, dejando inutilizable el sitio de recuperación.

Lo cierto es que la nube, por sí sola, no es una solución mágica. Requiere reconstrucciones completas de los entornos de aplicaciones, probadas y verificadas, para garantizar que cada configuración, credencial u objeto está en su lugar.

La resiliencia es imposible sin recuperación

La dura realidad es que la mayoría de las organizaciones han construido sus estrategias de ciberseguridad sobre una ilusión peligrosa: creer que es posible prevenir todos los ataques. Esta mentalidad centrada en la prevención crea una falsa sensación de seguridad que se derrumba en el momento en que un atacante atraviesa con éxito el perímetro. Sin una capacidad comprobada para recuperarse rápida y completamente, incluso las defensas más sofisticadas pierden sentido. Porque la resiliencia no consiste en evitar una caída, sino de recuperarse en caso de que ocurra.

Redefiniendo resiliencia como "confianza en la reconstrucción"

Si algo significa el concepto de resiliencia es "confianza"; la confianza de poder volver a encender las luces cuando se apagan. La ciberresiliencia no es el tiempo de actividad del firewall, ni la frecuencia de parcheo, sino la capacidad de recuperar servicios críticos del negocio (portales de clientes, sistemas de pago, líneas de producción, historiales médicos…) en minutos u horas, no en días o semanas.
El lema "Rebuild is imperative" implica tres cambios fundamentales:

- *Del backup a la reconstrucción completa de los entornos de aplicación:* el foco debe ampliarse más allá de la copia de archivos o bloques, hacia la capacidad de reconstruir cada componente (redes, computación, almacenamiento, identidades y, en particular, sus dependencias) para restablecer los servicios críticos.

- *De hacer ejercicios esporádicos de DR a realizar pruebas de recuperación periódicas:* en lugar de llevar a cabo ejercicios anuales, los equipos deben realizar "simulacros de reconstrucción" automatizados mensualmente en cuentas de nube aisladas de producción.

- *De la utilización de runbooks aislados a la recuperación como código (RaC):* los equipos de seguridad, nube, desarrollo, DR… deben acordar runbooks compartidos, versionados como código y probados en conjunto.

Pero, ¿y si el código RaC pudiera crearse y actualizarse automáticamente?

El coste de la complacencia

Cuando cada minuto de inactividad cuesta miles de dólares, resulta impactante comprender lo que significa un día completo sin operar. Un solo día puede desencadenar consecuencias devastadoras: millones en pérdidas de ingresos, sanciones regulatorias paralizantes y un daño reputacional irreparable.

Los minoristas cierran por no poder vender, los fabricantes detienen sus operaciones al no poder enviar productos, los hospitales quedan paralizados sin acceso a registros médicos vitales... cada minuto perdido puede significar un cliente perdido, un socio traicionado y una marca dañada.

Por el contrario, las organizaciones que adoptan estrategias coherentes de reconstrucción declaran haber reducido su tiempo medio de recuperación de 48 horas (2 días) a menos de 2 horas, y aseguran tener la confianza de que ni siquiera el ataque más sofisticado podrá derribarlas.

Ese es el retorno de inversión que ofrece la reconstrucción: no solo dinero ahorrado, sino confianza preservada. El próximo capítulo profundiza en el desarrollo de una función Rebuild sólida y automatizada.

CAPÍTULO 2

La ilusión de la seguridad: por qué los viejos métodos de recuperación fracasan y por qué el marco del NIST debe adoptar la función *Rebuild*

"No puedes apagar un incendio con una taza de té"

—Adaptado de la sabiduría de los bomberos forestales

A finales del siglo XIX, los ingenieros construyeron enormes diques entre los pueblos fronterizos y el río Misisipi, convencidos de que su tamaño bastaría para contener cualquier inundación. Las familias hacían picnic sobre estos terraplenes, creyendo que la batalla contra el agua estaba ganada. Pero cuando los deshielos de primavera desataron torrentes sin precedentes, los diques se resquebrajaron como cáscaras de huevo y el agua los atravesó, anegando los pueblos.

La lección que se esconde en esos cimientos empapados es relevante: ninguna defensa, por grandiosa que sea, es impenetrable si se basa en suposiciones equivocadas.

En la actualidad, las infraestructuras digitales se enfrentan a una crisis similar de confianza mal dirigida. Las industrias de ciberseguridad y backup han construido sus propios diques, convencidas de la suficiencia de su solución:

- La industria de la ciberseguridad erige barreras: perímetros, firewalls, defensa de endpoints, seguridad en la nube, marcos de identidad…
- La industria del backup se enfoca en repositorios de datos, archivos en cinta, snapshots y estrategias de replicación.

Sin embargo, las brechas de seguridad y los incidentes de ransomware de alto perfil han destruido esa ilusión. No importa cuán altas sean las murallas: los atacantes siempre encuentran un modo de atravesarlas.
De manera similar, los métodos tradicionales de backup resultan sin duda insuficientes para restaurar ecosistemas totalmente comprometidos tras un ataque moderno de ransomware. Este capítulo explora por qué los enfoques convencionales de backup no bastan, y cómo una función de reconstrucción (Rebuild) puede mejorar de forma sustancial los resultados de recuperación.

La peligrosa complacencia del backup y la protección de datos

Durante más de 50 años, hemos creído que proteger los datos era suficiente. Los sistemas de protección de datos se han centrado en la retención a largo plazo y la rentabilidad, en detrimento de una protección orientada a todo el ecosistema de aplicaciones. Por ello, cuando las organizaciones intentan restaurar sus sistemas tras un ataque de ransomware, descubren una cascada de fallos críticos que hacen que sus backups sean casi inútiles.

Por ejemplo: los backups de cinta preservan los archivos, pero restaurar los servidores toma días. Por su parte, los backups basados en disco mejoran la velocidad, pero residen en redes vulnerables. Los sitios de recuperación ante desastres prometen un failover sin interrupciones, pero suelen fallar debido al uso de procedimientos obsoletos, desviaciones de configuración y lagunas de conocimiento. La deficiencia fundamental no está en la protección de datos, sino en la ilusión de que realizar backups equivale a la capacidad de restaurar los sistemas en funcionamiento. Lo cierto es que una verdadera recuperación requerirá no solo almacenamiento offline, sino también capacidades integrales de restauración de los sistemas. Algo que la mayoría de las estrategias de backup no ofrecen.

Ransomware moderno: la muerte del "Backup and Restore"

Los ataques de ransomware no solo detectan los backups: los "cazan" desde el principio para asegurarse de que el "Plan B" de la organización quede comprometido ya antes de iniciar la siguiente fase. Una vez

que los atacantes obtienen privilegios de administrador, desmantelan sistemáticamente las capacidades de recuperación de la organización: deshabilitan o eliminan snapshots, manipulan las políticas de retención del backup y corrompen incluso repositorios supuestamente inmutables. Incluso pueden llegar a comprometer las capas de orquestación que gestionan estos sistemas, convirtiendo cada posible vía de recuperación en un callejón sin salida.

La amenaza va más allá de la simple destrucción. Las bandas de doble extorsión han perfeccionado un enfoque perfectamente calculado: primero roban datos sensibles para amenazar con su divulgación pública, y luego cifran lo que queda para paralizar las operaciones.

Estos ataques en dos frentes maximizan su poder de coerción, pues las organizaciones se enfrentan simultáneamente al cierre de sus operaciones y a una catástrofe reputacional.

El espejismo del almacenamiento inmutable

El almacenamiento inmutable está diseñado para que, una vez escritos, los snapshots no puedan modificarse. Pero los atacantes han desarrollado contramedidas sofisticadas que exponen las limitaciones fundamentales de esta tecnología. Su estrategia consiste en secuestrar el plano de gestión (la capa de control) para alterar las políticas de inmutabilidad antes de que las instantáneas se completen, neutralizando así la protección antes de que surta efecto. También explotan vulnerabilidades de configuración que les permiten purgar o volver a cifrar los archivos almacenados, convirtiendo los controles de seguridad de la organización en un arma en su contra.

Incluso aunque las bóvedas de datos permanezcan seguras desde un punto de vista técnico, su alcance es peligrosamente limitado: protegen los datos, pero dejan configuraciones de red, redes de microservicios e infraestructuras de identidad totalmente expuestas.

Herramientas de seguridad de datos: útiles, pero incompletas

Los avances recientes han introducido herramientas sofisticadas como DSPM (Data Security Posture Management), para visibilidad de datos, o DLP (Data Loss Prevention) para monitorizar el movimiento de los

datos, así como herramientas de seguridad con soporte de IA para detección y respuesta inteligente ante amenazas.

Aunque estas tecnologías representan un progreso significativo en cuanto a capacidades, se enfocan sobre todo en la prevención y la detección, no en la recuperación integral. Por ello, las organizaciones siguen siendo vulnerables cuando los atacantes logran superar sus defensas.

Cantos de sirena y escollos ocultos en la recuperación en la nube

Los proveedores de nube a hiperescala prometieron capacidad infinita, snapshots replicados por regiones y pipelines de recuperación ante desastres (DR) en modo autoservicio. Muchas organizaciones, creyendo que sus datos estarían más seguros, migraron terabytes de datos en pocas semanas. Sin embargo, esas promesas, en realidad, ocultaban deficiencias clave que solo se revelaron cuando más necesitaron las organizaciones de sus capacidades

Más allá del backup tradicional

Los métodos heredados no capturan las complejas dependencias que abarcan servicios en la nube, las inevitables desviaciones de configuración que ocurren en las redes y los dominios de identidad, ni el malware o las configuraciones erróneas que se ocultan en contenedores, funciones serverless o bibliotecas de aplicaciones. Sin "copias doradas" (golden copies: copias de aplicaciones y datos de un punto en el tiempo, limpias, verificadas y completas), las restauraciones se construyen sobre arena.

El antiguo enfoque de "esperemos que el backup funcione" es tan arriesgado como apostar todo el negocio a un único paracaídas sin revisar.

La pieza clave que falta: pruebas periódicas y completas de reconstrucción (Rebuild Testing)

Tanto la ciberseguridad basada en la defensa como las estrategias tradicionales de backup son, básicamente, incompletas. La solución real está en la realización de pruebas periódicas y reales de las capacidades de reconstrucción completa.

El Rebuild Testing representa un cambio fundamental: de simplemente esperar a que los backups funcionen a probar su efectividad para una validación integral. Este enfoque reconstruye todo el entorno digital tal como existía en un momento "limpio" conocido, y ofrece una recuperación integral que va mucho más allá de la simple restauración de los datos.

El proceso implica rebobinar todas las capas de la infraestructura de la organización; no solo los datos, sino también configuraciones de red, recursos de computación, marcos de identidad, contenedores, instancias serverless y pasarelas API, a fin de que el entorno restaurado sea un reflejo exacto del original.

Y, aún más importante: el Rebuild Testing incluye escaneos integrales de malware, vulnerabilidades, desviaciones de configuración y alteraciones no autorizadas que pudieran haberse infiltrado antes del snapshot. Este paso de validación hace que la restauración pase de ser un acto de fe a convertirse en un proceso de recuperación verificado y seguro en el que las organizaciones pueden confiar cuando la supervivencia está en juego.

El punto ciego del marco de ciberseguridad del NIST

El marco de ciberseguridad del National Institute of Standards and Technology (NIST) proporciona una estructura bien diseñada con seis funciones principales: Identificar, Proteger, Detectar, Responder, Recuperar y Gobernar. Sin embargo, su función Recuperar (Recover) se malinterpreta de manera peligrosa, creando un punto ciego crítico que deja a las organizaciones vulnerables incluso cuando creen estar protegidas.

Recuperar vs. Reconstruir: dos funciones distintas

La función Recover del NIST se centra en restaurar los sistemas para que vuelvan a un estado funcional después de un incidente. Este enfoque trata la recuperación como un control de daños, priorizando la velocidad sobre la validación. Las organizaciones restauran desde backups, ejecutan scripts de DR y celebran cuando las aplicaciones "parecen" funcionar, sin verificar que lo restaurado está completo y mantiene la integridad.

Rebuild, sin embargo, representa un cambio de paradigma hacia una reconstrucción con confianza. En lugar de simplemente restaurar lo perdido, la función Rebuild busca crear un entorno limpio y verificado

a partir de componentes fiables. Es la diferencia entre parchear una pared dañada y construir una nueva a partir de planos verificados. Ambas pueden parecer funcionales, pero solo una mantiene su integridad estructural.

Donde la recuperación no llega

En la práctica, la función Recover suele reducirse a actividades de cumplimiento superficiales, que aportan una garantía mínima sobre la verdadera capacidad de recuperación. Las organizaciones realizan ejercicios anuales teóricos de DR, prueban restauraciones de bases de datos o máquinas virtuales aisladas, pero ignoran las interdependencias complejas que exigen las aplicaciones modernas.

Y lo más crítico: rara vez se realizan restauraciones completas y validadas de aplicaciones-enteras para confirmar que todos los componentes coinciden con los datos del snapshot y funcionan juntos como un sistema integrado. La Tabla 2-1 identifica las carencias del marco actual del NIST y muestra cómo la función Rebuild puede cubrir esas brechas críticas.

Al elevar Rebuild a su propio pilar -como extensión viva de la función Recover-, orientamos la estrategia de defensa hacia pruebas de resiliencia más exigentes, como la capacidad de volver a un punto específico en el tiempo, seleccionar copias doradas seguras o reconstruir aplicaciones desde la capa de red hasta la de datos bajo demanda.

Tabla 2-1. Deficiencias en el marco actual del NIST y el papel de la función Rebuild para solucionarlas.

Función	Fortaleza tradicional	Deficiencia actual	Cómo Rebuild corrige el problema
Identificar	Inventarios de activos, análisis BIA	Sin garantía de recuperación regular	Catálogo histórico de copias maestras
Proteger	IAM, cifrado, firewalls	Incapacidad para detener ataques de día cero o internos	Snapshots inmutables para los elementos de reconstrucción
Detectar	SIEM, XDR, UEBA	Alerta ≠ restauración garantizada.	Pruebas de reconstrucción automatizadas activadas por feeds de eventos
Responder	Playbooks de IR, cuarentena	Los playbooks rara vez validan la restauración completa	Ejecuciones de reconstrucción integradas como parte de la respuesta
Recuperar	Scripts de backup y failover	Restauraciones parciales y manuales; runbooks no probados	Orquestación definida por código para una reconstrucción completa del entorno
Rebuild			Simulacros de reconstrucción periódicos y automatizados en un punto en el tiempo

El Framework extendido

Para mantener la resiliencia, debemos añadir la función Rebuild al marco del NIST. Recuperar sigue siendo la política, el plan y el análisis posterior, es decir, el marco estratégico que define lo que debe suceder cuando se produce un desastre. Rebuild es el motor vivo que puede hacer que la recuperación sea una realidad probada en lugar de una posibilidad teórica, como se muestra en la figura 2-1.

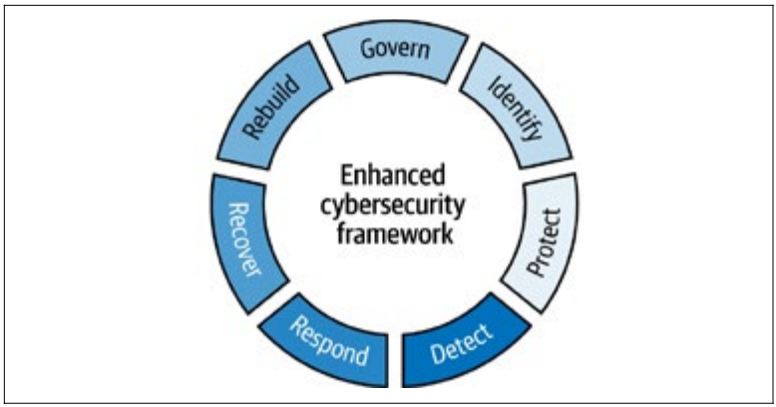

Imagen 2-1. El marco del NIST con la incorporación de la función Rebuild

La función Rebuild incorpora una serie de elementos:

Recuperación de infraestructuras en un punto en el tiempo
: Esta capacidad captura snapshots completos de los componentes de la infraestructura en un punto específico en el tiempo, incluyendo configuraciones de red, recursos de cómputo, imágenes de aplicaciones y sus interdependencias. A diferencia de los backups tradicionales, que se enfocan solo en los datos, estos snapshots están diseñados para recrear el contexto de infraestructura que las aplicaciones necesitan para funcionar correctamente.

Copias doradas
: Las copias doradas (golden copies) son imágenes de un punto en el tiempo que han pasado por escaneos exhaustivos en busca de malware, errores de configuración y vulnerabilidades, proporcionando puntos de recuperación validados y limpios. No son solo copias seguras de datos: son instantáneas verificadas y limpias de pilas completas de aplicaciones en las que se puede confiar plenamente, eliminando el temor a que la restauración reintroduzca los mismos problemas que se intentan resolver.

Recovery as code (RaC)
: RaC transforma los procedimientos de restauración ad hoc en procesos automatizados, versionados y repetibles. En lugar de depender de manuales obsoletos, RaC trata los procedimientos de reconstrucción como software vivo que evoluciona junto con la infraestructura, de modo que las capacidades de recuperación mejoran con el tiempo en lugar de degradarse por el abandono.

En definitiva, Rebuild transforma la mentalidad "Esperemos que el backup funcione" en "Tengo la confianza de que esta reconstrucción funcionará." Esto es así porque se ha probado, refinado y comprobado decenas de veces antes de que realmente se necesite.

CAPÍTULO 3

Aprovechando las ventajas de *Rebuild*: poniendo a prueba lo inesperado en la nube

A comienzos del siglo XX, la seguridad de los vehículos mejoró drásticamente, no solo porque los coches se volvieron más resistentes, sino porque las pruebas de choque se convirtieron en una parte central de su proceso de desarrollo, lo que vino a transformar la seguridad de una mera esperanza en resultados garantizados. De manera similar, en los primeros días de la aviación, los pilotos creían que dominar el vuelo significaba construir aviones más sólidos.

Sin embargo, cuando ocurría un desastre en pleno vuelo, no era solo la resistencia del avión lo que salvaba vidas, sino la capacidad del piloto para recuperarse de eventos inesperados. No importaba cuán bien diseñado estuviera el avión: la supervivencia dependía, a menudo, de un entrenamiento exhaustivo y riguroso mediante simulaciones de todas las emergencias posibles.

Hoy, la resiliencia digital se enfrenta a un momento de transformación similar. Las organizaciones deben ir más allá de suponer que los backups y las ciberdefensas funcionarán. Un elemento que falta —quizás el más crítico— es el de realizar pruebas periódicas. Las pruebas periódicas permiten a las organizaciones reconstruir de manera fiable sus entornos digitales tras producirse un fallo catastrófico. Este capítulo se centrará en cómo las organizaciones pueden implementar pruebas continuas de reconstrucción (Rebuild Testing).

Historias reales de backups que no funcionaron y planes de recuperación que fracasaron

Incidentes recientes revelan la fragilidad de nuestros ecosistemas digitales, a pesar de las ingentes inversiones que las organizaciones han realizado en ciberseguridad y backup. La escala e intensidad de los ataques de ransomware han aumentado drásticamente en los últimos años, demostrando que incluso los planes más completos de recuperación ante desastres fallan cuando no han sido probados frente a la realidad de las ciberamenazas modernas.

Consideremos cómo grandes empresas han sufrido en los últimos años cuando sus planes de recuperación fracasaron estrepitosamente a pesar de contar con una documentación meticulosa y una inversión significativa.

MGM Resorts y Caesars Entertainment
: Estas compañías se enfrentaron a ataques devastadores a finales de 2023, lo que provocó interrupciones generalizadas. A pesar de contar con planes de recuperación ante desastres (DR) completos, ambas tuvieron dificultades para restaurar funciones críticas del negocio con rapidez. Aunque existía documentación sólida, la restauración real falló debido a dependencias no probadas, configuraciones obsoletas y la falta de integración entre los backups de datos y la recuperación de aplicaciones.

Servicio Nacional de Salud (NHS), Reino Unido
: Un ataque con el ransomware Qilin en 2024 reveló una realidad alarmante: casi un millón de registros de pacientes y sistemas de datos de salud críticos fueron comprometidos, a pesar de contar con backups robustos. El NHS aprendió por las malas que restaurar solo las bases de datos era insuficiente; sin procedimientos verificados de restauración para aplicaciones, identidades y arquitecturas de red, los backups resultaron ser inútiles.

Ataques contra buckets AWS
: En el inquietante escenario de 2025, el ransomware Codefinger atacó buckets de almacenamiento AWS S3 de varias compañías, haciendo que las estrategias tradicionales de backup en la nube fueran ineficaces. Muchas organizaciones, a pesar de realizar backups regulares, despertaron descubriendo que los backups habían sido cifrados a través de un ataque de ransomware. Estos incidentes subrayan la necesidad de un enfoque completamente

nuevo para probar los procedimientos de restauración.

Estas historias ilustran una realidad preocupante: nuestras suposiciones tradicionales sobre protección y seguridad de datos están incompletas. El crecimiento exponencial de un ransomware cada vez más sofisticado, junto con los cada vez más frecuentes apagones de regiones cloud, exige una nueva disciplina en resiliencia digital: probar reconstrucciones completas de entornos de forma periódica, exhaustiva y rigurosa.

Más allá de la recuperación tradicional: el reto moderno de las reconstrucciones en la nube

Reconstruir entornos cloud implica mucho más que simplemente restaurar datos a partir de backups. Las aplicaciones modernas operan en ecosistemas altamente dinámicos, compuestos por numerosos servicios cloud-native y que cambian constantemente a través de sucesivos pipelines simultáneos de DevOps. Ahora, estos pipelines están, cada vez más, impulsados por la inteligencia artificial.

Dependencias ocultas y desviaciones de configuración

Cada canalización de DevOps puede actualizar configuraciones, desplegar microservicios y ajustar políticas de seguridad de forma independiente, lo que aumenta el riesgo de errores de configuración y oculta dependencias críticas. Los equipos que utilizan herramientas de integración y entrega continua (CI/CD) como AWS CodeDeploy, CodePipeline o CodeBuild modifican frecuentemente los entornos sin tener una visibilidad clara del impacto de esos cambios. De este modo, a menudo crean vulnerabilidades ocultas o dependencias inadvertidas, dificultando la reconstrucción completa y precisa si se produce una crisis.

Marco estratégico de viabilidad mínima: cómo hacer que la reconstrucción sea alcanzable

Al final, la realidad para la mayoría de las organizaciones es que reconstruirlo todo al mismo tiempo no es ni práctico ni necesario. Aquí es donde entra en escena el concepto de "viabilidad mínima", que actúa como puente estratégico entre la teoría del Rebuild y su implementación con éxito.

El marco de viabilidad mínima señala que las organizaciones comprenden cuáles son sus activos más críticos y qué acciones se requieren para restaurarlos a un estado totalmente operativo. En lugar de la abrumadora tarea de probar reconstrucciones completas, las organizaciones pueden implementar la función Rebuild gradualmente, centrándose primero en lo que realmente importa para la supervivencia del negocio.

Las organizaciones pueden implementar eficazmente esta función clasificando sus aplicaciones y servicios según marcos reconocidos como ISO 22301 (sistemas de gestión de continuidad del negocio) o directrices de análisis de impacto empresarial como las del NIST, que ayudan a categorizar los sistemas según su criticidad operativa:

- *De misión crítica:* sistemas sin los cuales no se puede operar (por ejemplo, Active Directory, sistemas de gestión de pedidos, sistemas de atención al paciente…) y que constituyen la base de la viabilidad mínima: sin ellos, la organización queda inhabilitada.

- *Críticos de negocio:* sistemas necesarios para la recuperación completa de las operaciones (correo electrónico, contabilidad, gestión de la cadena de suministro…) que permiten ampliar la capacidad operativa más allá de la supervivencia básica

- *No críticos:* sistemas adicionales que apoyan la funcionalidad completa pero no son esenciales para la continuidad inmediata del negocio.

Este enfoque por niveles transforma la función de reconstrucción de un desafío abrumador ("todo debe funcionar") a un proceso de recuperación estratégico y por fases. Las organizaciones pueden alcanzar la viabilidad mínima centrando primero las pruebas de reconstrucción en los sistemas críticos para el negocio, y luego escalando sistemáticamente a las aplicaciones de misión crítica y las no críticas.

Además, el modelo reduce drásticamente los objetivos iniciales de tiempo de recuperación (RTO) para las funciones esenciales del negocio, mientras mantiene la meta de una restauración completa del entorno.

Reconstrucción completa: metadatos, automatización y orquestación

Una reconstrucción eficaz implica capturar todos los metadatos relevantes, y no solo los datos de aplicación, sino también configuraciones detalladas, dependencias de recursos, políticas de identidad y acceso (IAM), topologías de red o puntos de enlace de APIs, entre otros.

Es crucial que las organizaciones repliquen estos metadatos de manera segura e inmutable en múltiples regiones de la nube o cuentas aisladas, para minimizar puntos únicos de fallo y mejorar la seguridad frente al ransomware y los cambios no autorizados.

La reconstrucción debe aprovechar técnicas de infraestructura como código (IaC), integrando procesos de recuperación previamente fragmentados en pipelines de automatización ejecutables. Este enfoque permite que las operaciones de resiliencia sean adaptables, consistentes y verificables.

Centralizar y actualizar continuamente el código de recuperación permite a los equipos gestionar la resiliencia de forma proactiva, en lugar de reaccionar ante las crisis. Por tanto, un proceso de reconstrucción integral no consiste solo en restaurar datos, sino en orquestar todo el entorno en la nube de manera fluida y coherente.

La función Rebuild: recuperación de infraestructuras en un punto en el tiempo y Recovery as Code

Commvault Cloud Rewind (anteriormente Appranix) aborda las debilidades de las prácticas tradicionales de recuperación ante desastres mediante dos conceptos innovadores para la reconstrucción bajo demanda de entornos de aplicación: recuperación de infraestructuras en un punto en el tiempo (PITR) y recuperación como código (RaC).

Históricamente, las organizaciones han lidiado con manuales de recuperación fragmentados, administrados de manera independiente por los equipos de seguridad, aplicaciones, arquitectura de negocio documentos dispersos, lo que prolongaba el tiempo de inactividad.

La recuperación de infraestructura en un punto en el tiempo (PITR) resuelve este problema proporcionando un snapshot automatizado y completo de todo el ecosistema digital, incluyendo no solo los datos, sino también toda la pila de aplicaciones, microservicios, funciones serverless, configuraciones de identidad y acceso, topologías de red y las dependencias entre ellos.

Al poder capturar de forma periódica estas imágenes completas en momentos específicos y de acuerdo con las políticas definidas, PITR permite a las organizaciones mantener copias doradas (Golden Copies) validadas y completas que estarán disponibles tanto para restauraciones de viabilidad mínima como para reconstrucciones completas de la pila de aplicaciones.

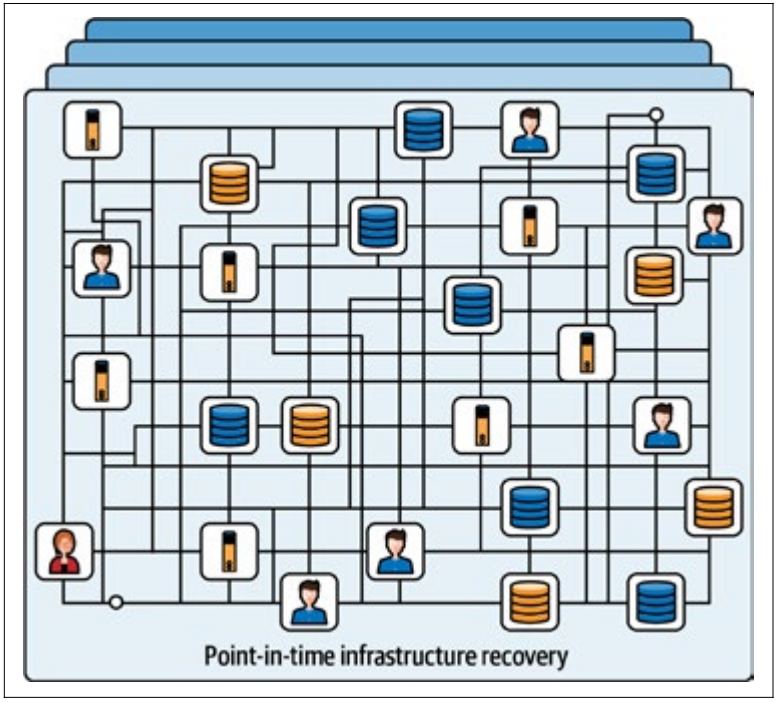

Imagen 3-1. PITR proporciona una captura integral (snapshot) de todo el ecosistema de aplicaciones en la nube

La capacidad de PITR para capturar snapshots jerarquizados se vuelve especialmente valiosa dentro de las estrategias de viabilidad mínima. Las organizaciones pueden configurar políticas que prioricen las aplicaciones críticas para el negocio con snapshots más frecuentes, otorgando a los sistemas de misión crítica puntos de recuperación verificados y manteniendo una protección base para las aplicaciones no críticas.

Este enfoque por niveles permite una restauración rápida de las operaciones incluidas en el concepto de viabilidad mínima, manteniendo al mismo tiempo una protección integral para todo el entorno.

Aprovechar plataformas cloud de hyperscalers como AWS, Azure o Google Cloud mejora aún más esta capacidad. Los vastos recursos de computación on demand y las funciones integradas de aislamiento de estos entornos permiten a las organizaciones ejecutar pruebas frecuentes y a gran escala de forma sencilla y eficiente. Estas plataformas simplifican las complejas validaciones de recuperación, transformando los costosos y esporádicos ejercicios de recuperación ante desastres en ejercicios de reconstrucción (Rebuild) rutinarios y rentables.

Como complemento a la recuperación PITR, Recovery as Code (RaC) transforma esta recuperación en un proceso unificado y automatizado que habilita la función Rebuild. En lugar de mantener manuales de recuperación engorrosos y aislados, RaC integra todos los pasos necesarios directamente en pipelines de automatización ejecutables (imagen 3-2).

El código controlado a través de versiones actúa como fuente única y genuina para la recuperación, alineando a equipos de seguridad, arquitectos, desarrolladores y especialistas en backup en torno a un proceso centralizado y consistente. Este enfoque impulsado por código integra las pruebas de reconstrucción regulares de forma fluida en los flujos de trabajo diarios de DevOps, reduciendo significativamente la complejidad operativa.

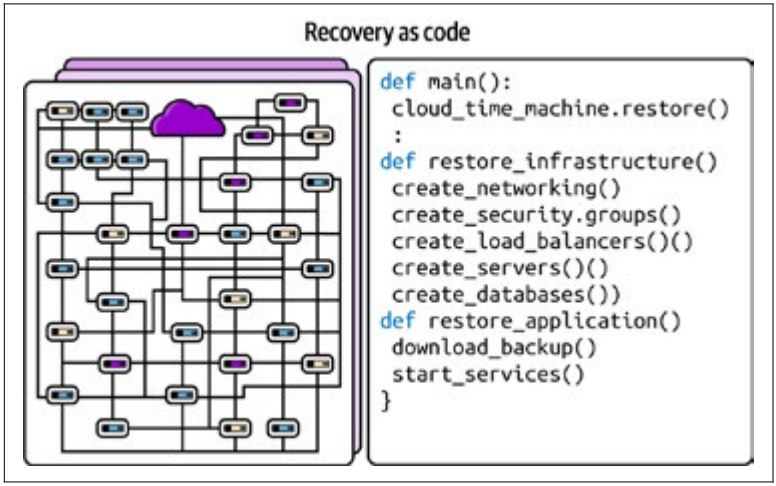

Imagen 3-2. PITR, mano a mano con RaC, integra todos los pasos de recuperación en pipelines de automatización ejecutables.

Uso estratégico de Rebuild

RaC puede estructurarse para respaldar flujos de trabajo de viabilidad mínima, con pipelines de automatización separados para aplicaciones críticas para el negocio, críticas para la operativa y no críticas. Esto permite a las organizaciones ejecutar restauraciones rápidas de viabilidad mínima mientras se preparan para una recuperación completa del entorno, haciendo que la función de Rebuild sea tanto estratégica como práctica.

En conjunto, PITR y RaC van a transformar decisivamente la resiliencia organizacional. Estas innovaciones permiten a las organizaciones pasar de la incertidumbre y la gestión reactiva de crisis a una capacidad proactiva y demostrable, reduciendo significativamente los tiempos de recuperación, simplificando los requisitos de cumplimiento y generando una confianza sin precedentes entre los stakeholders. Las pruebas regulares de Rebuild han dejado de ser un objetivo lejano y se han convertido en un imperativo estratégico para la resiliencia digital moderna.

El valor del Rebuild Testing periódico para el negocio gracias a la optimización de costes

Adoptar pruebas regulares de Rebuild con PITR y RaC transforma la resiliencia organizacional al hacer que la función de reconstrucción sea tanto económicamente viable como estratégicamente valiosa. En lugar de depender de planes de recuperación inciertos y de una gestión de crisis basada en el miedo, las organizaciones pueden adoptar capacidades de recuperación claras, medibles y demostrables.

Imaginemos una organización de atención médica que se enfrenta a un ataque de ransomware. En lugar de esperar la restauración completa de su infraestructura, la planificación de viabilidad mínima le permitiría una restauración rápida de los sistemas de atención a pacientes, las operaciones de urgencias y las capacidades críticas de comunicación. Otros sistemas, como los entornos administrativos, las plataformas de programación y las herramientas de reporting pueden restaurarse posteriormente sin afectar a la atención al paciente.

Este enfoque por niveles proporciona beneficios claros y medibles.

Mejoras operativas y en la confianza de los clientes

Al priorizar los sistemas generadores de ingresos dentro de la planificación de viabilidad mínima, las organizaciones pueden reanudar sus operaciones esenciales rápidamente, reforzando así la confianza de sus clientes. Esta confianza acabará por convertirse en ventaja competitiva, especialmente en industrias donde la fiabilidad digital impacta de forma directa en la relación con los clientes.

Beneficios regulatorios y de cumplimiento

La planificación de viabilidad mínima ayuda a las organizaciones a cumplir con los requisitos normativos para mantener servicios esenciales cuando se produce una interrupción. Las pruebas automatizadas de reconstrucción simplifican los procesos de cumplimiento al generar una evidencia integral de forma regular, lo que hará que las auditorías sean más eficientes.
Las organizaciones pueden demostrar su conformidad con normas como HIPAA o con marcos industriales como SOC 2, ISO 27001 o DORA (Digital Operational Resilience Act) con una intervención manual mínima, ofreciendo a los auditores visibilidad inmediata sobre sus capacidades de resiliencia.

Reducción de costes y tiempo

La automatización de reconstrucciones reduce sustancialmente la complejidad y los costes. Las pruebas tradicionales de recuperación ante desastres son caras, disruptivas y propensas a errores humanos. Al adoptar RaC, las organizaciones pueden reconstruir y probar bajo demanda, utilizando la programabilidad y los modelos de despliegue de las nubes a hiperescala.

Esto permite automatizar procesos complejos de Rebuild, pasando de manuales de operación dispersos a procedimientos basados en código, repetibles y optimizados. Esta automatización no solo reduce la carga operativa y elimina los costes de las pruebas manuales, sino que también promueve la consistencia y la fiabilidad en cada prueba.

Fiabilidad y seguridad organizacional

Pero quizá lo más importante es que las pruebas periódicas de Rebuild generan una confianza organizacional sin precedentes. Las capacidades de recuperación validadas regularmente brindan a la dirección una garantía clara y demostrable de su preparación para afrontar interrupciones.

Organismos reguladores, clientes y socios obtendrán la certeza de que la organización mitiga riesgos de forma proactiva y que podrá recuperarse rápidamente de cualquier ciberataque o fallo en la nube. Esta confianza, como decíamos, se convertirá en ventaja estratégica, diferenciando a las organizaciones resilientes en un mundo definido por amenazas digitales y disrupciones constantes.

Haciendo viable el *Rebuild Testing*: infraestructura y métodos de validación

Una vez establecido el marco estratégico de viabilidad mínima, surge la pregunta: ¿Cómo ejecutar pruebas regulares de Rebuild a gran escala para aplicaciones críticas? La respuesta pasa por dos factores que hacen que realizar pruebas frecuentes sea asequible y realista.

- Primero, las plataformas cloud a hiperescala aportan la infraestructura elástica necesaria para crear entornos completos de pruebas bajo demanda.
- Segundo, los principios del Chaos Engineering permiten a estas pruebas simular fallos reales en lugar de escenarios predecibles.

En conjunto, estos enfoques transforman las pruebas de Rebuild de un ejercicio costoso y anual a una capacidad operativa rutinaria.

Plataformas cloud como potenciador para las pruebas

Plataformas cloud como AWS, Azure y Google Cloud ofrecen un entorno ideal para pruebas periódicas de Rebuild gracias a su flexibilidad, escalabilidad y rentabilidad sin comparación. A diferencia de los centros de datos tradicionales, las nubes a hiperescala permiten a las organizaciones crear instantáneamente entornos sandbox totalmente aislados, ejecutar las pruebas más rigurosas y desmantelarlas sin afectar la producción.

Esta flexibilidad elimina las barreras tradicionales asociadas con las pruebas de recuperación ante desastres, permitiendo realizar pruebas de forma más frecuente, exhaustiva y significativa.

Una ventaja clave de estas plataformas es su enorme capacidad de proceso y almacenamiento bajo demanda, lo que permite a las organizaciones escalar recursos rápidamente según las necesidades de cada prueba. El uso estratégico de instancias temporales (spot instances) aporta capacidad computacional con costes hasta un 70–80% menores que los precios estándar, permitiendo incrementar la frecuencia de las pruebas sin causar problemas de presupuesto.

Los entornos cloud también permiten simular fallos parciales de infraestructura, probar capacidades de failover entre regiones para sistemas críticos y validar que los procedimientos de restauración de viabilidad mínima funcionan bajo diversas condiciones de fallo, todo dentro de entornos de prueba rentables y aislados.

Las pruebas periódicas de Rebuild, antes vistas como complejas y costosas, son ahora prácticas y accesibles, permitiendo que lo que solía ser una actividad de cumplimiento ocasional pase a ser una capacidad principal de la organización.

Chaos Testing: construyendo resiliencia a través del fallo intencionado

El Chaos Testing consiste en inyectar deliberadamente perturbaciones controladas en un sistema para descubrir debilidades ocultas y validar su resiliencia en condiciones realistas. Este enfoque introduce intencionadamente escenarios de fallo —caídas de infraestructura, latencia de red, picos inesperados de recursos, etc.— para comprobar si los sistemas continúan funcionando de manera fiable bajo estrés.
A diferencia de los ejercicios estándar de DR, que suelen simular escenarios predecibles, el Chaos Testing prospera en la imprevisibilidad, desafiando continuamente las suposiciones y revelando puntos ciegos en la resiliencia de aplicaciones e infraestructuras.

En el contexto de las pruebas de Rebuild, el Chaos Testing es particularmente crítico. Dado que los entornos de producción evolucionan constantemente —se despliegan nuevos servicios, algunas configuraciones cambian y las cargas de trabajo fluctúan—, las pruebas estáticas de reconstrucción se vuelven obsoletas rápidamente.
Las plataformas cloud permiten a las organizaciones ejecutar pruebas de reconstrucción adaptativas, que se ajustan a la naturaleza dinámica de las aplicaciones modernas. Al integrar los principios de ingeniería del caos con las prácticas de Rebuild, las pruebas evolucionan de forma proactiva, reflejando la complejidad de los entornos de producción y adaptándose continuamente a los cambios.

El Chaos Testing resulta ser aún más valioso cuando se aplica desde la perspectiva de la viabilidad mínima. En lugar de probar fallos aleatorios en todo el entorno, las organizaciones pueden centrar los experimentos de caos en los sistemas críticos para el negocio para entender cómo los fallos podrían propagarse e impactar a la restauración de viabilidad mínima.

Por ejemplo, durante un ejercicio de restauración de viabilidad mínima, el Chaos Testing podría desactivar deliberadamente los servicios de Active Directory para validar que los sistemas de autenticación de backup puedan mantener las operaciones esenciales del negocio. O podría simular fallos de partición de red entre microservicios críticos para confirmar que las aplicaciones de viabilidad mínima siguen funcionando incluso cuando los servicios dependientes no están disponibles.

Haciendo realidad las pruebas de Rebuild: de la teoría a los resultados concretos

Establecer pruebas periódicas de Rebuild transforma la resiliencia de la organización de una garantía teórica a una capacidad medible y tangible. Así como el desarrollo de software incorpora prácticas regulares de verificación de calidad (QA), la resiliencia digital debe adoptar pruebas de reconstrucción periódicas. Tanto los CIOs como los CISOs pueden esperar beneficios concretos: capacidad de recuperación demostrable, reducción medible del riesgo y alineación clara entre los equipos de seguridad, recuperación y operaciones en la nube.

Implementación de pruebas por niveles

Un enfoque estructurado comenzará por la programación de fechas para las pruebas, mensuales o trimestrales, que incluyan tanto escenarios de viabilidad mínima como de restauración completa del entorno. Estos eventos deberán planificarse cuidadosamente incorporando ejercicios de recuperación, pruebas de viabilidad mínima y experimentos de Chaos Testing controlados.

Días de prueba de viabilidad mínima

Las organizaciones deben realizar ejercicios centrados específicamente en restaurar sistemas críticos para el negocio dentro de ventanas de tiempo definidas. Estas pruebas validan que las funciones esenciales del negocio podrán restaurarse rápidamente —típicamente en horas, y no en días—.

Como métricas de éxito se incluyen el tiempo de restauración de servicios de identidad, el tiempo empleado para poner en línea las aplicaciones principales y la verificación de que las operaciones de mínima viabilidad podrán mantenerse mientras se aborda la recuperación completa.

Pruebas de reconstrucción completa del entorno

También es importante realizar ejercicios más amplios que prueben la restauración completa de la infraestructura, confirmando que tanto los sistemas críticos como los no críticos podrán restaurarse con éxito tras alcanzar la viabilidad mínima. En definitiva, estas pruebas permiten

validar la capacidad de la organización para retornar a su plena capacidad operativa.

Definición de roles y responsabilidades

Definir claramente los roles y responsabilidades será esencial para una ejecución efectiva, especialmente al equilibrar las prioridades de viabilidad mínima y restauración completa del entorno.

Equipos de seguridad

Los equipos de seguridad deberán analizar rigurosamente y validar que los entornos restaurados están libres de vulnerabilidades, firmas de ransomware y configuraciones incorrectas. Durante la restauración de viabilidad mínima, priorizarán la validación de los sistemas críticos al mismo tiempo que realizan evaluaciones de seguridad integrales para todo el entorno.

Equipos de operaciones y aplicaciones cloud

Estos equipos se enfocarán en el aprovisionamiento de infraestructura, la alineación de configuraciones y la orquestación de reconstrucciones completas a partir de los PITR del entorno. Gestionan la ejecución técnica tanto de la restauración de viabilidad mínima como de la reconstrucción completa, verificando que las dependencias están correctamente secuenciadas y que los servicios restaurados cumplen los requisitos funcionales.

Equipos de recuperación

Supervisarán todo el proceso de reconstrucción, actuando como nexo entre los distintos grupos y documentando los resultados con precisión, gestionarán la transición desde la viabilidad mínima hasta la capacidad operativa total y coordinarán los diferentes escenarios de prueba.

Midiendo el éxito y demostrando el valor

Para medir la efectividad y demostrar el valor de las pruebas de Rebuild se deben establecer y comunicar métricas claras que vayan más allá de los simples objetivos de tiempo (RTO) y punto de recuperación (RPO). Entre ellas podríamos destacar las siguientes:

Métricas de viabilidad mínima

: Tiempo para restaurar sistemas críticos para el negocio y sus dependencias, tasa de éxito de los procedimientos de viabilidad mínima bajo condiciones de estrés y capacidad para dar soporte a operaciones esenciales durante la recuperación completa

Métricas de recuperación completa
: Tiempo total de recuperación del entorno completo, tasa de éxito de los procedimientos de reconstrucción integral y verificación de que todos los sistemas funcionan correctamente tras la restauración

Métricas de pruebas de resiliencia
: Frecuencia y exhaustividad de las pruebas de caos realizadas, número de vulnerabilidades o configuraciones erróneas identificadas y corregidas. Mejora del rendimiento de recuperación con el tiempo

Métricas de impacto en el negocio
: Reducción potencial de pérdidas debidas a incidentes, mejora en los indicadores de confianza del cliente y análisis del cumplimiento normativo mediante pruebas periódicas

CIOs y CISOs deberían esperar informes periódicos que destaquen estas métricas, proporcionando transparencia y pruebas de mejora continua.

Las pruebas periódicas de Rebuild proporcionan pruebas tangibles de las capacidades de recuperación para presentarlas a todos los involucrados, desde los equipos de seguridad, que buscan validar la mitigación de amenazas, hasta la dirección, que necesita demostrar la resiliencia de las operaciones.

Consideradas durante mucho tiempo simplemente como una buena práctica, las pruebas periódicas de Rebuild se han convertido en un pilar esencial de la gestión de riesgos empresariales. Al integrar los principios de viabilidad mínima mediante pruebas exhaustivas, las organizaciones pueden demostrar con fiabilidad su capacidad para restaurar rápidamente las funciones clave del negocio manteniendo al mismo tiempo una resiliencia digital completa. Esta capacidad ha pasado a ser un elemento fundamental para la supervivencia del negocio a medida que las ciberamenazas continúan evolucionando e intensificándose.

CAPÍTULO 4

Tu camino hacia el éxito: implementa la función *Rebuild* para una verdadera ciberresiliencia

La verdadera ciberresiliencia depende de una capacidad crítica que va más allá de los marcos tradicionales de ciberseguridad. Como se establecía en el Capítulo 2, el Marco de Ciberseguridad del NIST requiere una séptima función: Rebuild. Esta función transforma la incertidumbre en confianza, haciendo obsoletas actitudes tipo "Esperemos que el backup funcione", demostrando las capacidades de recuperación mediante pruebas periódicas.

El enfoque de viabilidad mínima descrito en el Capítulo 3 hace que esta transformación sea alcanzable. En lugar de intentar probarlo todo al mismo tiempo, las organizaciones pueden optar por implementar la función Rebuild de forma sistemática, empezando por los sistemas críticos para el negocio y expandiéndose a entornos completos. Este marco estratégico convierte un desafío abrumador en un proceso manejable, paso a paso, que ofrece valor inmediato mientras se construye una resiliencia integral.

La amenaza agéntica: cómo la velocidad de los ataques cambia los requisitos de recuperación

Los expertos estiman que ya este año podríamos comenzar a vivir en un mundo de atacantes autónomos, con agentes de IA como una opción atractiva para los ciberdelincuentes, ya que son mucho más baratos que contratar hackers profesionales y pueden orquestar ataques más rápidos y a una escala mucho mayor que los humanos.

El ransomware agéntico consiste en un conjunto de bots de IA (agentes) que ejecutan todos los pasos necesarios para llevar a cabo con éxito ataques de ransomware, pero más rápido y mejor que los operadores humanos. Estos sistemas no solo superan en velocidad a los métodos de ataque existentes, sino que cambian las reglas del juego al operar a velocidad de máquina con capacidades de aprendizaje automático.
Las implicaciones para la recuperación son profundas. En casi uno de cada cinco casos, las exfiltraciones de datos ocurren durante la primera hora tras producirse la brecha. Los métodos tradicionales de backup y recuperación, diseñados para amenazas a velocidad humana -que concedían días o semanas de alerta-, se vuelven obsoletos cuando el ataque pasa del reconocimiento al cifrado en cuestión de minutos.

Por eso, la función Rebuild, rápida y automatizada, es crítica especialmente en la era actual de los agentes autónomos. Solo mediante pruebas regulares y automatizadas es posible mantenerse por delante de unos adversarios que aprenden y se adaptan a velocidad sobrehumana.

El camino estratégico: de la viabilidad mínima a la resiliencia total

El camino hacia la confianza con la función Rebuild sigue un marco de viabilidad mínima que hace posible las pruebas integrales. Las organizaciones comienzan identificando sus sistemas críticos para el negocio, esenciales para mantener la viabilidad mínima durante una crisis. Luego, implementan snapshots de recuperación (PITR) y automatización RaC para estos sistemas de carácter prioritario.

El éxito con la viabilidad mínima crea una base para la expansión. Luego, las organizaciones podrán ampliar sus capacidades de Rebuild a los sistemas de misión crítica (contabilidad, gestión de la cadena de suministro…), y después a las aplicaciones no críticas. Cada ampliación está basada en procesos comprobados y en el progreso de la experiencia organizacional, hasta alcanzar la capacidad de reconstrucción integral en todo el ecosistema digital.

Las plataformas cloud a hiperescala que se mencionan en el Capítulo 3 hacen que esta progresión sea económicamente viable. Las instancias temporales (spot instances) reducen los costes de prueba hasta un 90%

en comparación con el precio bajo demanda, según la documentación oficial de AWS y Azure, mientras que las infraestructuras elásticas permiten validaciones frecuentes sin afectar los sistemas de producción.

Las pruebas de caos (Chaos Testing) aseguran que los escenarios de prueba reflejan fallos reales, lo que genera una confianza genuina en las capacidades de recuperación.

Superando los desafíos de implementación

El enfoque de viabilidad mínima aborda de manera sistemática los obstáculos organizacionales comunes para implementar Rebuild. De hecho, cuando los líderes expresan preocupación por los costes, el caso de negocio se vuelve convincente: la restauración rápida de sistemas generadores de ingresos se paga sola tras ayudar a evitar el primer incidente.

Ejemplos reales del Capítulo 3 lo demuestran: MGM Resorts y Caesars Entertainment contaban con planes de recuperación ante desastres (DR) integrales, pero ambas organizaciones tuvieron dificultades con la restauración porque carecían de capacidades probadas de Rebuild. El enfoque de viabilidad mínima podría haber facilitado la restauración rápida de las operaciones principales, centradas en el juego y la hostelería, mientras la recuperación total podría haberse desarrollado en paralelo, minimizando la interrupción del negocio y el impacto en los clientes.

De manera similar, la experiencia del NHS de Londres con el ransomware Qilin demostró que los backups sólidos no significan nada si no hay procedimientos de restauración verificados para aplicaciones, identidades y arquitecturas de red. Una estrategia de viabilidad mínima habría priorizado la restauración de los sistemas de atención al paciente, haciendo que las operaciones críticas de salud continuaran al tiempo que se reconstruían los sistemas administrativos y de soporte.

Limitaciones de presupuesto y recursos

La automatización RaC consolida manuales fragmentados en canales de trabajo unificados y controlados por versiones. Los equipos de seguridad, operaciones en la nube, aplicaciones y recuperación colaboran sobre la misma base de código, en lugar de mantener documentación separada y aislada. Esta consolidación elimina la necesidad de simulacros separados entre equipos, proporciona coherencia y reduce el esfuerzo manual.

El retorno de inversión pasa a ser evidente cuando la organización mide los tiempos de restauración de viabilidad mínima. Por ejemplo, reducir el RTO (objetivo de tiempo de recuperación) de 48 a 2 horas para sistemas críticos genera valor inmediato. La automatización de la recopilación de pruebas para SOC 2, ISO 27001 y DORA reduce la carga de auditoría, al tiempo que aporta validación continua para las capacidades de recuperación.

Apoyo al liderazgo y alineamiento organizacional

Nada impulsa más el apoyo del liderazgo que una capacidad demostrable. Las organizaciones pueden mostrar métricas de reconstrucción en tiempo real mediante paneles, poner informes de auditoría al alcance de los ejecutivos y demostrar recuperaciones completas en menos de una hora, en lugar de días o semanas.

El enfoque de viabilidad mínima hace que el impacto empresarial sea inmediatamente visible. Cuando el liderazgo ve que los sistemas generadores de ingresos pueden restaurarse de manera rápida y fiable, el financiamiento y el apoyo organizacional surgen naturalmente. Cada prueba exitosa de viabilidad mínima aumenta la confianza hacia una implementación más amplia de Rebuild.

Mirando hacia adelante: convirtiendo Rebuild en una práctica estándar

El futuro de la ciberresiliencia ya está emergiendo, impulsado por la realidad de las amenazas autónomas. A medida que la IA de agentes se vuelve más capaz, los equipos de seguridad delegarán más tareas en agentes autónomos, permitiendo que los sistemas y redes se mantengan al día ante unas tácticas de amenaza en constante evolución. En cinco años, la función Rebuild será tan fundamental para la ciberseguridad como las funciones actuales del marco del NIST. La planificación de viabilidad mínima será una práctica estándar, y las organizaciones mantendrán procedimientos de recuperación probados para sistemas críticos con el mismo rigor que mantienen sus controles financieros.

Esta transformación cambiará la forma en que las organizaciones abordan la resiliencia digital:

- *Capacidades Rebuild mejoradas con IA:* los sistemas del futuro aprovecharán la IA para identificar automáticamente desviaciones de configuración, predecir posibles fallos y llevar a cabo pruebas de caos sistemáticas que anticipen nuevos vectores de ataque antes de que se desplieguen. Estos sistemas de recuperación autónomos trabajarán junto a los humanos para asumir tareas rutinarias, mejorar la toma de decisiones y automatizar flujos de trabajo.
- *Respuesta ajustada en velocidad:* a medida que los ataques se aceleren, las capacidades Rebuild deberán hacerlo también. Las organizaciones implementarán sistemas de recuperación impulsados por IA capaces de restaurar entornos completos más rápido de lo que los atacantes autónomos pueden adaptar sus estrategias.
- *Ventaja competitiva:* las organizaciones que puedan demostrar una recuperación rápida y fiable obtendrán una importante ventaja competitiva. Los clientes y socios prefieren proveedores cuya continuidad de servicio está garantizada. En sectores regulados, probar las capacidades de Rebuild serán un requisito para mantener licencias y certificaciones.

Las organizaciones que adopten hoy la función Rebuild, comenzando con la viabilidad mínima y escalando hasta una cobertura total, serán no solo las que sobrevivan a los ataques del mañana, sino que saldrán fortalecidas de ellos, ya que podrán transformar situaciones de desastre para el negocio en desafíos operativos manejables.

El camino a seguir: de la esperanza a la confianza

La elección está clara: seguir esperando que los métodos tradicionales de backup y recuperación sean suficientes frente a las amenazas modernas, o comenzar a construir capacidades probadas de Rebuild que ofrezcan una confianza real.

El enfoque de viabilidad mínima hace que esta elección pueda llevarse a la práctica, ya que puedes comenzar con un único sistema crítico. Implementa snapshots PTIR y automatización RaC. Realiza pruebas de caos para validar la restauración bajo presión. Mide y demuestra los resultados.

El éxito con este primer sistema construye la base para una expansión sistemática. Cada nuevo sistema se beneficiará de la experiencia acumulada, los procesos probados y la automatización establecida. El viaje desde la "esperanza en que el backup funcione" hasta la confianza en la reconstrucción se acelerará a medida que las capacidades maduren. Primero, prueba tu viabilidad mínima; luego, expande sistemáticamente. Recupera con confianza mediante capacidades probadas de Rebuild. Prospera haciendo de la resiliencia una ventaja competitiva.

Las ciberamenazas del mañana serán más sofisticadas, persistentes y devastadoras que las actuales. Las organizaciones que esperen soluciones perfectas o condiciones ideales descubrirán que no están preparadas cuando su supervivencia dependa de la velocidad y fiabilidad de su recuperación.

Tu viaje, pues, debe comenzar entendiendo aquellos sistemas críticos para el negocio para implementar el marco de viabilidad mínima. La tecnología existe, y las metodologías están probadas. La única pregunta es si comenzarás ahora o esperarás hasta que el próximo ataque te obligue a hacerlo.

Elige la confianza. Elige Rebuild. Elige prosperar a través de la incertidumbre.

Sobre el autor

Govind Rangasamy es el fundador y CEO de Appranix, ahora parte de Commvault, y miembro del Forbes Technology Council. Emprendedor fundador de numerosas empresas y con una amplia experiencia en gestión de entornos cloud empresariales, Rangasamy fundó Appranix para revolucionar los modelos de resiliencia enfocados basados en la infraestructura, que considera inadecuados para las aplicaciones en la nube actuales, distribuidas y dinámicas. Asimismo, contribuye regularmente en Forbes y es un invitado frecuente en podcasts y conferencias sobre resiliencia en la nube.