Machine Translated by Google

Año VII, vol. 2, 2026 | Envío: 8 de octubre de 2026 | Aceptación: 10 de octubre de 2026 | Publicación: 13 de octubre de 2026

Resiliencia de los datos en infraestructuras híbridas: arquitectura, protección, recuperación y gobernanza.

Resiliencia de los datos en infraestructuras híbridas: arquitectura, protección, recuperación y gobernanza.
Resiliencia de los datos en infraestructuras híbridas: arquitectura, protección, recuperación y gobernanza.

Eduardo Eneas Pereira Nunes

Licenciatura en Ciencias de la Computación por la Universidad Estatal de São Paulo “Júlio de Mesquita Filho” (Unesp), campus São José do Rio Preto; Postgrado (Lato Sensu) en Redes de Telecomunicaciones por la Universidad Federal de Minas Gerais; MBA en Gestión de Proyectos de la Universidad de São Paulo (USP), campus de Piracicaba; Profesional en Tecnologías de la Información.

RESUMEN

La continuidad de los servicios digitales depende menos de la existencia abstracta de una copia de seguridad que de la capacidad demostrada para restaurar datos, aplicaciones y dependencias dentro de los límites aceptados por la empresa. Este artículo examina la resiliencia de los datos en infraestructuras híbridas, donde los recursos locales, virtualizados y en la nube conforman cadenas técnicas y contractuales difíciles de observar en su conjunto. El problema de investigación consiste en determinar qué dimensiones permiten evaluar una arquitectura de protección más allá de la adquisición de productos.

Se adoptó una revisión bibliográfica y documental cualitativa, respaldada por estándares, publicaciones institucionales y literatura científica. El análisis organiza seis dimensiones: arquitectura de almacenamiento, copias y aislamiento, ciberamenaza, objetivos de recuperación, gobernanza híbrida y validación operativa. Concluye que la resiliencia es una propiedad sistémica y medible, producto de la coherencia entre criticidad, diseño, controles, pruebas y aprendizaje. La capacidad contratada sin recuperación efectiva se queda solo en una expectativa.

Palabras clave: resiliencia de datos; almacenamiento; copia de seguridad; recuperación ante desastres; nube híbrida; gobernanza.

ABSTRACTO

La continuidad del servicio digital depende menos de la existencia abstracta de una copia de seguridad que de la capacidad demostrada para restaurar datos, aplicaciones y dependencias dentro de los límites aprobados por la empresa. Este artículo examina la resiliencia de los datos en infraestructuras híbridas, donde los recursos locales, virtualizados y en la nube conforman cadenas técnicas y contractuales difíciles de observar en su conjunto. El problema de investigación plantea qué dimensiones permiten evaluar una arquitectura de protección más allá de la adquisición del producto.

Se realizó una revisión bibliográfica y documental cualitativa utilizando estándares, publicaciones institucionales y literatura científica. El análisis se organiza en torno a seis dimensiones: arquitectura de almacenamiento, copias y aislamiento, ciberamenazas, objetivos de recuperación, gobernanza híbrida y validación operativa. El estudio concluye que la resiliencia es una propiedad sistémica y medible, creada por la coherencia entre criticidad, diseño, controles, pruebas y aprendizaje. La capacidad adquirida sin restauración practicada sigue siendo una expectativa más que una capacidad operativa.

Palabras clave: resiliencia de datos; almacenamiento; copia de seguridad; recuperación ante desastres; nube híbrida; gobernanza.

Palabras clave: resiliencia de datos; almacenamiento; copia de seguridad; recuperación ante desastres; nube híbrida; gobernanza.

INTRODUCCIÓN

La información digital ocupa una posición paradójica en las organizaciones contemporáneas. Sostiene transacciones, logística, relaciones con los clientes, investigación y decisiones administrativas, pero su utilidad

Este es un artículo de acceso abierto publicado bajo la licencia Creative Commons Attribution, que permite su uso.
Se permite su distribución y reproducción en cualquier medio, sin restricciones, siempre que se cite correctamente la obra original.

Machine Translated by Google

Año VII, vol. 2, 2026 | Envío: 8 de octubre de 2026 | Aceptación: 10 de octubre de 2026 | Publicación: 13 de octubre de 2026

Depende de una infraestructura que a menudo desaparece de la vista mientras está en funcionamiento.
La interrupción hace visibles, de repente, las dependencias entre almacenamiento, identidad, red,
aplicaciones y personas. El costo no solo proviene de la pérdida de archivos; incluye el tiempo de inactividad,
Reconstrucción, investigación, obligaciones legales y erosión de la confianza.

La expansión de la nube aumenta la capacidad y la flexibilidad, sin eliminar el problema de la continuidad.
Gartner estimó que el gasto mundial de los usuarios finales en servicios de nube pública aumentaría de
De 595.700 millones de dólares en 2024 a 723.400 millones de dólares en 2025, un crecimiento del 21,5% (GARTNER,
2024). El mismo movimiento distribuye los datos por región, cuenta, proveedor y modelo.
Responsabilidad. La complejidad arquitectónica, y no la falta de tecnología, se convierte en una fuente central.
exhibición.

NIST (Instituto Nacional de Estándares y Tecnología)
Tecnología) – una agencia del gobierno de los Estados Unidos adscrita al Departamento de Comercio –
Describe la evolución del almacenamiento, desde los servicios de bloques, archivos y objetos hasta las abstracciones.
definido por el software y el acceso a la nube. Para Chandramouli y Pinhas (2020), este camino
Esto aumenta la complejidad de la gestión y la probabilidad de errores de configuración. La observación elimina
Una interpretación puramente capacitista: más copias o más terabytes no significan, en sí mismos, mayor
Seguridad. Es necesario integrar los controles de acceso, el aislamiento, el cifrado, la integridad y la recuperación.
un diseño coherente.

Ante este escenario, el artículo se pregunta cómo evaluar la resiliencia de los datos en entornos híbridos.
sin reducirlo a la compra de copias de seguridad. El objetivo es construir una síntesis analítica que relacione
Arquitectura, amenazas, recuperación, gobernanza y evidencia operativa. No se pretende realizar ninguna comparación.
Los proveedores no deben informar sobre experiencias profesionales individuales. La contribución radica en convertir
Recomendaciones dispersas que abarcan diversos criterios y que pueden servir de guía para el diseño, la auditoría y la investigación aplicada.

METODOLOGÍA

La investigación es cualitativa, exploratoria y se basa en una revisión de la literatura y los documentos.
Selección de publicaciones científicas clásicas sobre computación en la nube, redundancia y sistemas.
distribuidos, además de los estándares y guías técnicas producidas por NIST, ISO, CISA, ENISA, CIS, IBM y
Gartner. Esta combinación permite cerrar la brecha entre los fundamentos perdurables y los datos de mercado recientes.
y amenazas.

La búsqueda conceptual priorizó los descriptores resiliencia de datos, seguridad de almacenamiento, copia de seguridad y recuperación ante desastres.
Recuperación, continuidad del negocio, nube híbrida, ransomware y objetivos de recuperación. Inclusión obligatoria
Autoría identificable, afiliación institucional o publicación académica reconocida, fecha y dirección.

Este es un artículo de acceso abierto publicado bajo la licencia Creative Commons Attribution, que permite su uso.
Se permite su distribución y reproducción en cualquier medio, sin restricciones, siempre que se cite correctamente la obra original.

Machine Translated by Google

Año VII, vol. 2, 2026 | Envío: 8 de octubre de 2026 | Aceptación: 10 de octubre de 2026 | Publicación: 13 de octubre de 2026

Código persistente o DOI (Identificador de Objeto Digital)

Un código alfanumérico único y persistente utilizado para identificar documentos y archivos digitales. Contenido

Los anuncios publicitarios solo se utilizaban cuando presentaban datos de investigación o cifras de mercado.

atribuible, pero nunca como prueba suficiente de la eficacia de un producto.

El corpus fue analizado por categorías. La primera categoría incluye estructura y redundancia; la segunda trata sobre protección,

Aislamiento e inmutabilidad; el tercero abarca el riesgo cibernético; el cuarto examina la continuidad, RPO y

El quinto apartado aborda la nube híbrida y la responsabilidad compartida; el sexto trata sobre las pruebas.

Indicadores y aprendizaje. Se compararon declaraciones entre diferentes tipos de fuentes para reducir

dependencia de una sola institución.

La Tabla 1 resume esta organización y explica la correspondencia entre cada dimensión y la pregunta.

que orienta tu lectura y las fuentes predominantes, haciendo que el camino analítico sea verificable.

Tabla 1 - Dimensiones analíticas, preguntas orientadoras y fuentes del corpus

Dimensión analítica: Pregunta que guía la lectura.		Principal fuentes movilizado
Arquitectura de almacenamiento	Cómo se construye la disponibilidad ¿En capas?	Patterson, Gibson y Katz (1988); Chandramouli y Piñas (2020)
Copias, aislamiento y integridad	La copia es recuperable e independiente. ¿De la producción?	Chandramouli y piñas (2020); CEI (2021)
Amenaza cibernética	El oponente logra la producción y ¿recuperación?	ENISA (2024); CISA (2023)
Objetivos de recuperación	RPO y RTO se derivan del análisis de ¿Qué impacto tendrá en el negocio?	Swanson et al. (2010); ISO 22301:2019
Gobernanza híbrida	¿Quién es el responsable de la clasificación? ¿Retención y salida?	Mell y Grance (2011); Armbrust et al. (2010); Gartner (2024, 2025)
Validación operacional	Hay evidencia de que la restauración ha sido probada. ¿Y con fecha de nacimiento?	CIS (2021); ISO/IEC 27001:2022

Fuente: elaboración propia (2025).

Las cifras financieras se presentan en dólares estadounidenses corrientes y respetan el marco temporal de la fuente.

Las predicciones se identifican como predicciones, no como resultados obtenidos. El gráfico reproduce

Valores publicados por Gartner en noviembre de 2024. Las limitaciones incluyen la rápida...

La evolución tecnológica, las diferencias regulatorias entre países y la ausencia de datos primarios sobre

organizaciones específicas.

Este es un artículo de acceso abierto publicado bajo la licencia Creative Commons Attribution, que permite su uso.
Se permite su distribución y reproducción en cualquier medio, sin restricciones, siempre que se cite correctamente la obra original.

Machine Translated by Google

Año VII, vol. 2, 2026 | Envío: 8 de octubre de 2026 | Aceptación: 10 de octubre de 2026 | Publicación: 13 de octubre de 2026

Las tablas y figuras de este artículo fueron creadas por el autor. Al reproducir datos de una fuente...
En el contexto primario, el origen se indica en el propio pie de foto; al organizar el contenido analizado en la reseña,
Se trata de resúmenes analíticos, y los valores de referencia son solo a título ilustrativo, sin intención de representar una medición.
empírico.
La interpretación adopta una lógica sociotécnica. Los controles se evalúan en relación con las personas,
procesos de negocio, contratos y objetivos, evitando la suposición de que la presencia de una herramienta
Demostrar la funcionalidad. La validez analítica se deriva de la trazabilidad de las fuentes y la coherencia.
Entre categorías, no se trata de una generalización estadística. Futuros estudios empíricos podrían poner a prueba el modelo.
en diferentes sectores y tamaños.

ARQUITECTURA DE ALMACENAMIENTO Y CONSTRUCCIÓN DE LA DISPONIBILIDAD

La disponibilidad moderna resulta de capas, no de un único componente infalible. El enfoque clásico
Patterson, Gibson y Katz (1988) demostraron cómo los arreglos de discos podían combinar la interpretación.
y tolerancia a fallos mediante redundancia. La idea sigue siendo relevante, pero necesita ser contextualizada:
RAID (Matrices redundantes de discos independientes)
Protege contra ciertos defectos en los soportes; no reemplaza las copias independientes ni el historial de versiones.
o recuperación tras un deterioro lógico.
La transición del almacenamiento conectado directamente a redes, sistemas distribuidos,
La hiperconvergencia y los servicios en la nube han aumentado las opciones de escalabilidad. También han multiplicado los planes para...
control, credenciales e interfaces. Chandramouli y Pinhas (2020) recomiendan que la seguridad
Considere la autenticación, la autorización, la configuración, la protección de medios, el aislamiento, el cifrado y...
Respuesta. El objeto protegido ya no es solo el volumen; incluye metadatos y mecanismos que lo hacen...
volumen útil.
La redundancia y la recuperabilidad pertenecen a categorías diferentes. Las réplicas síncronas pueden mantener
El servicio falla cuando falla un nodo, pero también puede propagar exclusiones, corrupción o acciones maliciosas.
Las copias versionadas conservan los estados anteriores, aunque pueden permanecer inaccesibles si...
Comparten credenciales o dominio administrativo con el entorno de producción. Una arquitectura madura.
Combina mecanismos con distintos modos de fallo.
La tabla 2 organiza esta distinción, relacionando cada mecanismo con las deficiencias que cubre eficazmente.
hasta los límites que preserva y el papel que desempeña en la recuperación del servicio.

Este es un artículo de acceso abierto publicado bajo la licencia Creative Commons Attribution, que permite su uso.
Se permite su distribución y reproducción en cualquier medio, sin restricciones, siempre que se cite correctamente la obra original.

Machine Translated by Google
RCMOS – Revista Científica Multidisciplinaria
Conocimiento. ISSN: 2675-9128. São Paulo-SP.

Año VII, vol. 2, 2026 | Envío: 8 de octubre de 2026 | Aceptación: 10 de octubre de 2026 | Publicación: 13 de octubre de 2026

Tabla 2 - Mecanismos de protección: fallas cubiertas, límites y función en la recuperación

Mecanismo	Protege contra	No protege contra	Papel en la recuperación
RAID y protección medios de comunicación	Fallo del disco, sector defectuoso	Exclusión lógica, corrupción, acceso con credencial válida	Mantener el servicio. disponible; no crea histórico
réplica sincrónica	Falla de nodo, controlador o sitio	Propagación inmediata de exclusión y corrupción	Apoya la operación; no ofrece un punto de devolver
Instantánea nodo mismo sistema	Error reciente de usuario o aplicación	Pérdida del sistema que aloja la instantánea	Regreso rápido a ventanas cortas
Respaldo versionado en otro dominio	Exclusión, corrupción y pérdida del sitio	Credencial privilegiada compartido con producción	Base del punto recuperación histórica
Copia inmutable (GUSANO)	Cambiar y eliminar durante la detención	Datos ya cifrados anteriormente para ser copiado	Garantiza la persistencia. de la versión conservada
Copia sin conexión o aislado (espacio de aire)	Ataque que llega al plan de control	Ventana de pérdida más amplia y restauración más lenta	Último recurso cadena confiable

Fuente: Elaboración propia basada en Patterson, Gibson y Katz (1988) y Chandramouli y Pinhas.

(2020).

La figura 1 convierte la misma lectura en una matriz de cobertura. La diagonal incompleta resalta...

El argumento central: ningún mecanismo único explica todos los modos de fallo y la resiliencia.

Esto resulta de una combinación de controles con fallos independientes.

Este es un artículo de acceso abierto publicado bajo la licencia Creative Commons Attribution, que permite su uso.
Se permite su distribución y reproducción en cualquier medio, sin restricciones, siempre que se cite correctamente la obra original.

Machine Translated by Google
RCMOS – Revista Científica Multidisciplinaria
Conocimiento. ISSN: 2675-9128. São Paulo-SP.

Año VII, vol. 2, 2026 | Envío: 8 de octubre de 2026 | Aceptación: 10 de octubre de 2026 | Publicación: 13 de octubre de 2026

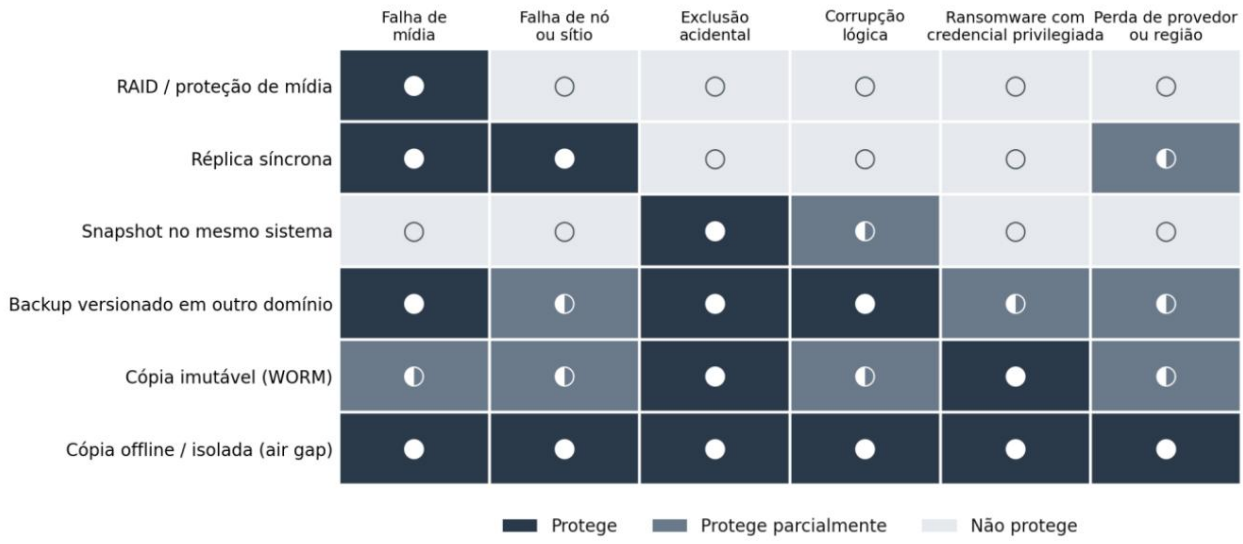

Figura 1 - Matriz de cobertura entre mecanismos de protección y modos de fallo. Fuente: [Nombre de la empresa]

propio (2025).

Otro punto es la granularidad. Las aplicaciones transaccionales requieren coherencia entre bancos, colas,

archivos y catálogos; copiar cada componente en momentos desconectados puede producir un conjunto

Es imposible reiniciarlo. Por lo tanto, la protección debe basarse en mapas de dependencias y estados consistentes.

El diseño físico solo adquiere sentido cuando se relaciona con la secuencia lógica de restablecimiento del servicio.

La clasificación de datos evita tratar todo de la misma manera. Criticidad, frecuencia de cambio,

La retención legal, la sensibilidad y el costo de recuperación guían las diferentes políticas. Una base

Los datos operativos pueden requerir una pérdida mínima permitida, mientras que un repositorio histórico tolera un margen mayor.

La diferenciación tiene costes e impide que las prioridades reales se disuelvan en una política uniforme.

La arquitectura debe, en última instancia, registrar sus premisas. Volumen, tasa de crecimiento, ventana de protección,

El ancho de banda, las dependencias y las responsabilidades deben ser medibles. Sin este inventario,

La capacidad está limitada por el desempeño pasado y falla silenciosamente ante el crecimiento. Proyecto

El término "resiliente" se refiere a una característica cuya idoneidad puede recalcularse cuando el entorno cambia.

COPIAS, AISLAMIENTO E INTEGRIDAD

La copia de seguridad es un proceso de preservación orientado a la recuperación, no un repositorio de archivos.

La calidad depende de la cobertura, la coherencia, la retención y la capacidad de localizar versiones.

Útil. Un alto índice de finalización de tareas puede ocultar aplicaciones y credenciales eliminadas.

Copias caducadas o lógicamente inconsistentes. El indicador central debería aproximarse al resultado.

restaurable.

Este es un artículo de acceso abierto publicado bajo la licencia Creative Commons Attribution, que permite su uso.
Se permite su distribución y reproducción en cualquier medio, sin restricciones, siempre que se cite correctamente la obra original.

Machine Translated by Google

Año VII, vol. 2, 2026 | Envío: 8 de octubre de 2026 | Aceptación: 10 de octubre de 2026 | Publicación: 13 de octubre de 2026

La separación entre dominios de fallos es un principio crucial. Si la producción y las copias dependen de...
Incluso con las mismas identidades privilegiadas, una credencial comprometida puede afectar a ambas. Aislamiento
Las medidas físicas, lógicas o temporales reducen esta propagación. NIST (2020) incluye protección, aislamiento y
La restauración garantizada se encuentra entre las recomendaciones específicas para la infraestructura de almacenamiento.
La tabla 3 compara las estrategias de redacción publicitaria que se utilizan con frecuencia en la práctica.
operativo, mostrando lo que añade cada disposición y qué limitaciones persisten tras su adopción.

Tabla 3 - Estrategias de redacción publicitaria: qué refuerzan y qué no resuelven

Estrategia el	Composición	Lo cual refuerza	Límite que queda
3-2-1	Tres copias, dos tipos de medios, uno fuera de lugar	Diversidad de los medios y dispersión geográfica	No requiere inmutabilidad. ni verificación de integridad
3-2-1-1-0	Agregar una copia inmutable o fuera de línea y No hay errores en la verificación.	Resistencia al ransomware y evidencia de copia legible	Costo y complejidad de gestión de retención
4-3-2	Cuatro copias, tres ubicaciones, dos fuera del sitio	Redundancia adicional para entornos regulados	Requiere orquestación y pruebas continuas

Fuente: elaboración propia basada en CISA (2023) y CIS (2021).

La inmutabilidad añade resistencia al cambio durante un período definido, pero no corrige la retención.
Un cifrado inadecuado no garantiza que el contenido esté limpio. Una copia inmutable de datos ya cifrados por
El atacante preserva el daño. El control debe estar asociado con la detección, versiones anteriores y análisis de...
Punto de recuperación. La tecnología útil se vuelve peligrosa cuando su etiqueta reemplaza la comprensión.
del mecanismo.

La criptografía protege la confidencialidad tanto en tránsito como en reposo, pero introduce una dependencia de la clave.
Las claves no disponibles hacen que una copia intacta sea inutilizable; las claves expuestas invalidan los datos.
Parte de la protección. Gestión del ciclo de vida, segregación de funciones, rotación y recuperación segura.
Deben integrarse en el mismo plan. La seguridad de las copias de seguridad incluye la seguridad de sus métodos de acceso.
La integridad requiere verificación continua. Los hashes y las validaciones detectan cambios, pero solo las pruebas...
Los procesos de lectura y restauración revelan problemas de catalogación, vinculación o compatibilidad.
La automatización puede aumentar el muestreo y la frecuencia, siempre que los fallos den lugar a tratamiento y no a
Solo se aceptan alertas acumuladas. La evidencia operativa debe incluir una persona asignada, una fecha límite y criterios de aceptación.
La retención también tiene dimensiones económicas y legales. Mantener todo indefinidamente aumenta
costo, superficie y complejidad de búsqueda; eliminando compromisos prematuros
Recuperación y responsabilidades. Las políticas deben conciliar las necesidades empresariales, la legislación y los litigios.

Este es un artículo de acceso abierto publicado bajo la licencia Creative Commons Attribution, que permite su uso.
Se permite su distribución y reproducción en cualquier medio, sin restricciones, siempre que se cite correctamente la obra original.

Machine Translated by Google
RCMOS - Revista Científica Multidisciplinaria
Conocimiento. ISSN: 2675-9128. São Paulo-SP.

Año VII, vol. 2, 2026 | Envío: 8 de octubre de 2026 | Aceptación: 10 de octubre de 2026 | Publicación: 13 de octubre de 2026

predecible y minimización. El resultado es una matriz de retención justificable, revisada y vinculada a clasificación de datos.

Ransomware y ciberresiliencia

El ransomware ha transformado la recuperación en un problema de seguridad estratégico. El panorama de ENISA (Agencia de la Unión Europea para la Ciberseguridad)

El informe sobre ciberseguridad para 2024 situó las amenazas a la disponibilidad en primer lugar, seguidas de cerca por el ransomware. seguido de un análisis de miles de incidentes reportados. Los datos sugieren que la confidencialidad Eso no es suficiente: la organización necesita mantener o reconstruir los servicios bajo presión y con acceso a la información. incompleto.

La figura 2 detalla esta distribución. Las amenazas a la disponibilidad y el ransomware, en conjunto, representan...

Las amenazas representan aproximadamente dos tercios de los incidentes analizados, y las amenazas a los datos ocupan el tercer lugar. El perfil refuerza la interpretación del artículo: la mayor parte del volumen observado ataca precisamente la capacidad. operar y regresar.

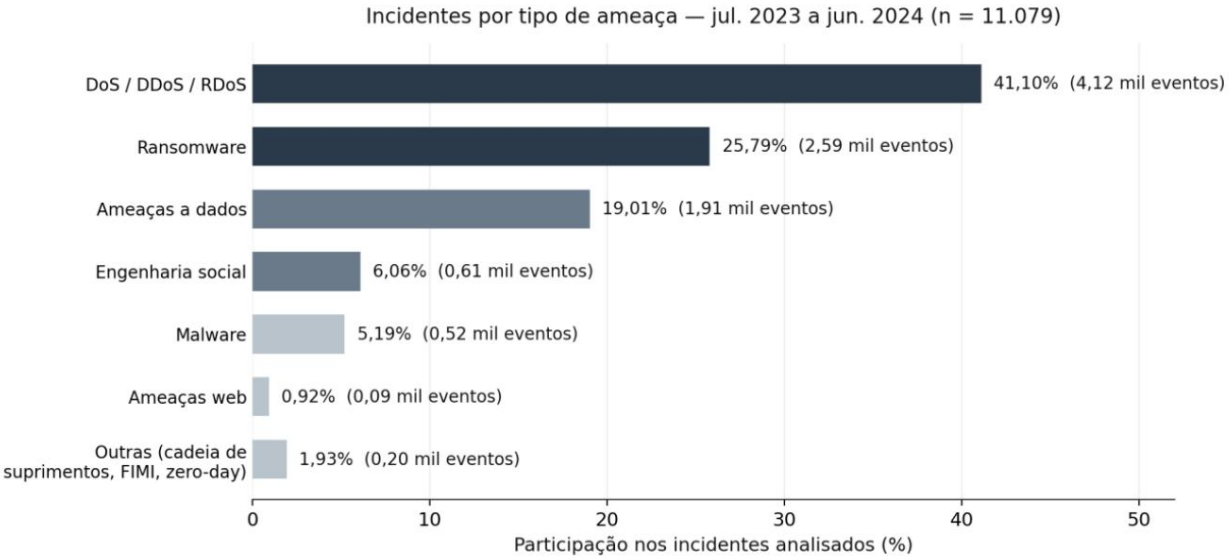

Figura 2 - Distribución de los incidentes analizados por tipo de amenaza, de julio de 2023 a junio de 2024.

Fuente: elaboración propia con datos de ENISA (2024).

Los ataques modernos tienen como objetivo las credenciales, las consolas de administración, los hipervisores y los sistemas de seguridad de los repositorios. Copia. La defensa no puede dar por sentado un perímetro intacto. Privilegios mínimos, autenticación robusta. La segregación de cuentas, las vías administrativas protegidas y el registro de acciones reducen la probabilidad de Un único punto de acceso puede dominar toda la cadena. El diseño debe tener en cuenta al adversario ya presente.

La Tabla 4 enumera los objetivos más frecuentes en la cadena de recuperación, el efecto previsto por El atacante, el control de prioridad y la evidencia que permite afirmar que dicho control está en funcionamiento.

Este es un artículo de acceso abierto publicado bajo la licencia Creative Commons Attribution, que permite su uso.
Se permite su distribución y reproducción en cualquier medio, sin restricciones, siempre que se cite correctamente la obra original.

Machine Translated by Google

Año VII, vol. 2, 2026 | Envío: 8 de octubre de 2026 | Aceptación: 10 de octubre de 2026 | Publicación: 13 de octubre de 2026

Tabla 4 - Objetivos del ransomware en la cadena de recuperación y controles correspondientes

Objetivo en prisión	Objetivo de agresor	Control de prioridad	Evidencia esperada
Identidad y cuentas privilegiado	Para obtener acceso amplia administración	Privilegio mínimo, Autenticación fuerte, cuentas apartado	Inventario de cuentas revisión privilegiada
Consola de respaldo	Reducir retención, para apagar empleos y catálogos	Dominio administrativo Aprobación doble y distinta	Registro de cambios política de retención
Hipervisor y plan de control	Cifrar muchos servicios individuales tiempo	Red de gestión segregada y registro de acciones	Registro de auditoría con revisión periódica
Repositorio de copias	Prevenir un regreso a estados anteriores	Inmutabilidad, Copiar aislado y credenciales propio	Restauración probada en partiendo de la copia aislada
Instantáneas y réplicas	Eliminar puntos de retornos recientes	Mantener fuera del alcance del informe de producción	Verificación automático de existencia y edad
Llaves de criptografía	Para dejarlo inutilizable copia completa	Custodia aislado, rotación y copia de recuperación	Ejercicio documentado de recuperación clave

Fuente: elaboración propia basada en CISA (2023), ENISA (2024) y Chandramouli y Pinhas (2020).

CISA (Agencia de Ciberseguridad y Seguridad de Infraestructuras)

(Infraestructura) recomienda copias de seguridad sin conexión, encriptadas y probadas como parte de la respuesta a

Ransomware. La palabra "probado" cambia el enfoque: almacenar no es lo mismo que recuperar. Ejercicios

Necesitan verificar los datos, la secuencia de carga, las identidades, las redes, las claves y la capacidad del equipo.

La restauración exitosa de un archivo no garantiza que todo el servicio vuelva a estar operativo dentro del plazo requerido.

La detección debe llegar al plano de datos. Cambios abruptos en la tasa de modificación, compresión,

Eliminaciones de cuentas o comportamientos pueden indicar un ataque antes de un bloqueo completo. Sin embargo,

Los umbrales estrictos generan falsos positivos en rutinas legítimas. La línea base debe tener en cuenta los ciclos.

Los procedimientos de cierre, las cargas analíticas y el mantenimiento se utilizan para distinguir las anomalías de la estacionalidad.

La recuperación tras un entorno comprometido puede reiniciar el incidente. Es necesario definir un área segura.

Criterios de confianza y pasos de validación antes de volver a conectar los sistemas. Imágenes, configuraciones y

Este es un artículo de acceso abierto publicado bajo la licencia Creative Commons Attribution, que permite su uso.
Se permite su distribución y reproducción en cualquier medio, sin restricciones, siempre que se cite correctamente la obra original.

Machine Translated by Google

Año VII, vol. 2, 2026 | Envío: 8 de octubre de 2026 | Aceptación: 10 de octubre de 2026 | Publicación: 13 de octubre de 2026

Es necesario examinar las credenciales; volver a autorizar las dependencias externas. La velocidad importa.
Sin embargo, una restauración apresurada podría prolongar el tiempo total de inactividad.
La comunicación es una parte integral de la resiliencia. Decisiones relativas a cierres, priorización, notificación y reanudación.
Incluye las áreas de gestión, legal, seguridad, operaciones y negocios. Los roles están predefinidos.
Reducen las disputas durante la crisis. Después del evento, el análisis debería transformar la evidencia en...
Correcciones arquitectónicas y de procedimiento, cerrando el círculo entre el incidente y el aprendizaje.

RPO, RTO y continuidad del negocio

Dos parámetros organizan la conversación sobre la recuperación. El objetivo de punto de recuperación, RPO, expresa
La pérdida máxima de datos permitida en el tiempo; el objetivo de tiempo de recuperación (RTO) indica el plazo.
deseado para la restauración. Ambos son objetivos, no características automáticas de un
herramienta. Deben derivarse del impacto en los procesos y enfrentarse a la capacidad técnica.
real.

Swanson et al. (2010) sitúan la planificación de contingencias dentro del ciclo de vida de los sistemas y
Recomiendan evaluar las operaciones para determinar las prioridades. El análisis del impacto empresarial proporciona
Esta conexión. Identifica los servicios esenciales, las dependencias, los efectos de las interrupciones y las tolerancias.
Sin esa base, RPO y RTO tienden a reflejar conveniencia técnica o ambición sin presupuesto.

Los objetivos ambiciosos tienen un coste. Reducir las pérdidas aceptables puede requerir una replicación frecuente, lo que se traduce en una mayor eficiencia.
Ancho de banda y mecanismos de captura consistentes. Reducción de los tiempos de respuesta.
Capacidad reservada, automatización y equipos capacitados. El equilibrio no se trata de elegir entre seguridad y...
economía, pero especifica cuánto cuesta cada nivel y qué pérdida pretende limitar.
La tabla 5 ilustra cómo la clasificación de criticidad traduce esta negociación en parámetros distintos.
por categoría de servicio, evitando políticas uniformes para necesidades desiguales.

Este es un artículo de acceso abierto publicado bajo la licencia Creative Commons Attribution, que permite su uso.
Se permite su distribución y reproducción en cualquier medio, sin restricciones, siempre que se cite correctamente la obra original.

Machine Translated by Google

Año VII, vol. 2, 2026 | Envío: 8 de octubre de 2026 | Aceptación: 10 de octubre de 2026 | Publicación: 13 de octubre de 2026

Tabla 5 - Clases de criticidad, objetivos de referencia y mecanismos asociados

Clase	Ejemplo de servicio	RPO / RTO de referencia	Mecanismo predominante	Costo relativo
Revisar	Transacción en línea, servicio hacia cliente	Minutos / hasta 1 hora	Replicación continuo con copia inmutable	Muy alto
Básico	ERP, facturación, integraciones	Hasta 1 hora / hasta 4 horas	réplica asíncrona y copias de seguridad frecuentes	Alto
Importante y	Colaboración, informes internos	Hasta 12 horas / hasta 24 horas	Respaldo a diario versionado	Moderado
De apoyo	Archivo histórico, archivos fríos	Hasta 24 horas / hasta 72 horas	Copia de seguridad periódica con retención prolongada	Bajo

Fuente: elaboración propia basada en Swanson et al. (2010) e ISO 22301:2019. Los intervalos son

Estos datos son ilustrativos y deben derivarse de un análisis del impacto en el negocio de cada organización.

La figura 3 representa la tendencia que sustenta esta diferenciación. A medida que los objetivos se convierten

Se vuelven más estrictos, el costo aumenta drásticamente, lo que explica por qué se requieren requisitos uniformes.

Suelen abandonarse en la práctica o financiarse únicamente en el discurso.

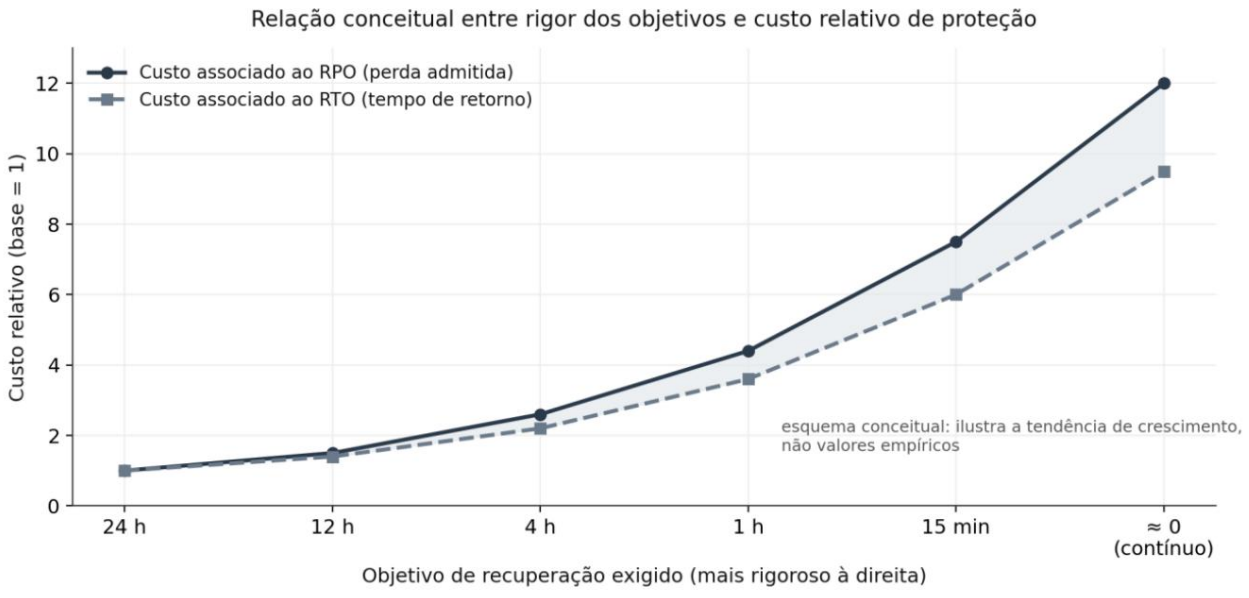

Figura 3 - Relación conceptual entre el rigor de los objetivos de recuperación y el costo relativo de la protección.

Fuente: elaboración propia (2025); esquema conceptual, sin valores empíricos.

La recuperación se produce de forma secuencial. La identidad, la red, los servicios de nombres, las bases de datos y las integraciones pueden verse afectadas.

Preceda a la aplicación visible para el usuario. Medir solo el tiempo de restauración del volumen subestima el

Este es un artículo de acceso abierto publicado bajo la licencia Creative Commons Attribution, que permite su uso.
Se permite su distribución y reproducción en cualquier medio, sin restricciones, siempre que se cite correctamente la obra original.

Machine Translated by Google

Año VII, vol. 2, 2026 | Envío: 8 de octubre de 2026 | Aceptación: 10 de octubre de 2026 | Publicación: 13 de octubre de 2026

Duración del servicio. Los mapas de dependencias y los manuales de procedimientos ordenados transforman el RTO en un plan.

Los archivos ejecutables permiten localizar cuellos de botella antes de que se produzca una crisis.

ISO 22301:2019 aborda la continuidad como un sistema de gestión, con política, análisis, estrategia,

Planes, ejercicios y mejora. Esta estructura evita que la recuperación sea un evento anual aislado.

Los cambios en la arquitectura, el equipo o el proveedor deberían dar lugar a una revisión de los planes. El objetivo

Solo se mantiene estable mientras sus premisas sigan siendo ciertas.

Las métricas deben distinguir entre intención y evidencia. Cobertura de la aplicación, antigüedad de la última copia.

Validez, porcentaje de restauraciones aprobadas, tiempo de observación y desviación del objetivo.

Proporcionan una visión más honesta. Los resultados deben segmentarse por criticidad; un promedio

En general, puede que esté ocultando precisamente el servicio que no puede fallar.

Nube híbrida, portabilidad y responsabilidad

La definición de nube del NIST hace hincapié en el acceso bajo demanda a un conjunto compartido de recursos.

configurable (MELL; GRANCE, 2011). El modelo traslada parte de la operación al proveedor, pero

No transfiere automáticamente la clasificación, retención, identidad y continuidad. Responsabilidades

Varían según el servicio y el contrato. Hacer suposiciones sobre ellas es un riesgo recurrente.

La Tabla 6 ilustra esta variación por modelo de servicio y muestra que la clasificación, las pruebas de

La restauración y la portabilidad permanecen con el cliente en todos los arreglos, incluso si la operación

cambio subyacente de manos.

Este es un artículo de acceso abierto publicado bajo la licencia Creative Commons Attribution, que permite su uso.
Se permite su distribución y reproducción en cualquier medio, sin restricciones, siempre que se cite correctamente la obra original.

Machine Translated by Google

Año VII, vol. 2, 2026 | Envío: 8 de octubre de 2026 | Aceptación: 10 de octubre de 2026 | Publicación: 13 de octubre de 2026

Tabla 6 - Distribución de responsabilidades por modelo de servicio

Artículo de protección	Instalación local	IaaS	PaaS	SaaS
Infraestructura física	Cliente	Proveedor	Proveedor	Proveedor
Ajustes de servicio	Cliente	Cliente	Proveedor compartido	
Clasificación de datos	Cliente	Cliente	Cliente	Cliente
Identidad y acceso del cliente		Cliente	Compartido	Compartido
Copia y retención	Cliente	Cliente	Compartido	Eso depende. de contrato
Gestión clave	Cliente	Cliente o compartido	Compartido	Proveedor o opcional
Prueba de restauración del cliente		Cliente	Cliente	Cliente
Portabilidad y salida del cliente		Compartido	Compartido	Eso depende. de contrato

Fuente: Elaboración propia basada en Mell y Grance (2011) y Armbrust et al. (2010). Atribución
La efectividad depende del contrato y del servicio contratado.

Armbrust et al. (2010) identificaron la elasticidad y las economías de escala como fuerzas impulsoras de la informática.
en la nube, junto con obstáculos como la disponibilidad, la dependencia del proveedor y la confidencialidad.
En entornos híbridos, estas tensiones se acumulan. Los datos pueden circular entre instalaciones dedicadas,
Software como servicio y múltiples regiones, cada una con diferentes mecanismos de protección y
exportar.

La portabilidad debe probarse, no inferirse de cláusulas genéricas. Formatos, API, metadatos,
Las claves y las tasas de salida influyen en la posibilidad de recuperación o migración. Una copia almacenada
dentro del mismo servicio, puede responder a exclusiones accidentales, pero ofrece poca independencia frente a
Indisponibilidad generalizada o rescisión del contrato. El escenario determina el grado de separación.
necesario.

La soberanía añade jurisdicción y ubicación al diseño. Normas de privacidad, acceso
Las transferencias gubernamentales e internacionales pueden limitar las regiones y los operadores. Gartner (2025)
Destacó la soberanía digital como una de las tendencias que están dando forma a la nube y predijo un crecimiento significativo.
de estrategias específicas en empresas multinacionales hasta 2029. Las predicciones no son hechos consumados, sino
Señalan la presión ejercida sobre el gobierno.

Este es un artículo de acceso abierto publicado bajo la licencia Creative Commons Attribution, que permite su uso.
Se permite su distribución y reproducción en cualquier medio, sin restricciones, siempre que se cite correctamente la obra original.

Machine Translated by Google

Año VII, vol. 2, 2026 | Envío: 8 de octubre de 2026 | Aceptación: 10 de octubre de 2026 | Publicación: 13 de octubre de 2026

Los costos variables requieren observabilidad financiera. Almacenamiento, solicitudes, recuperación y
Las transferencias pueden cambiar el costo total dependiendo de la retención y los ejercicios. Optimización que reduce
Copiar o realizar pruebas para ahorrar gastos puede aumentar la exposición operativa. FinOps aplicado a
La protección debe vincular el gasto con la criticidad, la cobertura y las pruebas de recuperación.
Los contratos completan la arquitectura. Niveles de servicio, notificación de incidentes, soporte, exclusión voluntaria,
La devolución de datos y la rendición de cuentas deben corresponder a los procesos técnicos. El diseño
La resiliencia incluye una estrategia de salida: cómo restablecerla en otro entorno, preservar las pruebas y dar por concluido el proceso.
Proveedor sin perder el control. Se puede gestionar la dependencia conocida; dependencia invisible.
Se convierte en una sorpresa.

GOBERNANZA, PRUEBAS E INDICADORES DE EFICACIA

La gobernanza comienza con la asignación de decisiones. Los responsables de los servicios definen la criticidad;
La tecnología traduce los requisitos; la seguridad establece los controles; el departamento legal interpreta las obligaciones; la gestión
Acepta el riesgo residual. ISO/IEC 27001:2022 organiza la seguridad de la información como un sistema de
Gestión orientada al riesgo, personas, políticas y tecnología. Cuando los roles se difuminan, los objetivos
Se convierten en listas sin autoridad. Una matriz de responsabilidades debería acompañar la arquitectura y...
para revisarlo con ella.

Las pruebas deben variar en profundidad. Se pueden realizar comprobaciones de integridad automatizadas diariamente;
Restauración de archivos, frecuente; recuperación de aplicaciones, periódica; simulacro de recuperación ante desastres, más frecuente.
completo y bien planificado. Cada capa responde a diferentes preguntas. Para confundir una prueba simple con
La validación completa genera confianza sin necesidad de pruebas equivalentes.
La tabla 7 distingue las capas de prueba por la pregunta que responde cada una y, sobre todo, por...
Esta pregunta deja la cuestión abierta, explicando por qué la verificación automática no reemplaza la práctica.
lleno.

Este es un artículo de acceso abierto publicado bajo la licencia Creative Commons Attribution, que permite su uso.
Se permite su distribución y reproducción en cualquier medio, sin restricciones, siempre que se cite correctamente la obra original.

Machine Translated by Google

Año VII, vol. 2, 2026 | Envío: 8 de octubre de 2026 | Aceptación: 10 de octubre de 2026 | Publicación: 13 de octubre de 2026

Tabla 7 - Capas de prueba, frecuencia de referencia y evidencia generada

Capa de prueba	Alcance verificado	Frecuencia de referencia	Evidencia generada	Pregunta que no respuesta
Verificación de integridad	Hash, lectura y catalogar	A diario	Copia legible y lleno	Si la aplicación Reanudar
Restauración de archivos	Artículos y directorios	Semanal	Recuperación granular funcional	Si el servicio devoluciones completas
Recuperación de solicitud	Servicio con su dependencias	Trimestral	Consistencia y secuencia de ascenso	Si el equipo actúa bajo presión
Ejercicio de desastre	Sitio, identidad, red y personas	Anual	Tiempo observado y verdaderos cuellos de botella	Cambios eventos que ocurrieron después ejercicio

Fuente: elaboración propia basada en CIS (2021), CISA (2023) e ISO 22301:2019.

CIS Controls v8 incluye la recuperación de datos entre sus controles esenciales y hace hincapié en el proceso.

Copias de seguridad, protección y pruebas documentadas y automatizadas. La fortaleza de este enfoque reside en...

Operacionalización. En lugar de tratar la continuidad como una intención, requiere salvaguardas observables.

Sin embargo, el uso responsable adapta la frecuencia y el alcance al riesgo, sin transformar en última instancia la lista de verificación.

Los indicadores deben permitir la acción. La tasa de éxito laboral es útil para las operaciones, pero insuficiente para...

Gobernanza. Cobertura por criticidad, restauraciones aprobadas, tiempo real versus RTO, punto.

La recuperación frente al RPO, las excepciones ganadas y la concentración por dominio de fallos ofrecen una lectura

Más completo. Las tendencias importan más que un retrato aislado.

La tabla 8 resume los indicadores analizados y asocia cada uno con su medida y lectura correspondientes.

lo que permite a la gobernanza separar las métricas operativas de las métricas de eficacia.

Este es un artículo de acceso abierto publicado bajo la licencia Creative Commons Attribution, que permite su uso.
Se permite su distribución y reproducción en cualquier medio, sin restricciones, siempre que se cite correctamente la obra original.

Machine Translated by Google

Año VII, vol. 2, 2026 | Envío: 8 de octubre de 2026 | Aceptación: 10 de octubre de 2026 | Publicación: 13 de octubre de 2026

Tabla 8 - Indicadores de eficacia de la protección de datos

Indicador	Cómo medir	Lectura sobre gobernanza
Cobertura poner criticidad	Servicios protegido en servicios clasificados, por clase	Revela brechas ocultas por promedio general
Edad de la última copia válido	Tiempo transcurrido desde la copia verificado más recientemente	Acerca el RPO real al objetivo. declarado
Restauraciones aprobado	Pruebas con criterios de aceptación respondió en relación con las pruebas realizadas	Mide la recuperación, no la finalización. tarea
Tiempo observado frente a RTO	Tiempo de devolución del servicio en ejercicio controlado	Muestra si el objetivo es ejecutable.
Punto recuperado frente a RPO	Diferencia entre el estado obtenido y la pérdida admitida	Deja al descubierto promesas sin mecanismo alguno. correspondiente
Excepciones vencidas	Desviaciones aceptadas cuyo plazo es La corrección ha caducado.	Indica el riesgo residual acumulado.
Concentración poner dominio de fallas	Copias que dependen de la misma identidad, sitio o proveedor	Señala la posible propagación de una evento único

Fuente: elaboración propia basada en CIS (2021), ISO/IEC 27001:2022 y Swanson et al. (2010).

La figura 4 muestra el crecimiento proyectado del gasto en la nube pública. El aumento de escala

Los factores económicos refuerzan la necesidad de controles que acompañan a la dispersión y la dependencia. No se debe...

Para concluir que un mayor gasto genera un mayor riesgo de forma lineal, el gráfico solo contextualiza la velocidad.

del mercado y la magnitud financiera de las decisiones arquitectónicas.

Este es un artículo de acceso abierto publicado bajo la licencia Creative Commons Attribution, que permite su uso.
Se permite su distribución y reproducción en cualquier medio, sin restricciones, siempre que se cite correctamente la obra original.

Machine Translated by Google
RCMOS - Revista Científica Multidisciplinaria
Conocimiento. ISSN: 2675-9128. São Paulo-SP.

Año VII, vol. 2, 2026 | Envío: 8 de octubre de 2026 | Aceptación: 10 de octubre de 2026 | Publicación: 13 de octubre de 2026

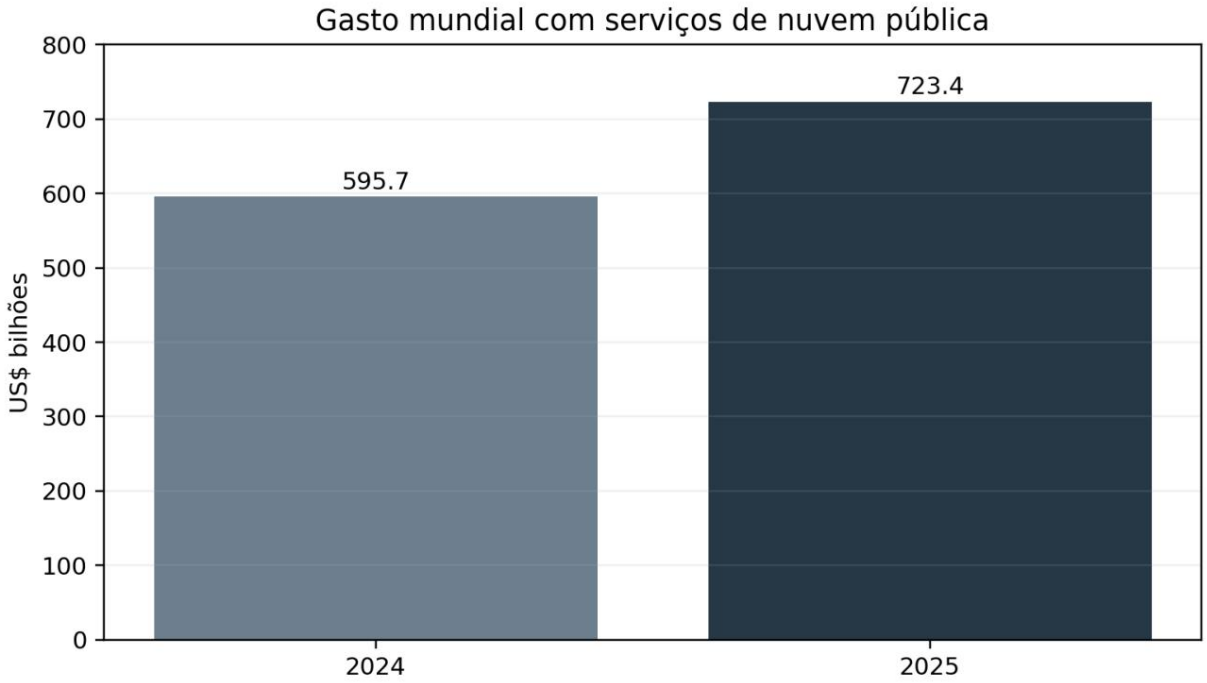

Figura 4 - Gasto global de los usuarios finales en servicios de nube pública, 2024-2025. Fuente:

Elaboración propia con datos de Gartner (2024).

El aprendizaje completa el ciclo. Cada fallo en las pruebas, cada cambio relevante y cada incidente deben contribuir al proceso.
Lista de tareas pendientes con prioridad, responsable y fecha límite. La gobernanza madura cuando cesan las desviaciones.
Estos eventos pueden ser episodios que conllevan cambios en patrones, contratos y habilidades. La resiliencia no es un estado del ser.
definitiva; es una disciplina de revisión frente a sistemas que están en constante cambio.

CONSIDERACIONES FINALES

El análisis demuestra que la resiliencia de los datos no se puede comprar como un atributo aislado.
surge de la articulación entre arquitectura, copias independientes, identidades protegidas y objetivos.
definido por el negocio, los contratos y las personas capaces de ejecutarlos. La presencia de redundancia o
La copia de seguridad es una condición parcial; la propiedad relevante es la recuperación comprobada del servicio.
La evolución tecnológica ha ampliado la escala y la flexibilidad, pero ha creado barreras de gestión. Entornos
Los sistemas híbridos combinan diferentes abstracciones y responsabilidades, por lo que los errores de configuración y
Las lagunas contractuales pueden neutralizar inversiones sólidas. Mapas de inventario y dependencias.
Hacen visible esta complejidad y, por lo tanto, la hacen manejable.
El ransomware pone de manifiesto por qué la disponibilidad y la seguridad han convergido. Un atacante busca lograr
Los mecanismos de producción y recuperación hacen que una defensa centrada en el perímetro sea insuficiente.

Este es un artículo de acceso abierto publicado bajo la licencia Creative Commons Attribution, que permite su uso.
Se permite su distribución y reproducción en cualquier medio, sin restricciones, siempre que se cite correctamente la obra original.

Machine Translated by Google

Año VII, vol. 2, 2026 | Envío: 8 de octubre de 2026 | Aceptación: 10 de octubre de 2026 | Publicación: 13 de octubre de 2026

La separación de privilegios, el aislamiento de copias, la detección y un área de restauración limpia comprenden un una cadena de acontecimientos que debe ensayarse antes del incidente.

RPO y RTO ofrecen un lenguaje común entre tecnología y gestión cuando se derivan del análisis de Impacto. Si se definen sin dependencias, presupuesto ni pruebas, se convierten en promesas. Mide lo que se observa. Trabajar en contra del objetivo convierte la intención en evidencia y permite negociar conscientemente el costo, el riesgo y prioridad.

El crecimiento financiero de la nube no elimina las responsabilidades organizativas. Proveedores Ofrecen funcionalidades importantes, pero la clasificación, la retención, la portabilidad y la continuidad también lo son. Los costos siguen siendo compartidos o responsabilidad del cliente, según el servicio. Contratos Deben reflejar la arquitectura real y, además, prever la salida, la investigación y la recuperación.

Los indicadores útiles evitan la comodidad de los promedios. Cobertura segmentada por criticidad y antigüedad de la copia. La validez, el tiempo de restauración y las excepciones revelan dónde se concentra el riesgo. Los paneles deben orientar Decisiones y correcciones; acumular métricas sin consecuencias solo digitaliza la inercia.

La principal implicación gerencial es tratar las pruebas como producción de conocimiento. Cada ejercicio Verifica supuestos, detecta cuellos de botella y entrena la coordinación. Fallos detectados en un entorno controlado. Los resultados son valiosos cuando conducen a la corrección. Una cultura que castiga las pruebas fallidas tiende a... Ocultar las debilidades hasta que sobreviene un desastre real.

Para los fines de esta investigación, siguen siendo posibles las comparaciones empíricas entre sectores, tamaños y modelos de nube. Los estudios futuros pueden vincular la madurez de la gobernanza con los tiempos de recuperación observados y Pérdidas evitadas, al tiempo que se preserva la confidencialidad. También vale la pena examinar cómo la automatización y La inteligencia artificial está transformando la detección, la priorización y generando nuevos modos de fallo.

En resumen, la pregunta correcta no es si la organización tiene copias de seguridad, sino a qué servicios puede acceder. Reconstruir, pero ¿desde qué punto, en qué plazo, bajo qué condiciones y con qué pruebas?

Cuando estas respuestas se verifican y revisan, la protección deja de ser simplemente un inventario tecnológico y Comienza a funcionar como una capacidad institucional.

REFERENCIAS

ARMBRUST, Michael et al. Una visión de la computación en la nube. Communications of the ACM, Nueva York, vol. 53, n.º 4, págs. 50-58, 2010. DOI: 10.1145/1721654.1721672.

CENTRO PARA LA SEGURIDAD EN INTERNET. Control de seguridad crítico 11 de CIS: Recuperación de datos. East Greenbush: CIS, 2021. https://www.cisecurity.org/controls/data-recovery.

CHANDRAMOULI, Ramaswamy; PINHAS, Doron. Directrices de seguridad para la infraestructura de almacenamiento. Publicación especial 800-209 del NIST. Gaithersburg: NIST, 2020. DOI: 10.6028/NIST.SP.800-209.

CISA. #GuíaParaDetenerElRansomware. Washington, DC: Agencia de Ciberseguridad y Seguridad de Infraestructura, 2023. https://www.cisa.gov/stopransomware/ransomware-guide.

ENISA. Panorama de amenazas de ENISA 2024. Atenas: Agencia de la Unión Europea para la Ciberseguridad, 2024. https://www.enisa.europa.eu/publications/enisa-threat-landscape-2024.

Este es un artículo de acceso abierto publicado bajo la licencia Creative Commons Attribution, que permite su uso.
Se permite su distribución y reproducción en cualquier medio, sin restricciones, siempre que se cite correctamente la obra original.

Machine Translated by Google

Año VII, vol. 2, 2026 | Envío: 8 de octubre de 2026 | Aceptación: 10 de octubre de 2026 | Publicación: 13 de octubre de 2026

GARTNER. Gartner pronostica que el gasto mundial de los usuarios finales en la nube pública ascenderá a 723 mil millones de dólares en 2025. Stamford, 19 de noviembre de 2024. https://www.gartner.com/en/newsroom/press-releases/2024-11-19-Gartner pronostica que el gasto mundial de los usuarios finales en la nube pública alcanzará los 723 mil millones de dólares en 2025.

GARTNER. Gartner identifica las principales tendencias que dan forma al futuro de la nube. Stamford, 13 de mayo de 2025. https://www.gartner.com/en/newsroom/press-releases/2025-05-13-gartner-identifies-top-trends-shaping-the-future-of-cloud.

ORGANIZACIÓN INTERNACIONAL DE NORMALIZACIÓN. ISO 22301:2019: Seguridad y resiliencia - Sistemas de gestión de la continuidad del negocio - Requisitos. Ginebra: ISO, 2019.

ORGANIZACIÓN INTERNACIONAL DE NORMALIZACIÓN. ISO/IEC 27001:2022: Seguridad de la información, ciberseguridad y protección de la privacidad - Sistemas de gestión de la seguridad de la información - Requisitos. Ginebra: ISO, 2022.

MELL, Peter; GRANCE, Timothy. Definición de computación en la nube del NIST. Publicación especial 800-145 del NIST. Gaithersburg: NIST, 2011. DOI: 10.6028/NIST.SP.800-145.

PATTERSON, David A.; GIBSON, Garth; KATZ, Randy H. Argumentos a favor de las matrices redundantes de discos económicos (RAID). En: Conferencia Internacional ACM SIGMOD sobre Gestión de Datos, 1988, Chicago. Actas [...]. Nueva York: ACM, 1988. págs. 109-116.
DOI: 10.1145/50202.50214.

SWANSON, Marianne et al. Guía de planificación de contingencias para sistemas de información federales. Publicación especial NIST 800-34 Rev. 1. Gaithersburg: NIST, 2010. DOI: 10.6028/NIST.SP.800-34r1.

Este es un artículo de acceso abierto publicado bajo la licencia Creative Commons Attribution, que permite su uso.
Se permite su distribución y reproducción en cualquier medio, sin restricciones, siempre que se cite correctamente la obra original.