arcserve®

Estado de la capacidad de recuperación de datos en la empresa

Perspectivas de otros expertos e ideas que invitan a la reflexión para evaluar y mejorar la capacidad de recuperación de datos de su organización

Investigación independiente encargada por Arcserve

Resumen

Introducción

La capacidad de recuperación de datos se ha convertido en un factor crucial para la supervivencia de la mayoría de las organizaciones, y es probable que la suya no sea una excepción. Con el crecimiento explosivo y la proliferación de herramientas basadas en IA, el riesgo de sufrir un ataque de ransomware o una filtración de datos sigue aumentando a medida que los ciberdelincuentes encuentran nuevas formas de burlar o superar sus ciberdefensas de primera línea. Incluso la Agencia Federal de Investigación (FBI) advirtió recientemente sobre la creciente amenaza de los ciberdelincuentes que aprovechan la inteligencia artificial para aumentar «la velocidad, la escala y la automatización de los ciberataques».[1]

Al mismo tiempo, cada vez más empresas se embarcan en sus propias iniciativas de IA; quizá la suya también. Estos proyectos casi siempre requieren grandes cantidades de datos privados y se paralizan si esos datos se pierden o son robados. Además, una vez finalizado el entrenamiento del modelo, los datos de entrenamiento deben conservarse con fines de gobernanza y cumplimiento (por ejemplo, para respaldar una auditoría antiprejuicio de las predicciones del modelo).

El 97 %
de los encuestados está de acuerdo en que los datos privados son «moderadamente» o «extremadamente» críticos para el éxito de su empresa.

El 69 %
de los encuestados afirma que las operaciones comerciales de su organización se detendrían si perdiera el acceso a sus datos.

Mientras tanto, todos los riesgos «heredados» para sus datos siguen ahí: agentes maliciosos (especialmente con el trabajo remoto), errores accidentales de los usuarios, desastres naturales, etc.

Arcserve encargó un estudio a profesionales de TI de alto nivel directamente implicados en la copia de seguridad y la protección de datos para comprender mejor cómo afrontan las pequeñas y medianas empresas estos retos en constante evolución. Nos complace compartir con usted nuestros resultados y algunas de nuestras ideas para mitigar los riesgos de pérdida de datos y el tiempo de inactividad.

Esperamos que esta perspectiva de los retos de protección de datos de sus homólogos y de cómo reaccionan ante ellos le ayude a reflexionar a la hora de evaluar la estrategia de capacidad de recuperación de datos de su organización y sus posibles carencias. Puede que incluso le ayude a respaldar sus recomendaciones a las partes interesadas internas.

El equipo de Arcserve

1 El FBI advierte de la creciente amenaza de los ciberdelincuentes que utilizan inteligencia artificial. 8 de mayo de 2024

Copyright © 2024 Arcserve (USA), LLC, sus afiliadas y subsidiarias. Todos los derechos reservados. Todas las marcas registradas, nombres comerciales, marcas de servicio y logotipos mencionados aquí pertenecen a sus respectivas compañías.

La aprobación de los ejecutivos es importante. 1 de cada 4 aún no la tiene.

Implantar las mejores prácticas de protección de datos y ciberseguridad con tecnologías eficaces requiere inversiones en TI y de otro tipo. Es indispensable contar con la aprobación de los directivos que manejan los hilos de la empresa.

Demasiados directivos siguen sin dar prioridad a la capacidad de recuperación de datos, y nuestros datos anecdóticos corroboran esta conclusión. En conversaciones con pequeñas y medianas empresas, oímos cosas como: «Somos demasiado pequeños para que nos ataquen». La cruda realidad es que no lo son. Cuando les «atacan», probablemente son demasiado pequeñas para salir en las noticias.

El éxito de una iniciativa de capacidad de recuperación de datos empieza en la cúpula, con la implicación de los líderes empresariales y el consejo de administración. Pero, como cualquier iniciativa de cambio, necesita el apoyo y la aceptación cultural de toda la empresa, desde la oficina central hasta la primera línea, pasando por todos los departamentos. También requiere la alineación y el compromiso de partners y proveedores de servicios.

Más del 25 %
de los encuestados no puede decir que los líderes de su empresa se preocupen por cuidar adecuadamente los datos de la organización.

y sin embargo...

El 69 %
de los encuestados afirma que las operaciones comerciales de su organización se detendrían si perdiera el acceso a sus datos privados.

La publicación de la Agencia de Ciberseguridad y Seguridad de las Infraestructuras, «Making a Business Case for Security»,[2] ofrece consejos útiles para conseguir la implicación de los ejecutivos.

Crecen las inversiones en protección de datos

Los encuestados afirman que su organización de TI ya invierte una cantidad sustancial de su presupuesto de TI en la protección y recuperación de datos.

Sin embargo, la elevada desviación estándar (21 %) entre las respuestas corrobora la conclusión anterior de que, posiblemente, un número considerable de empresas invierte muy poco en este ámbito. Presumiblemente, los presupuestos generales de TI más reducidos imponen a los responsables de TI compromisos difíciles.

El siguiente dato ofrece cierta tranquilidad: en su inmensa mayoría, los responsables de TI aspiran a aumentar su presupuesto de protección de datos.

Un 22 %
es la parte media del presupuesto de inversión en TI de la organización de los encuestados asignada a la protección y recuperación de datos.

El 89 %
de las organizaciones encuestadas espera aumentar su presupuesto de protección de datos en el futuro.

Puede que les resulte útil el Informe sobre el presupuesto de seguridad de 2023, que muestra que el presupuesto medio de seguridad informática aumentó un 6 %. En general, se trata de un ritmo de crecimiento un 65 % más lento que antes.[3] En muchos casos, sin embargo, el crecimiento debe acelerarse en el ámbito de la protección de datos.

Aunque se asigne un mayor presupuesto a la protección de datos, ¿cómo puede una organización aprovecharlo al máximo?
Es importante tener en cuenta las ventajas y desventajas de tener un mosaico dispar de componentes configurados individualmente y ajustados con precisión y una solución integrada y unificada que haga el trabajo de forma fiable. La primera puede ofrecerle oportunidades únicas de personalización, mientras que la segunda debería ser más fácil de implantar y más rápida a la hora de aportar valor.

2 Argumentos empresariales a favor de la seguridad I Una práctica recomendada del Comité de Seguridad Interinstitucional. Edición de 2023
3 Informe resumido del presupuesto de seguridad de 2023

Recuperación de datos y continuidad de negocio

Parte 1: El tiempo es esencial

¿Cuáles serían los costes -en dinero y en daños a la reputación- si su empresa no pudiera acceder a sus datos?

He aquí algunas indicaciones de fuentes acreditadas:

Solo el 31 %
de los encuestados confía en su capacidad para recuperar datos perdidos en 24 horas.

Riesgos financieros	Riesgos de cumplimiento	Riesgos de reputación
• **2,7 millones de dólares:** coste medio de recuperación de ransomware, sin contar los pagos de rescates (Sophos State of RANSOMWARE: 2024) • **2 millones de dólares:** pago medio del rescate, +50 % interanual • **9000 dólares/minuto:** coste medio del tiempo de inactividad para las grandes organizaciones (Forbes) • **5 millones de dólares/hora** para organizaciones de alto riesgo (finanzas, sanidad) • **4,4 millones de dólares:** coste medio de una filtración de datos en 2023	• **EE. UU.:** Ley de privacidad de datos (CCPA) • **Europa:** RGPD • **Japón:** Ley de protección de datos personales	• Relaciones dañadas con clientes, partners y partes interesadas

¿Tardar más de 24 o 48 horas en recuperarse es aceptable para las empresas?

Hicimos esa pregunta, y la respuesta fue un rotundo no para dos de cada tres empresas.

Solo el 34 %
de los encuestados afirma que su organización puede tardar más de 48 horas en recuperar sus datos y evitar una interrupción significativa de la actividad empresarial.

Parte 2: La práctica hace al maestro

Aunque la buena noticia es que la mayoría de las organizaciones (70 %) afirma realizar simulacros de recuperación de datos semanales o mensuales, más de una de cada cinco empresas no comprueba sus sistemas con la frecuencia suficiente.

El 70 %
de los encuestados afirma que su empresa realiza simulacros semanales o mensuales de recuperación de datos para garantizar la continuidad de negocio.

Los simulacros periódicos de recuperación de datos son esenciales porque ayudan a garantizar que el objetivo de tiempo de recuperación (RTO) y el objetivo de punto de recuperación (RPO) de la organización puedan cumplirse cuando se produce un desastre.

Riesgos heredados: Duras lecciones para muchos. Exceso de confianza, ¿para algunos?

Muchos responsables de TI con los que hemos hablado son veteranos. Han visto esta película antes, y han visto materializarse los riesgos.

Casi la mitad de los encuestados respondieron «sí» cuando se les preguntó si habían experimentado pérdidas significativas de ingresos debido a incidentes de pérdida de datos.

Reflexione sobre este hallazgo y su impacto en los líderes de las organizaciones. Para quienes se centran en aumentar los ingresos y controlar los costes, esta perspectiva de pérdida de ingresos debería ser una llamada de atención. Pero no fue ninguna sorpresa oír a los encuestados expresar confianza en su postura:

El 47 %
de los encuestados afirma que su organización ha experimentado una pérdida significativa de ingresos debido a incidentes de pérdida de datos.

De forma abrumadora, los responsables de TI con los que hemos hablado afirman confiar en su capacidad para detectar y recuperarse de amenazas a sus datos procedentes de riesgos heredados, como amenazas internas y catástrofes naturales.

El 86 %
de los encuestados afirma que su organización confía «mucho» o «muchísimo» en su capacidad para detectar catástrofes naturales y reaccionar ante ellas.

De hecho, el informe «2024 Verizon Data Breach Investigations» descubrió que el **25 %** de las filtraciones implicaban a usuarios de dentro de la organización.[4] Mientras tanto, según la NOAA, hasta julio de 2024 se han confirmado quince catástrofes meteorológicas o climáticas en Estados Unidos, con pérdidas **superiores a 1000 millones de dólares cada una**.

Estas amenazas «establecidas» de pérdida de datos ya son conocidas y comprendidas. Y no, no van a desaparecer.

Lo sorprendente, entonces, fue lo que oímos en relación con nuestra pregunta de seguimiento. ¿Puede explicarse este nivel de confianza por su adopción de las prácticas recomendadas en torno a la estrategia de copia de seguridad 3-2-1-1?

El 23 %
de los encuestados afirma que su organización no ha adoptado la estrategia de copia de seguridad 3-2-1-1, y otro 6 % no está seguro.

Resulta que casi una de cada cuatro organizaciones puede estar confiando demasiado en esto.

Ransomware: Amplio impacto y consecuencias duraderas

¿Sabía que…?

El último «1» en 3-2-1-1 significa almacenamiento de copias de seguridad inmutable, vital para sus esfuerzos de recuperación tras desastres y prevención de pérdida de datos. Las copias de seguridad inmutables se guardan en un formato de una sola escritura, lectura múltiple (WORM), que los usuarios no autorizados no pueden alterar ni borrar, por lo que constituyen una defensa de última línea contra la pérdida de datos.

Con un entorno de amenazas en desarrollo y el crecimiento de los servicios de ransomware (RaaS), ser víctima de un ataque de ransomware es una cuestión de cuándo, no de si.

Hemos oído a responsables de TI decir que se sienten preparados. En la práctica, no todos los datos se recuperan tras un ataque.

El 80 %
de las organizaciones encuestadas se han visto afectadas por ransomware.

30 %
30 % es el porcentaje medio de datos que los encuestados no pudieron recuperar tras sufrir un ataque de ransomware.

Y el proceso de recuperación sigue siendo lento y perturbador para la empresa.

Hemos visto que la mayoría de las organizaciones no pueden permitirse tardar más de 48 horas en recuperarse de un incidente de datos y mantener alguna esperanza de evitar el impacto en los ingresos.

El 82 %
de los encuestados afectados por ransomware afirma que se recuperó en 48 horas, mientras que el 18 % no lo hizo.

Las catástrofes naturales, las amenazas internas y el ransomware están ahora siempre presentes. Lo que ha cambiado para estos factores de riesgo es que su probabilidad de ocurrencia ha aumentado, al igual que su impacto si (cuando) se materializan.

La preparación es la mejor defensa. Su objetivo debe ser una sólida infraestructura de capacidad de recuperación de datos que consolide sus componentes de protección, copia de seguridad y recuperación en un entorno de protección de datos unificado, implementado como parte de una estrategia de copia de seguridad 3-2-1-1.

Aplicaciones SaaS: Un pilar infravalorado de la capacidad de recuperación de datos

Hoy en día, las aplicaciones SaaS desempeñan un papel crucial en casi todas las organizaciones.

Aproximadamente el 82 % de los encuestados indica que sus organizaciones utilizan diez o más aplicaciones SaaS, lo que pone de relieve la escala y su importancia en la empresa moderna. Estas aplicaciones generan y utilizan una gran cantidad de datos, vitales para mantener el buen funcionamiento de las operaciones y la satisfacción de los clientes.

Muchas organizaciones tienen un punto ciego cuando se trata de datos dentro de esas aplicaciones:

Solo una fracción de las aplicaciones SaaS es supervisada y protegida por las propias organizaciones.

El 59 %
de las organizaciones encuestadas utilizan entre 10 y 30 aplicaciones SaaS

El 19 %
utilizan entre 30 y 50

El 30 %
de las aplicaciones SaaS no están supervisadas ni protegidas

Entre el 70 % que sí están supervisadas o protegidas, el 40 % tiene esa responsabilidad externalizada o desatendida

Los datos de SaaS suelen estar sujetos al modelo de responsabilidad compartida, en el que el propietario de los datos (es decir, su organización) es responsable de su protección y recuperación.

Ejemplo: Modelo de responsabilidad compartida de Microsoft

	Cliente	Microsoft
Preparación	• Continuidad de negocio y planificación en caso de catástrofe • Documentación de estados buenos conocidos • Supervisión y retención de datos • Seguridad operativa	• Funciones de administración de identidades y accesos • Herramientas de documentación • Disponibilidad y coherencia de los registros • Seguridad de la plataforma
Recuperación	• Restauración de recursos suprimidos por software • Restauración de configuraciones anteriores	• Disponibilidad de recursos suprimidos por software (por tiempo limitado) • Disponibilidad de API

Y, sin embargo, entre el 40 % de los encuestados que afirma que su empresa ha sufrido una pérdida de datos debido a la violación de una aplicación SaaS en el último año, algo más de la mitad (51 %) considera que su proveedor de SaaS es el culpable.

Con este contexto adicional, la importancia de las soluciones de copia de seguridad SaaS se hace evidente, ya que ofrecen un alto grado de seguridad y autonomía para las organizaciones que desean preservar sus datos SaaS sin depender de los propios proveedores de aplicaciones SaaS.

El impacto del incumplimiento

Los requisitos de cumplimiento existen desde hace décadas y no hacen más que reforzarse. Paralelamente, el cumplimiento de las normas es cada vez más difícil, ya que la infraestructura informática es cada vez más compleja.

Por ejemplo, la reciente Directiva NIS2 de la UE introdujo más cobertura y requisitos normativos para el sector.
En todo el mundo se están desarrollando marcos normativos que podrían tener un impacto similar en el futuro.

Casi la mitad de los encuestados confirma que sus organizaciones han tenido que hacer frente a multas reglamentarias provocadas por medidas inadecuadas de protección de datos.

Directiva NIS2, artículo 21, apartado 2:
Las medidas ... se basarán en un enfoque que tenga en cuenta todos los riesgos y cuyo objetivo sea proteger los sistemas de información de la red y el entorno físico de dichos sistemas frente a incidentes, e incluirán al menos lo siguiente:

Sección (c): Continuidad de negocio, como administración de copias de seguridad y recuperación tras desastres, y administración de crisis[5]

El 43 % de las empresas encuestadas han tenido que hacer frente a multas reglamentarias debido a medidas inadecuadas de protección de datos.

Garantizar que su empresa cumpla las normativas pertinentes, como GDPR, CCPA e HIPAA, no solo es vital para su reputación. No hacerlo puede salirle caro.

¿Cuál es la mejor manera de cumplir la normativa? La más difícil es que sus equipos internos busquen asesoramiento y orientación a través de terceros. La forma más fácil es emplear una solución de capacidad de recuperación de datos con palancas de cumplimiento integradas, como controles de acceso y versionado.

5 DIRECTIVA (UE) 2022/2555 DEL PARLAMENTO EUROPEO Y DEL CONSEJO de 14 de diciembre de 2022 relativa a medidas para un elevado nivel común de ciberseguridad en toda la Unión, por la que se modifican el Reglamento (UE) n.º 910/2014 y la Directiva (UE) 2018/1972, y por la que se deroga la Directiva (UE) 2016/1148 (Directiva NIS 2).

Resumen

Aunque las organizaciones mejoran sus prácticas de protección de datos y su capacidad de recuperación de datos, el riesgo de pérdida de datos y la importancia de garantizar la continuidad de negocio siguen siendo temas prioritarios para los responsables de TI. Al mismo tiempo, existen discrepancias visibles entre las expectativas y la realidad, ya que las organizaciones profesan su dedicación a la protección de datos y, sin embargo, siguen sufriendo las consecuencias de la pérdida de datos.

Y no es ninguna sorpresa. Con el ransomware y otras amenazas potenciales, surgen nuevos riesgos para las empresas pequeñas y grandes (e intermedias). En general, los responsables de TI buscan inversiones adicionales en protección de datos, copia de seguridad y recuperación tras desastres. Seguir las prácticas recomendadas sobre el terreno puede ayudar a maximizar la protección con presupuestos limitados.

Como pionero en la capacidad de recuperación de datos, Arcserve está bien posicionado para ayudar. Arcserve Unified Data Protection (UDP) y Arcserve SaaS Backup son soluciones de capacidad de recuperación de datos rentables, fáciles de implementar y rápidas para ofrecer valor al garantizar la recuperación y minimizar el tiempo de inactividad y la pérdida de datos.

Arcserve está aquí para responder a sus preguntas y mostrarle cómo proteger mejor sus datos dondequiera que residan.
Si desea más información, póngase en contacto con nosotros en arcserve.com/es/contact-us
Explore todas las funciones de Arcserve en arcserve.com/es/products-overview
Póngase en contacto con nosotros en info@arcserve.com

METODOLOGÍA

Arcserve quería comprender mejor cómo los responsables de la seguridad de los datos pueden volver a sus actividades en caso de que se produzca una filtración de datos o una interrupción del servicio. Arcserve encargó a una empresa de investigación independiente que encuestara a 150 líderes de seguridad de datos de Estados Unidos sobre recuperación de datos y capacidad de recuperación de datos. La audiencia se divide a partes iguales entre PYMES (<1000 empleados) y grandes empresas (entre 1000 y 5000 empleados). El margen de error de este estudio es de +/- 6,9 % con un nivel de confianza del 95 %.

Para ver las soluciones de capacidad de recuperación de datos de Arcserve en acción, solicite una demostración en arcserve.com/es/request-demo

Acerca de Arcserve

Arcserve, uno de los 5 principales proveedores de protección de datos del mundo, ofrece el conjunto más amplio de soluciones de primera clase para gestionar, proteger y recuperar todas las cargas de trabajo de datos, desde pymes hasta grandes empresas e independientemente de su ubicación o complejidad. Las soluciones de Arcserve eliminan la complejidad a la vez que aportan la mejor seguridad y protección de datos de su clase, es rentable, ágil e increíblemente escalable en todos los entornos de datos. Esto incluye infraestructuras locales, externas (incluidas DraaS, BaaS y de nube a nube), hiperconvergentes y perimetrales. Las cuatro décadas de IP galardonada de la empresa y su continuo foco en la innovación significan que sus partners y clientes, incluidos los MSP, VAR, LAR y los usuarios finales, tienen asegurada la ruta más rápida a las cargas de trabajo e infraestructuras de datos de próxima generación.

Copyright © 2024 Arcserve (USA), LLC, sus afiliadas y subsidiarias. Todos los derechos reservados. Todas las marcas registradas, nombres comerciales, marcas de servicio y logotipos mencionados aquí pertenecen a sus respectivas compañías.