



Acronis

DOCUMENTO TÉCNICO

# Un plan de 12 pasos de respuesta al ransomware para empresas

Cómo defenderse y recuperarse de la ciberamenaza más urgente a nivel mundial

En solo unos años el ransomware se ha convertido en la herramienta de malware elegida por los ciberdelincuentes para enriquecerse amenazando a las empresas con pérdidas de datos e interrupciones de la actividad. Esta generalización del ransomware ha disparado el coste medio de una violación de datos. Se estima que alcanzará los 5 millones de dólares por incidente en 2023. Mientras los ciberdelincuentes amplían sus operaciones de desarrollo y distribución de malware, la frecuencia de los ataques aumenta a un ritmo alarmante, con nueve millones de nuevas muestras de malware en circulación cada mes.

Los ciberdelincuentes desarrollan continuamente nuevas tácticas y aprovechan nuevas tecnologías, como la inteligencia artificial, para mejorar la eficacia de sus ataques. Por ejemplo, en los ataques de ransomware, ya no se limitan a cifrar los datos esenciales de la víctima para convencerla de que pague el rescate. Ahora, en la mayoría de los casos, antes de la fase de cifrado, los atacantes roban datos confidenciales y amenazan con filtrarlos en Internet si la víctima no paga. También pueden contactar con sus clientes y partners y amenazarla con filtrar también los datos de ellos, lo que añade presión para ceder a la extorsión. Otra táctica que emplean es amenazar con que si no se paga se producirá un ataque DDoS en los servidores públicos de la víctima.

Actualmente los ciberdelincuentes aprovechan nuevas herramientas basadas en IA, como ChatGPT, para mejorar la apariencia de autenticidad y fiabilidad de los mensajes de phishing, analizar las aplicaciones automáticamente para descubrir vulnerabilidades y mejorar la organización de ataques multifase. Las mejoras que ofrece a los ataques la inteligencia artificial, las nuevas tácticas de extorsión y la proliferación de ataques cada vez más frecuentes han provocado que las ciberseguradoras cancelen la cobertura para empresas que no pueden demostrar que poseen defensas sólidas, con lo que podría desaparecer una protección muy utilizada para cubrir los costes de recuperación.

A pesar de esta perspectiva desalentadora, existen medidas concretas que pueden tomar las empresas para reducir significativamente las probabilidades de que un ataque de ransomware consiga su objetivo y minimizar los daños en cuanto a tiempo de inactividad y pérdida de datos si no consiguieran neutralizarlo. Acronis recomienda que se adopte el siguiente plan de 12 pasos para luchar contra la amenaza del ransomware. Las tácticas se dividen en tres categorías: medidas de defensa activa, nuevas competencias y procesos para TI y para los empleados, y un refuerzo de la mitigación de ataques y los programas de recuperación.



# Actualizar las medidas de protección activa

## **Primer paso** Desplegar medidas antimalware capaces de identificar el ransomware por su comportamiento y así complementar al antivirus tradicional basado en firmas.

El aprendizaje automático y la inteligencia artificial son componentes esenciales en este caso, ya que facilitan la detección de patrones de comportamiento malicioso, en lugar de limitarse a comparar la firma de una instancia de malware con una base de datos de amenazas conocidas. Sin este enfoque basado en el comportamiento, ninguna medida antimalware podría identificar los miles de instancias de malware de día cero que se generan a diario.

## **Segundo paso** Actualizar las medidas como la seguridad del correo electrónico y el filtrado de URL.

En 2022, el 30,6 % de todos los mensajes recibidos eran spam y el 1,6% contenían malware o enlaces de phishing. El phishing fue el vector utilizado en el 76 % de todos los ataques que consiguieron su objetivo en 2022, y aproximadamente un 8 % de los endpoints intentaron acceder a URL maliciosas ese año. Los ciberdelincuentes han mejorado mucho sus estrategias para ocultar los enlaces y archivos adjuntos maliciosos en los mensajes de correo electrónico, así que una de las medidas más eficaces que puede aplicar una empresa para la detección es invertir en una solución de seguridad del correo electrónico actualizada que pueda identificar y extraer los mensajes de phishing antes de que lleguen a la bandeja de entrada del empleado.

## **Tercer paso** Desplegar herramientas que incrementen su visibilidad de los recursos de TI y los flujos de datos.

Una pregunta típica que suelen hacer los directivos al personal de TI tras un ataque de ransomware es: "¿Cómo ha conseguido el ciberdelincuente filtrar un terabyte de datos confidenciales nuestros, sin que lo advirtiéramos?" Para evitar verse en esta desagradable tesitura, debe supervisar y mantener un registro de la actividad que tiene lugar en su infraestructura, incluido el acceso a los servicios en la nube, y llevar a cabo análisis continuos de los registros. Las herramientas de inventario de TI y prevención de pérdida de datos (DLP) también proporcionan una mejor visibilidad de dónde se encuentran los datos y cómo se mueven, lo que permite detectar casos de robo de datos y evitar cualquier exposición de la información. Plántese desplegar tecnología de detección y respuesta (EDR), que emplea supervisión en tiempo real, análisis basados en comportamientos y aprendizaje automático para identificar el malware, las intrusiones y el acceso no autorizado.

**Cuarto paso** Eliminar las exposiciones de la red internas y externas. Desactive el Protocolo de escritorio remoto de Microsoft (RDP), excepto cuando sea necesario, y refuerce la protección de los endpoints inhabilitando los servicios que no se utilizan. Use firewalls y sistemas de prevención de intrusiones para limitar el acceso de Internet entrante.

Puede limitar el acceso de VPN a zonas geográficas específicas y establecer una política de teletrabajo que limite o prohíba el acceso a los recursos de la empresa desde dispositivos personales. Para minimizar las amenazas potenciales por parte de empleados malintencionados o negligentes, segmente sus redes internas para impedir la propagación del ransomware desde los sistemas comprometidos a otros endpoints y servidores.

**Quinto paso** Gestionar las contraseñas y los derechos de acceso con precauciones. Las credenciales filtradas o robadas han sido la causa de casi la mitad de las violaciones de seguridad comunicadas en 2022. En los ataques de ransomware, los ciberdelincuentes suelen usar contraseñas filtradas, que se han reutilizado en varias cuentas diferentes, que no son seguras o bien que solo utilizan autenticación de un factor. Con frecuencia, se apropian de herramientas de operaciones de TI, como Mimikatz, para robar las contraseñas almacenadas en la memoria de los servidores. Para combatir estas tácticas, debe implementar la autenticación multifactor, especialmente en los sistemas que contienen datos confidenciales. Cambie siempre las credenciales de administración predeterminadas. Si ha recibido un ataque, cambie todas las contraseñas. Se sabe que los ciberdelincuentes suelen volver a atacar a objetivos anteriores utilizando las mismas credenciales que en el primer ataque. Adopte el principio del mínimo de privilegios para otorgar los derechos de acceso. Controle de cerca el acceso a los sistemas que albergan herramientas de administración o datos confidenciales, excluyendo a todos los empleados a excepción de los imprescindibles y otorgando privilegios por períodos limitados y de un solo uso, siempre que sea posible.



## Optimizar las competencias y los procesos

**Sexto paso** **Crear un programa de formación para concienciar en seguridad.** El phishing sigue siendo una de las técnicas más eficaces para conseguir que el malware supere las defensas externas de una empresa, por lo que reducir el número de clics en archivos adjuntos y enlaces maliciosos en los mensajes de correo electrónico (así como SMS, mensajes instantáneos y redes sociales) puede reducir el riesgo considerablemente. Entrene a sus empleados para que estén atentos para detectar comunicaciones sospechosas, enviándoles de vez en cuando mensajes de correo electrónico de phishing falsos, y a los que muerdan el anzuelo, ofrézcales un curso de repaso. Todos los empleados deben participar y, en particular, los directivos, ya que, debido a sus privilegios elevados y su capacidad para autorizar transferencias de fondos, son un objetivo de preferencia de los atacantes.

**Séptimo paso** **Implementar análisis de vulnerabilidades y administración de parches de manera automatizada y programada.** Normalmente, las pequeñas o medianas empresas suelen tener dificultades para instalar de manera puntual los parches de software de sus proveedores, lo que deja vulnerabilidades sin corregir durante más de 90 días de media. Los ciberdelincuentes son conscientes de esta exposición de la información e intentan aprovecharla continuamente. Para cerrar estas brechas de forma rápida y eficaz, debe emplear herramientas automatizadas para estas operaciones de TI que, si bien son tediosas, también son fundamentales.

**Octavo paso** **Reducir la cantidad de agentes en los endpoints y las consolas en su centro de operaciones.**

Es habitual que las empresas hayan ido implementado sus soluciones de ciberseguridad y protección de datos de manera gradual y poco sistemática a lo largo del tiempo. Esto ha provocado una proliferación de agentes remotos en los endpoints y en las consolas de administración en el centro de operaciones de TI. La multiplicidad de agentes supone un desperdicio de recursos y suele generar conflictos. La necesidad de cambiar entre consolas reduce la eficiencia operativa del personal de TI y aumenta los costes de formación. Siempre que sea posible, deben consolidarse los agentes para eliminar brechas y conflictos, y para mejorar el rendimiento de los endpoints. Es conveniente combinar las consolas de administración para incrementar la eficacia y agilizar la incorporación del personal de TI.

**Noveno paso** **Aprovechar los marcos de seguridad, como el del NIST, para evaluar y actualizar periódicamente sus estrategias de defensa y mitigación frente al ransomware y otras ciberamenazas.** Estos marcos ofrecen mejores prácticas y directrices demostradas, para priorizar las correcciones de problemas de seguridad y mejorar continuamente la tecnología, los procesos y la experiencia de su personal.

## Reforzar la mitigación y la recuperación tras un ataque

**Décimo paso** **Implementar un programa eficaz de protección de datos.** Los ciberdelincuentes siempre van por delante y es posible que ni siquiera las mejores defensas consigan hacer frente a las nuevas tácticas y tecnologías que emplean. Dé por hecho que en algún momento habrá un ataque que consiga su objetivo y haga todo lo posible por mejorar su programa de protección de datos. La capacidad de restaurar los datos a partir de una copia de seguridad reciente puede permitir a la empresa reanudar rápidamente sus operaciones, posiblemente sin pagar un rescate. Sin embargo, tenga en cuenta que los ciberdelincuentes suelen intentar localizar y cifrar o eliminar los archivos de copia de seguridad, desactivar las medidas de protección y las copias de seguridad, y utilizar sus propias herramientas para robar datos y propagar el ataque por toda la red. Por lo tanto, es esencial conservar varias copias de seguridad, preferentemente cifradas, en distintos soportes y lugares: ubicaciones externas, sin conexión a Internet y en la nube. Debe probar con regularidad su plan de copia de seguridad para verificar la integridad de sus archivos y procesos, y para

asegurarse de que puede realizar la restauración según los objetivos de tiempo de recuperación de su empresa. Por último, debe analizar las copias de seguridad para descubrir si contienen malware y vulnerabilidades sin parche, y corregir estos problemas antes de restaurar los sistemas y devolverlos a producción.

**Decimoprimer paso** **Plantearse la posibilidad de implementar un programa de recuperación ante desastres.**

El proceso de limpieza y recuperación tras un ataque de ransomware, incluida la restauración de grandes cantidades de datos a partir de las copias de seguridad, puede retrasar la reanudación de las operaciones habituales de la empresa días o semanas. Por eso, la posibilidad de retomar inmediatamente las operaciones utilizando aplicaciones y datos replicados (ya sea en una ubicación externa o en la nube) evita este tipo de interrupciones prolongadas. Gracias a la reciente opción de recuperación ante desastres como servicio, esto es ahora mucho más asequible y fácil de administrar, incluso para las empresas más pequeñas.

**Decimosegundo paso** **Crear un plan de respuesta ante incidentes, y probarlo y actualizarlo con frecuencia.**

Conserve una copia impresa de los nombres y los números de sus contactos internos y externos esenciales; si se produce un ataque de ransomware, es posible que no pueda acceder a sus registros online. Identifique y pruebe un canal interno de comunicaciones de respaldo (por ejemplo, una aplicación de mensajería o redes sociales en un smartphone), por si sus sistemas habituales dejaran de funcionar. Diseñe una estrategia de comunicaciones que identifique, en función de la gravedad

y la fase del ataque, a quién informar y quiénes deben hacerlo: el personal de operaciones y administración de seguridad y TI; los directivos; los equipos del departamento legal y de cumplimiento normativo; los partners y clientes; la prensa y el público; las autoridades reguladoras; los bancos e inversores, etc. Pruebe el plan regularmente, con ejercicios prácticos y en directo. En caso de ataque, recopile datos forenses y utilícelos para identificar y cerrar las vulnerabilidades que han facilitado el ataque, y actualice el plan de respuesta como corresponda.

## Conclusión

Toda empresa que pretenda reducir el riesgo que presenta la amenaza creciente del ransomware debe adoptar una defensa agresiva, pero también prepararse ante la posibilidad de que un ataque prospere. Para contrarrestar las amenazas de ransomware, que son cada vez más frecuentes y sofisticadas, los directivos de las empresas deben centrar sus planes de defensa y mitigación en los procesos y las tecnologías, con el fin de reducir la complejidad general y mejorar la eficacia de su personal de TI, gracias al empleo de inteligencia artificial, automatización e integración.

## Recursos

Informe semestral de Acronis sobre ciberamenazas: segundo semestre de 2022

<https://www.acronis.com/es-es/resource-center/resource/726/>

Global Cyber Protection Landscape in 2022: Key Trends and Gaps

(Panorama global de ciberprotección: tendencias y brechas de seguridad principales)

<https://www.acronis.com/es-es/resource-center/resource/721/>

Acronis Cyber Protect

<https://www.acronis.com/es-es/products/cyber-protect/>

