White Paper

Por qué la recuperación rápida es más segura que pagar el rescate

Patrocinado por: Veeam

Johnny Yu Jennifer Glenn Phil Goodwin

Junio de 2022

INTRODUCCIÓN

Cada minuto de inactividad puede conllevar pérdidas de miles de dólares para la empresa. Cuando el *ransomware* ataca, pagar el rescate puede resultar tentador, pero no es la solución rápida que buscan las organizaciones.

El pago no siempre garantiza la recuperación, y mucho menos que ésta sea adecuada. Según la Worldwide Future Enterprise Resiliency and Spending Survey (Encuesta mundial sobre la resistencia y el gasto de las empresas del futuro) de IDC, menos del 28 % de los encuestados pudieron recuperar tras pagar el rescate (véase la imagen 1).

Además, pagar el rescate no es tan sencillo como parece. Cuando una organización decide pagar el rescate, los responsables deben dedicar, en primer lugar, tiempo a sopesar la decisión con el equipo jurídico y otras partes que puedan verse afectadas. A continuación, el equipo puede dedicar tiempo a negociar con los ciberdelincuentes. Luego, se invierte aún más tiempo en el proceso de descifrado en sí y, como se señala en la misma encuesta, el proceso de descifrado puede incluso fallar en algunos casos.

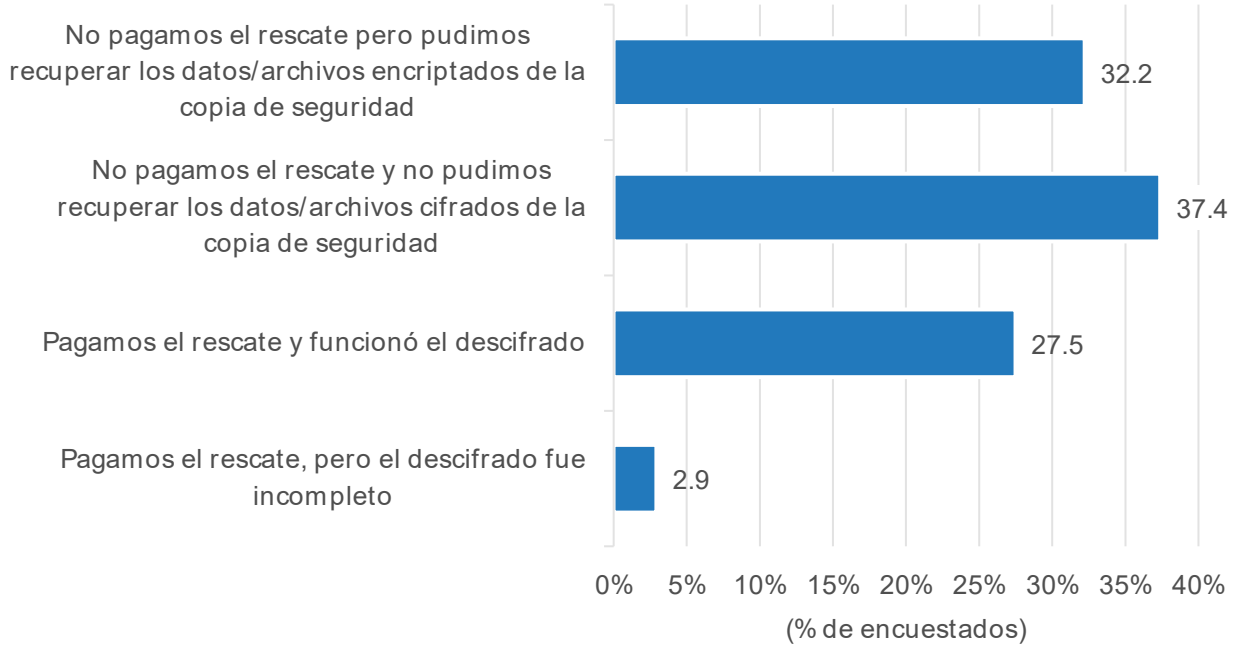
Optar por no pagar el rescate también tiene sus propios riesgos. La encuesta reveló que menos de un tercio de los participantes fue capaz de recuperar los datos cifrados de sus archivos de copia de seguridad. Sin embargo, este número puede incrementarse, pues ahora se dispone de herramientas y técnicas para configurar un plan de recuperación de datos fiable y rápido. Con ellas, las empresas pueden centrar sus esfuerzos –y su valioso tiempo– en la recuperación sin tener que dedicar ciclos de gasto en decidir si se paga el rescate.

Junio de 2022, IDC #US49290622

IMAGEN 1

Menos de un tercio de las organizaciones son capaces de recuperarse por sí mismas

P: En el último incidente de ransomware que bloqueó el acceso a sus sistemas o datos, ¿cuál de las siguientes situaciones se produjo?



n = 444

Notas:

Los datos son gestionados por el Grupo de Investigación Cuantitativa de IDC.

Los datos no están ponderados.

Se recomienda prudencia al interpretar tamaños de muestra pequeños.

Fuente: *Encuesta mundial sobre la resistencia y el gasto de las empresas del futuro* de IDC, diciembre de 2021

Crear una recuperación rápida y fiable

El *ransomware* suele ser un conjunto de ataques que llegan a través de las defensas de seguridad y acceden a información esencial para usarla como rehén. Aunque evitar por completo los ataques de *ransomware* es, sin duda, la mejor solución para proteger los datos, no siempre es posible. Las exigencias de las empresas digitales en cuanto a servicios ágiles, soluciones innovadoras y disponibilidad permanente requieren que la seguridad no obstaculice las operaciones. Esto también significa que no basta con confiar solo en la protección.

En su lugar, las organizaciones de éxito están ampliando sus esfuerzos de protección de datos para centrarse en una recuperación rápida y fiable que mantenga las operaciones en movimiento y la información a salvo. Esto incluye:

- **Detección:** identificar las anomalías e intrusiones de seguridad y actuar con rapidez
- **Protección:** crear y mantener copias limpias e inmutables de los datos esenciales
- **Recuperación:** reponer rápidamente los datos y aplicaciones esenciales para la empresa

El primer paso para una recuperación rápida y fiable es saber inmediatamente cuándo se produce un incidente de seguridad y detenerlo. Para ello, las organizaciones tienen que saber dónde se alojan sus datos, las características de estos, quién o qué tiene acceso a ellos y cómo pueden utilizarse. Con esta información, los equipos de TI y operaciones de seguridad pueden colaborar en la creación de políticas que determinen qué usuarios o dispositivos pueden acceder a ciertos tipos de datos, así como cuándo y cómo pueden utilizarse.

Una vez definidas estas políticas, pueden aplicarse a diversos puntos de control de seguridad y gestión de datos para proteger la información sensible de accesos no autorizados, usos indebidos o fuga/robo. Estas políticas pueden ajustarse a medida que surgen nuevos riesgos o cambian las operaciones de la empresa. También proporcionan una base de protección de datos que puede configurar los procesos de respuesta a incidentes y manuales de técnicas ante cualquier futuro ataque de *ransomware* que pueda surgir.

El componente de protección de la recuperación rápida de *ransomware* implica tener copias de seguridad de los datos limpias y de acceso rápido desde las que recuperar. Las herramientas que hacen que las copias de seguridad sean difíciles de comprometer, como el cifrado, el almacenamiento inmutable y el *air gapping*, ya llevan algunos años en el mercado y, probablemente, sean conocidas por los profesionales de la protección de datos.

Aparte de las herramientas en sí, es necesario igualmente aplicar las mejores prácticas de protección de datos. Esto incluye tener varias copias de respaldo de los datos guardadas en varias ubicaciones, así como restringir quién puede borrar o sobrescribir las copias de seguridad o iniciar una recuperación.

El componente de recuperación y atenuación para la recuperación rápida del *ransomware* es similar a cualquier proceso de recuperación de interrupciones no planificadas, pero con algunos pasos adicionales. Una respuesta integral al *ransomware* debe incluir la seguridad en el proceso de recuperación. La recuperación inicial debe llevarse a cabo en un entorno aislado para que los equipos de seguridad puedan efectuar análisis forenses y analizar las copias de seguridad en busca de *malware* o signos de intrusión.

Una vez establecido un método de recuperación, éste debe probarse periódicamente. Esto garantiza que las copias de seguridad sean recuperables y también proporciona oportunidades para que todas las partes implicadas entrenen su respuesta a los incidentes. Gracias a este entrenamiento reiterado, las organizaciones pueden organizar y mejorar su recuperación, y rechazar con confianza el pago de cualquier rescate.

Al involucrar a los equipos de seguridad en lo que, en esencia, es un proceso normal de recuperación de desastres (DR, por sus siglas en inglés), las organizaciones pueden localizar y eliminar los restos de un ciberataque y asegurarse de que los datos de la copia de seguridad están limpios antes de pasarlos a producción.

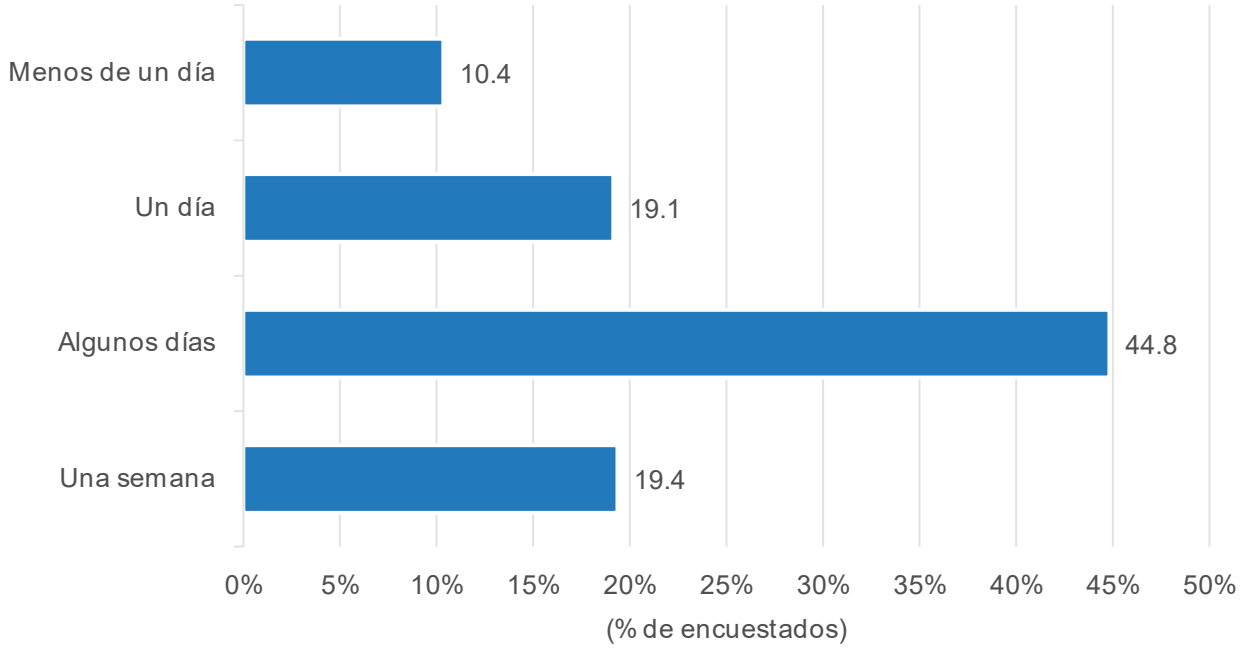
Pagar el rescate o elegir la recuperación rápida

Según la *Encuesta mundial sobre la resistencia y el gasto de las empresas del futuro* de IDC de diciembre de 2021, casi el 45 % de los participantes que se habían visto afectados por el *ransomware* afirmaron que la actividad se vio interrumpida durante unos días. Casi una quinta parte de los encuestados (19,4 %) declaró que las interrupciones duraron una semana entera (véase la imagen 2).

IMAGEN 2

La mayoría de las organizaciones experimentan más de un día de inactividad cuando el *ransomware* ataca.

P: *En su incidente de* ransomware *más reciente que bloqueó el acceso a los sistemas o datos, ¿cuántos días se vio interrumpida la actividad empresarial?*



n = 444

Notas:

Los datos son gestionados por el Grupo de Investigación Cuantitativa de IDC.

Los datos no están ponderados.

Se recomienda prudencia al interpretar tamaños de muestra pequeños.

Fuente: *Encuesta mundial sobre la resistencia y el gasto de las empresas del futuro* de IDC, diciembre de 2021

Puesto que minimizar el tiempo de inactividad es uno de los principales objetivos de la respuesta al *ransomware*, algunas organizaciones optan por pagar el rescate (véase la imagen 3). Sin embargo, la percepción de que el pago del rescate inicia inmediatamente a la empresa hacia la recuperación es un mito.

La decisión de pagar el rescate no suele ser inmediata. La mayoría de las organizaciones probarán todos los métodos de recuperación de datos que tengan a su alcance mientras los responsables de la toma de decisiones y los equipos jurídicos se reúnen antes de considerar la posibilidad de efectuar un pago. Un plan de recuperación de desastres documentado y probado puede acortar este paso y, si la capacidad de recuperación de una organización resulta insuficiente, debe pasarse al siguiente paso.

Cuando una organización decide pagar un rescate, entran en juego las compañías de ciberseguros y las agencias gubernamentales, además de los propios ciberdelincuentes. Con el fin de presentar una reclamación al seguro con éxito, una empresa debe negociar con todas estas entidades y argumentar que siguió las mejores prácticas, para demostrar que cumplía con la ley y para reducir el precio que solicitan los ciberdelincuentes. Cada día transcurrido deliberando supone un día más de inactividad.

Una vez que se ha realizado el pago y los delincuentes entregan una clave de descifrado, el proceso de recuperación no puede comenzar hasta que los datos cifrados se hayan descifrado. Los descifradores suelen ser programas no optimizados, por lo que el descifrado lleva mucho tiempo. Tampoco hay garantía de que el propio programa de descifrado no esté contaminado o funcione realmente.

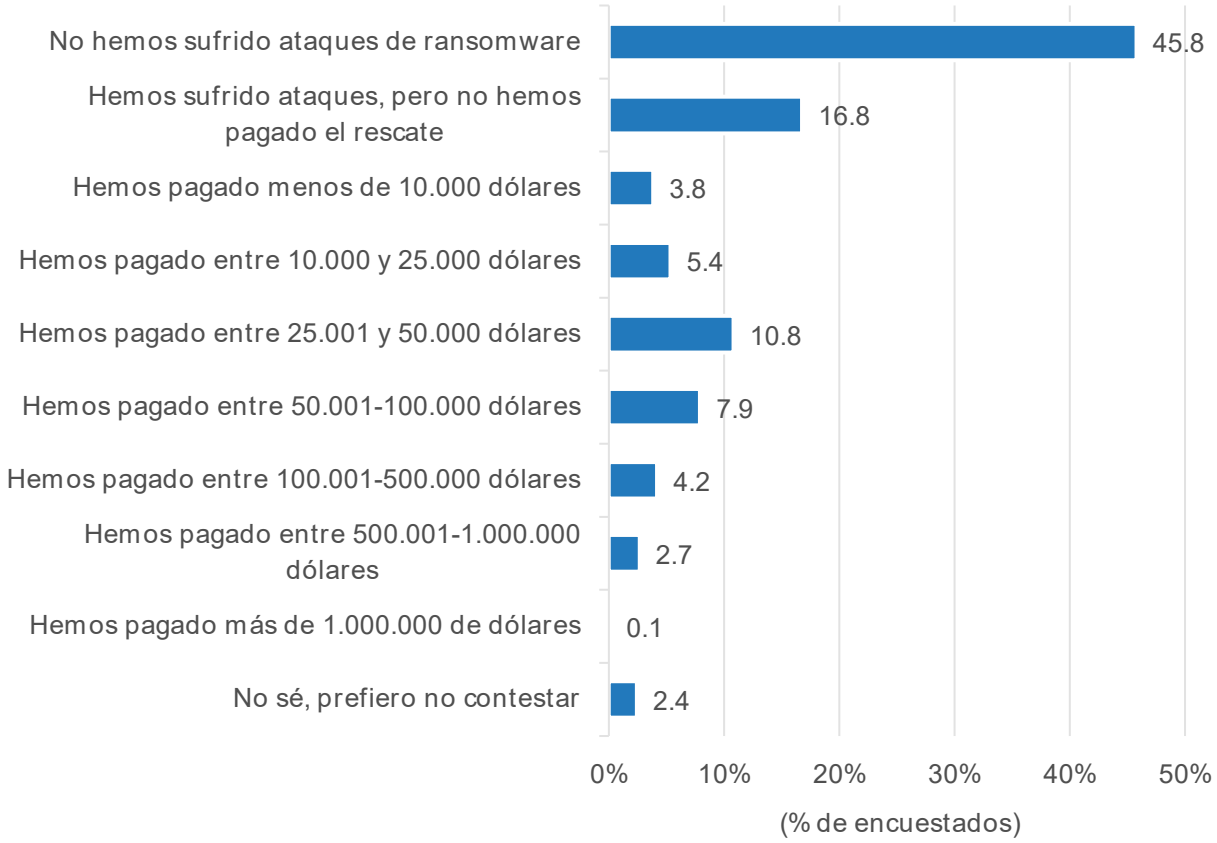
Además, el pago del rescate no bloquea el método por el que los delincuentes entraron en primer lugar, por lo que una organización podría seguir siendo vulnerable al mismo tipo de ataque en el futuro. Asimismo, al fomentar un modelo de negocio criminal y demostrar que es lucrativo, el pago del rescate prácticamente garantiza que se producirán más ataques en el futuro.

En cambio, reforzar la tecnología y los procesos de las copias de seguridad de los datos puede ser decisivo para una recuperación rápida y fiable. Según la *Encuesta mundial sobre la resistencia y el gasto de las empresas del futuro* de IDC, menos del 32,2 % de los participantes afectados por *ransomware* pudo recuperar satisfactoriamente sus archivos a partir de la copia de seguridad sin pagar el rescate (véase de nuevo la imagen 1).

IMAGEN 3

El coste del pago de rescates puede superar decenas de miles de dólares

P: Si su organización pagó un rescate en los últimos 12 meses para recuperar el acceso a sistemas o datos, ¿cuánto se pagó?



n = 858

Notas:

Los datos son gestionados por el Grupo de Investigación Cuantitativa de IDC.

Los datos no están ponderados.

Se recomienda prudencia al interpretar tamaños de muestra pequeños.

Fuente: *Encuesta mundial sobre la resistencia y el gasto de las empresas del futuro* de IDC, diciembre de 2021

Dado que un sistema de recuperación rápida y fiable se basa en la recuperación de desastres, es adecuado para restablecer el estado funcional de una empresa en cuestión de horas. Permitir un tiempo extra para los análisis de seguridad y forenses probablemente conduciría a una recuperación más rápida para una organización mientras se evita el pago de cualquier rescate.

Además, la recuperación rápida ante el *ransomware* permite a las organizaciones ser proactivas, ya que controlan la solidez y la fiabilidad de su sistema de recuperación. Las organizaciones que comprueban periódicamente su recuperación tendrán un conocimiento sólido de sus plazos durante

un incidente de *ransomware* y no tendrán que preocuparse de si los delincuentes cumplirán su parte del trato una vez realizado el pago.

Desde el punto de vista de los costes, una recuperación rápida y fiable es más sostenible que pagar el rescate cada vez que se produce un ataque (véase la imagen 3). Además, una organización no tiene que invertir necesariamente en nuevas herramientas para crear un sistema de recuperación rápida, ya que puede entrelazar sus activos existentes de copia de seguridad, recuperación ante desastres y seguridad.

El coste del tiempo de inactividad puede aumentar considerablemente. Según la encuesta de IDC de 2020, *Coste del tiempo de inactividad y la importancia de la asistencia técnica,* el coste medio del tiempo de inactividad de las cargas de trabajo locales es de 2800 dólares por hora, y para las cargas de trabajo que se ejecutan en la nube, de 3275 dólares por hora. Estos parámetros incluyen los costes asociados a la pérdida de productividad, la posible pérdida de ingresos, los costes de restauración, las sanciones y otros pagos. Lo más alarmante es que se trata de costes medios por carga de trabajo, y que los ataques de *ransomware* pueden hacer caer varios sistemas a la vez.

En la misma encuesta, los participantes también calificaron la importancia de los factores no financieros causados por el tiempo de inactividad. Les preocupaba que un tiempo de inactividad prolongado tuviera un impacto negativo en el ánimo de los empleados, la productividad y la reputación de la empresa. El tiempo de inactividad causado por el *ransomware* conlleva costes adicionales, como posibles acciones reguladoras y acciones legales interpuestas por los accionistas de la empresa.

PERSPECTIVA FUTURA

La protección y la seguridad de los datos se han entrelazado tanto que las organizaciones buscan ahora soluciones que ofrezcan un enfoque integral de prevención, detección y corrección. Dado que el *ransomware* evoluciona constantemente, es imposible desarrollar defensas contra técnicas de ataque que aún no se han encontrado.

Para estar al tanto de esta amenaza en constante cambio, las organizaciones tratarán la recuperación como un esfuerzo de grupo. Las actividades inusuales de copia de seguridad o cifrado, los cambios de nombre de los archivos y la eliminación de datos detectados por el programa de protección de datos se compartirán con los equipos de seguridad y de respuesta a incidentes para alertar de una posible infracción. Del mismo modo, las amenazas y los accesos inusuales a los datos pueden ayudar a los administradores de copias de seguridad a determinar cuándo se realizó la última copia de seguridad buena.

Con el tiempo, las organizaciones desarrollarán una respuesta al *ransomware* más proactiva que reactiva. Además de una respuesta bien ensayada, se tomarán medidas para garantizar que se sigan las mejores prácticas de seguridad, se actualicen las políticas cada vez que se introduzca una nueva infraestructura y se pueda contener la onda expansiva de cualquier posible ataque. Las herramientas de los proveedores, tanto del lado de la seguridad como de la protección de datos, podrán compartir información para ayudar en estos esfuerzos.

LA APORTACIÓN DE VEEAM

La plataforma Veeam proporciona funcionalidades de protección de datos en el núcleo local, la nube y los repositorios de borde. Aunque Veeam es más conocida por su gestión de datos en entornos virtuales, sus capacidades se extienden también a la infraestructura física y a los entornos Unix. La plataforma Veeam cuenta con estos módulos básicos:

- **Copia de seguridad y recuperación.** Proteja los datos en las instalaciones y en la nube con Veeam Backup, cuya impronta es la simplicidad. Veeam Backup and Recovery está diseñado para ofrecer los niveles de servicio más exigentes, al tiempo que reduce el trabajo humano necesario para su gestión.
- **Orquestación.** Automatice la recuperación ante desastres, la documentación, las pruebas y el cumplimiento. Muchas organizaciones no tienen un plan de recuperación de desastres o solo tienen un plan parcial, debido en especial a la complejidad y el coste de la implementación de un plan completo. La orquestación está diseñada para simplificar el proceso de recuperación de un desastre mediante la automatización de muchas de las tareas comunes asociadas a la recuperación.
- **Supervisión y análisis.** Con Veeam ONE, las organizaciones pueden ver toda su infraestructura desde un solo panel. Veeam ONE ofrece una perspectiva de la optimización de la infraestructura, así como una rápida identificación de las brechas de protección de datos y la garantía de éxito de la recuperación.

DESAFÍOS Y OPORTUNIDADES

Los ataques de *ransomware* evolucionan constantemente y la defensa contra ellos ha sido predominantemente reactiva. IDC cree que los responsables de TI deben ser lo más proactivos posible, y la tecnología que lo permite está disponible.

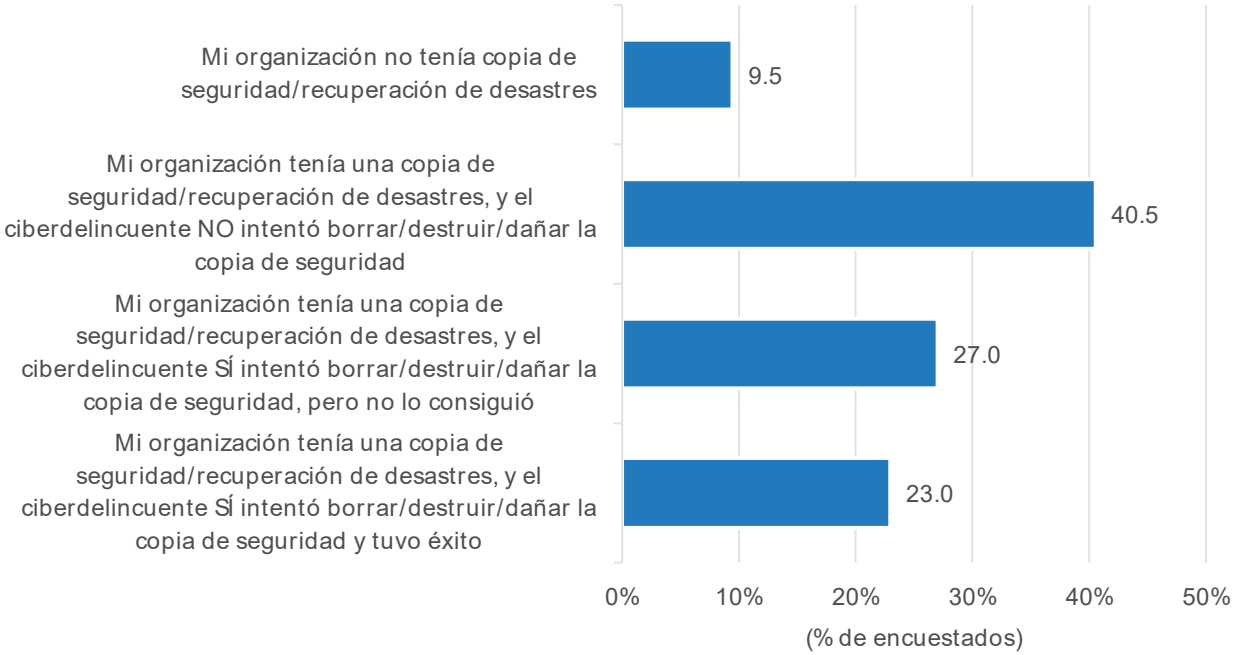
En el pasado, el mercado ha ofrecido productos singulares como soluciones contra el *ransomware*, pero ninguna solución puede abordar todos los aspectos de los ataques de *malware* y *ransomware*. Por lo tanto, las organizaciones de TI tienen que construir la solución total e invariablemente necesitarán productos tanto de protección de datos como de seguridad.

Los proveedores de protección de datos deben seguir haciendo hincapié en la seguridad de las copias de seguridad, ya que el intento de eliminarlas sigue siendo un método de ataque muy popular. Según la *Encuesta mundial sobre la resistencia y el gasto de las empresas del futuro* de IDC, la mitad de los encuestados afirmaron que los atacantes malintencionados tenían como objetivo sus copias de seguridad y, de esos intentos, aproximadamente la mitad tuvieron éxito (véase la imagen 4).

IMAGEN 4

Los atacantes de *ransomware* suelen intentar desactivar las copias de seguridad

P: En el último incidente de ransomware que bloqueó el acceso a sus sistemas o datos, ¿qué postura adoptó su organización respecto a las copias de seguridad/recuperación de desastres?



n = 444

Notas:

Los datos son gestionados por el Grupo de Investigación Cuantitativa de IDC.

Los datos no están ponderados.

Se recomienda prudencia al interpretar tamaños de muestra pequeños.

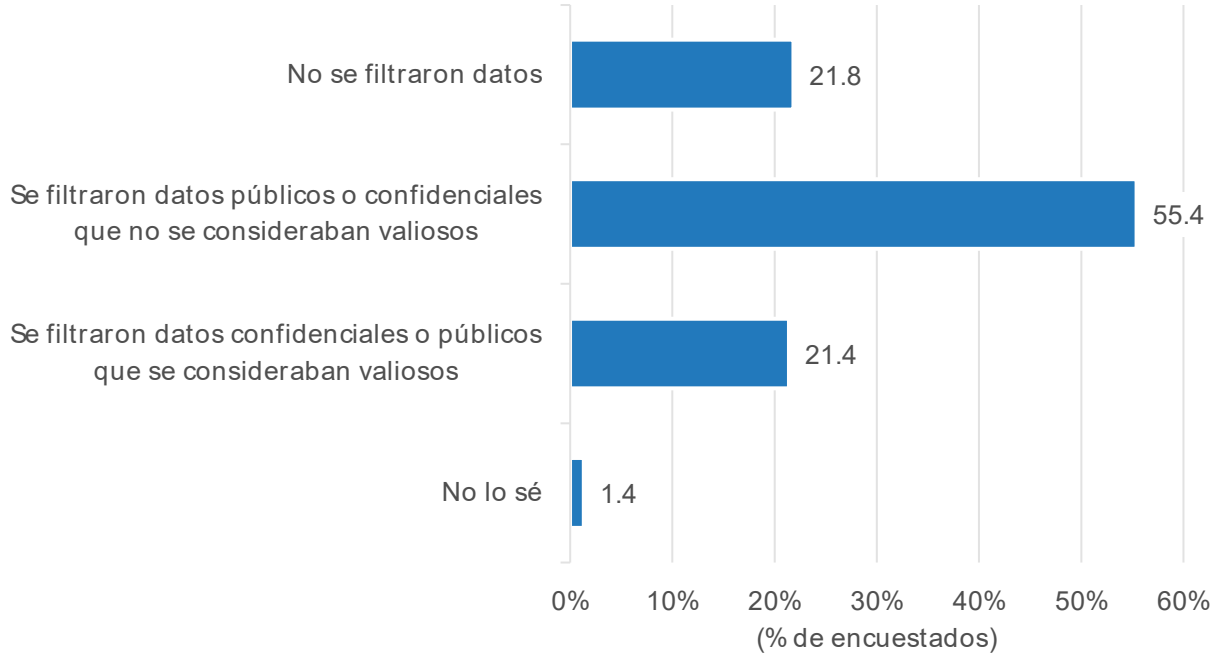
Fuente: *Encuesta mundial sobre la resistencia y el gasto de las empresas del futuro* de IDC, diciembre de 2021

La necesidad de seguridad se ve acentuada por los crecientes casos de fuga de datos. Casi tres cuartas partes de los encuestados que sufrieron un incidente de ransomware dijeron que los datos fueron robados en su ataque más reciente (véase la imagen 5). La participación de la seguridad en el proceso de recuperación y reparación de los datos podría ayudar a garantizar que los datos robados se cifren y sean inútiles para los delincuentes, o al menos a determinar si se ha robado algo importante o sensible.

IMAGEN 5

Se roban datos en más del 75 % de los incidentes de *ransomware*

P: En el último incidente de ransomware *que bloqueó el acceso a sus sistemas o datos, ¿cuál de las siguientes situaciones se produjo?*



n = 444

Notas:

Los datos son gestionados por el Grupo de Investigación Cuantitativa de IDC.

Los datos no están ponderados.

Se recomienda prudencia al interpretar tamaños de muestra pequeños.

Fuente: *Encuesta mundial sobre la resistencia y el gasto de las empresas del futuro* de IDC, diciembre de 2021

Dado que el *ransomware* evoluciona continuamente y los departamentos de TI están constantemente a la defensiva, las organizaciones tendrán que adoptar posturas más proactivas contra ataques inevitables. Buscarán implementar un modelo de confianza cero, la contención de amenazas y otras prácticas, y los proveedores de TI tienen una oportunidad de mercado para ayudar a las organizaciones con estas implementaciones.

CONCLUSIÓN

Una pequeña parte de las organizaciones son capaces de recuperarse por completo del *ransomware* sin pagar el rescate, y hacer esto se considera a menudo como un medio más rápido de restaurar las operaciones de negocio a la normalidad. Sin embargo, el simple hecho de pagar el rescate no significa que las organizaciones puedan comenzar inmediatamente la recuperación, ni asegura que los datos puedan recuperarse en su totalidad.

Los algoritmos de descifrado suelen ser lentos y ya se ha invertido tiempo en consultar con abogados y agencias de la Administración y en negociar con los atacantes. Todo ese tiempo podría ahorrarse si las organizaciones deciden, desde el primer minuto, iniciar un proceso de recuperación de datos en el que confíen.

Las organizaciones tienen que desarrollar un sistema de recuperación de datos garantizado que se base en los principios de detectar, proteger y recuperar. La integración de la seguridad en los procesos de protección y recuperación de datos garantiza la integridad y permite a las organizaciones minimizar el tiempo de inactividad en caso de *ransomware*.

Acerca de IDC

International Data Corporation (IDC) es el principal proveedor mundial de inteligencia de mercado, servicios de asesoramiento y eventos para los mercados de tecnología de la información, telecomunicaciones y tecnología de consumo. IDC ayuda a los profesionales de TI, ejecutivos de negocios y la comunidad de inversionistas a tomar decisiones basadas en hechos sobre compras de tecnología y estrategia comercial. Más de 1100 analistas de IDC brindan experiencia global, regional y local sobre tecnología y oportunidades y tendencias de la industria en más de 110 países en todo el mundo. Durante 50 años, IDC ha proporcionado información estratégica para ayudar a nuestros clientes a alcanzar sus objetivos comerciales clave. IDC es una subsidiaria de IDG, la empresa líder mundial de medios, investigación y eventos de tecnología.

Sede mundial

140 Kendrick Street
Edificio B
Needham, MA 02494
EE. UU.
508.872.8200
Twitter: @IDC
blogs.idc.com
www.idc.com