Insights

Resumen ejecutivo

# Tendencias de ransomware 2024

## Edición para LATAM

Según el informe Tendencias de protección de datos 2024, elaborado a partir de las entrevistas a responsables de TI e implementadores de 10 países en todo el mundo:

- Solo el 25 % de las organizaciones creen que no fueron atacadas por ransomware en 2023
- El 49 % afirma haber sido atacado entre una y tres veces ese año.
- El 26 % de las organizaciones declararon que fueron atacadas cuatro o más veces

Debido a los altos porcentajes de ataque que se muestran en este informe imparcial todos los años, se encargó la realización del informe Tendencias de ransomware con el objetivo de comprender mejor los ataques, las recuperaciones y las lecciones aprendidas. Para elaborar el informe, se utilizó una encuesta anónima doble ciega a los líderes de TI seleccionados con experiencia de primera mano en esos ciberataques para profundizar aún más en el tema a través de un estudio adicional: Informe Tendencias de ransomware 2024.

## Análisis del informe Tendencias de ransomware 2024

El informe Tendencias de ransomware 2024 es la tercera publicación anual de un estudio imparcial realizado por un equipo de analistas independientes que encuestó a organizaciones anónimas pero seleccionadas que, en los últimos 12 meses, sufrieron al menos un ciberataque que tuvo éxito. Cada año, este informe recopila 1 200 respuestas con un desglose intencionado de aproximadamente 400 personas en tres roles clave que son responsables de una parte de la estrategia de ciberresiliencia de una organización:

- **CISO o alto ejecutivo:** Responsable de la estrategia de ciberresiliencia de una organización
- **Profesional de seguridad de la información:** Responsable de la prevención y detección de incidentes cibernéticos
- **Administrador de backups:** Responsable de la protección y recuperación continua de los datos de TI

El ransomware sigue siendo una preocupación creciente para todo el mundo dentro de la industria de TI. Gartner pronostica a nivel mundial un aumento planificado del 3,5 % en los presupuestos generales de TI para 2024. En esta encuesta, los encuestados de LATAM esperan aumentos presupuestarios de:

**6,2%**

Aumento del presupuesto para tecnologías de ciberprevención y detección

**5,9%**

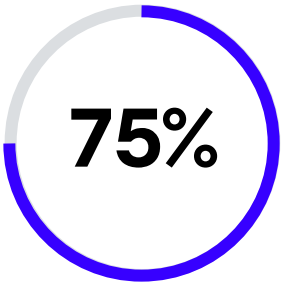
aumento del presupuesto para tecnologías de recuperación como el backup y la continuidad del negocio/recuperación ante desastres (BCDR)

El gasto global en TI ha aumentado, y los presupuestos para la ciberresiliencia se han incrementado hasta casi duplicar el aumento general del gasto en TI. Por lo tanto, las inversiones en backup y ciberseguridad están acaparando "más de lo que les corresponde" del aumento de las inversiones en TI y se está restando prioridad a otras áreas para dárselo a la lucha contra las ciberamenazas. Copias de backup limpias, que se supone contienen datos que "han sobrevivido" a los ataques y no contienen código malicioso.

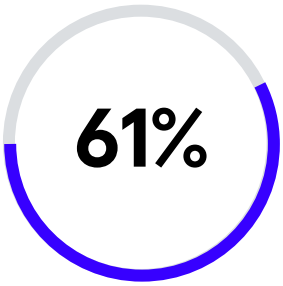
# El 63 % de las organizaciones no están coordinadas

Por tercer año consecutivo, más de la mitad de las organizaciones (69 % en LATAM) creen que es necesaria una "mejora significativa" o una "revisión completa" para que las organizaciones puedan coordinar a sus equipos de backup y de ciberseguridad.

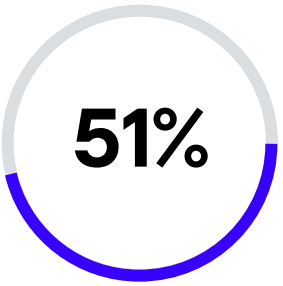
A nivel global, de los tres roles encuestados, los administradores de backups fueron los menos satisfechos con la coordinación de sus equipos.




de los administradores de backups creen que es necesaria una reestructuración completa de sus sistemas




de los profesionales de la seguridad buscan cambios en su organización




de los CISO u otros ejecutivos equivalentes tienen preocupaciones sobre la coordinación dentro de su organización

# Hará falta la unión de todos para recuperarse

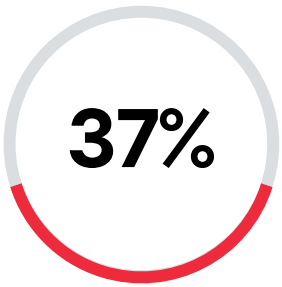
Según los encuestados, los dos equipos que reciben notificaciones con más frecuencia para poner en marcha los esfuerzos de remediación son los ejecutivos responsables de la prevención y remediación y el equipo de backups de TI. A esto le siguen inmediatamente los expertos en ciberseguridad y el equipo general de gestión de riesgos de la organización.

El 89 % de las organizaciones encuestadas declararon que también recurrieron a terceros durante el proceso de recuperación, siendo estos cuatro tipos de expertos los más contratados:

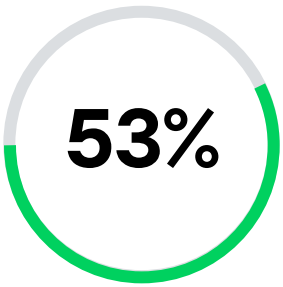
- **Proveedores de software de seguridad**
- **Proveedores de software de backup**
- **Especialistas en seguridad forense**
- **Revendedores, socios o proveedores de servicios**

# Lo más probable es que pierda el 18 % de sus datos después de un ciberataque

Dos de las estadísticas más impactantes de las 1200 lecciones globales que aprendimos en 2023 son:




de los datos de producción fueron cifrados con éxito por personas mal intencionadas en los ataques del año pasado




de los datos afectados pudieron recuperarse tras ser cifrados en un ataque de ransomware

Desgraciadamente, si solo el 53 % de sus datos pudo recuperarse, el 47 % no se recuperaron; por tanto, el 17 % de sus datos de producción fueron irrecuperables. En esta encuesta, participaron organizaciones de todos los tamaños y sorprendentemente pusieron de manifiesto que ni el tamaño de su organización ni su ubicación tenían un efecto significativo en sus porcentajes de ataque o recuperabilidad. Todas las organizaciones sufrieron aproximadamente la misma cantidad de impactos en todo el mundo y se enfrentaron a una cantidad de daños parecida.

Las organizaciones también se sorprendieron al descubrir que no hubo una variación significativa entre los efectos del centro de datos que se detectaron en las oficinas remotas frente a las sucursales, o incluso en los datos alojados en una nube pública frente a una privada.

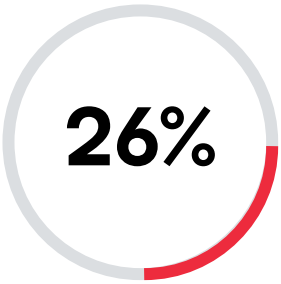
# ¿Pagó el rescate? ¿Funcionó?

Dos preguntas clave que se hacen cada año en esta encuesta son:

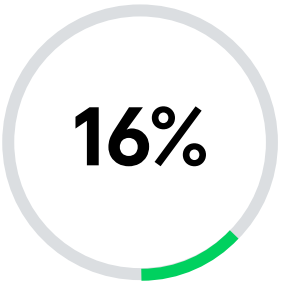
- **¿Pagó el rescate?**
- **¿Pudo recuperar los datos?**

## En 2023 dentro de LATAM:


Pagaron y pudieron recuperar sus datos tras el ataque




Pagaron pero no pudieron recuperar los datos perdidos en el ataque




Recuperados *sin pagar* el rescate exigido

Los resultados globales fueron similares:

- El 54 % pagó y pudo recuperar sus datos tras el ataque
- El 27 % pagó pero no pudo recuperar los datos perdidos en el ataque
- El 15 % recuperó los datos sin pagar el rescate exigido

Con el restante 4 %, no se pidió ningún rescate. Estas estadísticas son significativas, sobre todo porque muestran que aproximadamente **una de cada cuatro de las organizaciones que pagaron el rescate no pudo recuperar sus datos *incluso después de pagar***.

# Un ataque va más allá del rescate

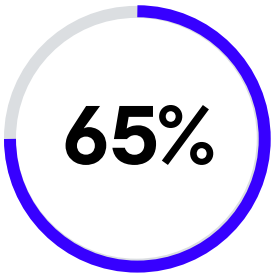
El 73 % de las organizaciones creen que están protegidas por un seguro, aunque el 21 % de esas pólizas de seguro excluyen específicamente el ransomware. Sin embargo, los costes de la prevención, detección, servicios de recuperación y el propio rescate no son, ni mucho menos, los únicos factores económicos que pueden afectar a su organización en caso de sufrir un ataque de ransomware. De hecho, de todas las respuestas a la encuesta de este año, solo 1 de cada 9 organizaciones (11 %) declaró que el pago de un rescate generó la mayor parte del impacto financiero general para su organización. Para el resto de víctimas cibernéticas, el impacto económico global fue sustancialmente mayor que "solo" el rescate en sí.

# El 65 % de las organizaciones pagaron su rescate con dinero del seguro

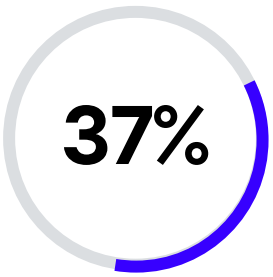
En cuanto a las políticas internas de las empresas en 2023, solo un número reducido de organizaciones (14 %) no tenía una política sobre si pagar o no un rescate. Si bien la mayoría de las organizaciones tenían una política, ***las opiniones estaban casi igualmente divididas hacia pagar (49 %) y no pagar (38 %)***.

Independientemente de si tenían una política o no, no debería sorprender a nadie que, si bien solo una minoría de las organizaciones tenía una política de pagar, el 76 % terminó pagando. Dicho esto, el 66 % pagó con un seguro y otro 17 % tenía un seguro, pero optó por pagar sin reclamarlo. Esto significa que en 2023, el 83 % de las organizaciones tenían un seguro que podrían haber utilizado para un ciberevento.

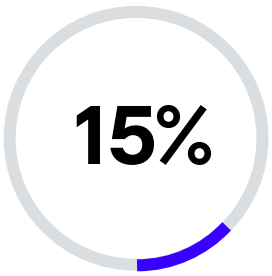
Estas opciones disminuirán a medida que los ciberseguros sigan cambiando como respuesta al aumento de las reclamaciones. En la última renovación:




de las organizaciones recibieron un recargo como respuesta al cambiante panorama de las TI




sufrieron un aumento de su franquicia debido a que el ransomware y los ciberataques se hicieron más frecuentes




vieron reducidos sus beneficios de cobertura a medida que las compañías de seguros trataban de protegerse de la creciente amenaza del ransomware

# Los ciberdelincuentes quieren sus backups

De la misma manera que el manual de su equipo de prevención tiene como objetivo realizar un backup limpio y recuperable, el manual del ciberdelincuente tiene como objetivo desactivar su capacidad para recuperar sus propios datos. Desafortunadamente, en demasiados ataques, los atacantes logran eliminar su capacidad para salvarse. Así pues, los datos muestran que solo el 16 % de las organizaciones se recuperaron sin pagar. De media, el 36 % de los repositorios de backup se vieron afectados por un ataque que tuvo éxito.

# El 72 % no tienen un plan de recuperación

En el 95 % de las organizaciones (que tenían un equipo con un plan), los dos aspectos más frecuentes de su manual de respuesta a incidentes eran la garantía de unos datos ***limpios*** y ***recuperables***.

Esto explica por qué el 28 % de las organizaciones de LATAM tienen una infraestructura alternativa en sus planes, lo cual significa, desgraciadamente, que el otro 72 % no tiene un plan sobre dónde se recuperarán después de una crisis a nivel de ubicación.

Sin embargo, los ciberataques no solo afectan a la organización y sus equipos, sino que también atrapan a las personas en la refriega. De los encuestados este año, los efectos personales clave incluyeron el aumento de la carga de trabajo, el estrés y otros factores humanos que la mayoría de las organizaciones ya luchan por equilibrar o mitigar incluso en días "normales".

# El ataque será peor de lo que imaginaba y le costará más de lo que esperaba

Con el 37 % de los datos afectados por un ciberataque y con solo el 53 % de los datos afectados recuperables, es razonable que las organizaciones esperen perder un 17 % de los datos en cada ciberataque. Además, el rescate promedio representa solo el 37 % del impacto financiero total, en tanto que solo el 68 % del impacto total es de alguna manera reclamable a través de seguros u otros medios. A esto se suma todo lo demás que va en contra del presupuesto mínimo de la organización.

# 2024: la inmutabilidad aún no es suficiente

En 2024, no es descabellado que las organizaciones adopten el almacenamiento inmutable dentro de sus discos locales, complementado con repositorios cloud inmutables y cintas aisladas. Desgraciadamente, incluso de todos aquellos que han sufrido al menos un ciberataque en el pasado, solamente el 76 % utiliza discos endurecidos en las instalaciones y solo el 80 % utiliza nubes con inmutabilidad.

**Solo el 49 % del almacenamiento de backup total de la organización es inmutable.**

Dicho esto, es alentador que las organizaciones estén adoptando la regla 3-2-1 estándar de la industria de tener múltiples tipos de medios, independientemente de si esos tipos de medios pueden ser inmutables o no. En 2024, además de los repositorios de disco que hay en las instalaciones, el 45 % de los datos de producción se conservan en al menos una cinta, mientras que el 52 % también se replica en una nube.

Este informe de investigación se basa en 1200 respuestas a encuestas, incluidas 250 de LATAM. Todos los encuestados eran líderes y ejecutores de TI imparciales responsables de las estrategias de ciberresiliencia de sus organizaciones, como CISO, profesionales de seguridad de TI y administradores debackups. La encuesta se realizó a principios de 2024 y se publicó en junio de 2024. Los datos fueron seleccionados y las opiniones fueron redactadas por dos antiguos analistas del sector, anteriormente de ESG y Gartner, con una experiencia combinada de 70 años en protección de datos.

Las preguntas sobre este estudio y la información/recursos publicados a partir de ella se pueden enviar a StrategicResearch@veeam.com

## El punto de vista de Veeam

Veeam® cree que un backup seguro es su mejor línea de defensa contra el ransomware. Veeam se ha comprometido a que las organizaciones reduzcan el tiempo de inactividad y la pérdida de datos, para que nunca tengan que pagar un costoso rescate. Solo Veeam ofrece el mayor número de opciones de recuperación del mercado, y un formato de datos verdaderamente portable que le capacitan para recuperar en cualquier lugar: de lo físico a lo virtual, entre nubes o incluso de la nube a un centro de datos en las instalaciones locales. No existe una solución mágica para resolver el problema del ransomware, y por eso Veeam aplica un enfoque multicapa para la protección y recuperación frente al ransomware.
Para obtener más información, visite https://www.veeam.com/ransomware-protection.html

### Acerca de Veeam Software

Veeam®, el líder n.º 1 del mercado mundial en protección de datos y recuperación de ransomware, tiene la misión de dotar a todas las organizaciones no solo de lo que necesitan para recuperarse de una interrupción o una pérdida de datos, sino también para seguir adelante. Con Veeam, las organizaciones logran una resiliencia radical a través de seguridad de datos, recuperación de datos y libertad de datos para su nube híbrida. Veeam Data Platform proporciona una solución única para entornos cloud, virtuales, físicos, SaaS y Kubernetes que proporciona a los responsables de TI y seguridad la tranquilidad de saber que sus datos y aplicaciones están siempre protegidos y disponibles. Con sede en Seattle y oficinas en más de 30 países, Veeam protege a más de 450 000 clientes en todo el mundo, incluido el 74 % de las empresas de Global 2000, que confían en Veeam para mantener sus negocios en funcionamiento. La resiliencia más innovadora comienza con Veeam.

Obtenga más información o http://www.veeam.com siga a Veeam en LinkedIn (@veeam-software) y X (@veeam).