arcserve®

Proteja lo más valioso.

# GUÍA PARA UN FUTURO LIBRE DE RANSOMWARE

## UN ENFOQUE PROACTIVO ANTE LA AMENAZA DEL RANSOMWARE

INFORME TÉCNICO

# EL RANSOMWARE SE HA CONVERTIDO EN UNO DE LOS MAYORES RIESGOS EMPRESARIALES Y ES LA AMENAZA MÁS PELIGROSA PARA LAS EMPRESAS DE TI.

El ransomware se ha convertido en uno de los mayores riesgos empresariales y es la amenaza más peligrosa para las empresas de TI. Ha alcanzado proporciones epidémicas en todo el mundo, con unos costes que se prevé que lleguen a los 20.000 millones de dólares para el año 2021[1].

Aun así, para los profesionales de TI y los responsables de las decisiones empresariales, esta noticia no debería ser tan terrible. Si bien los atacantes cibernéticos no tienen ninguna intención de bajar la guardia, los avances en tecnologías de recuperación de desastres y frente a ciberataques, junto con las buenas prácticas en administración de TI, permiten a las empresas dar un paso al frente.

En este informe se analiza la creciente amenaza que representa el ransomware, las tecnologías y las prácticas de administración de TI que se utilizan para su defensa, y un enfoque basado en posibilidades para lograr un futuro libre de ransomware.

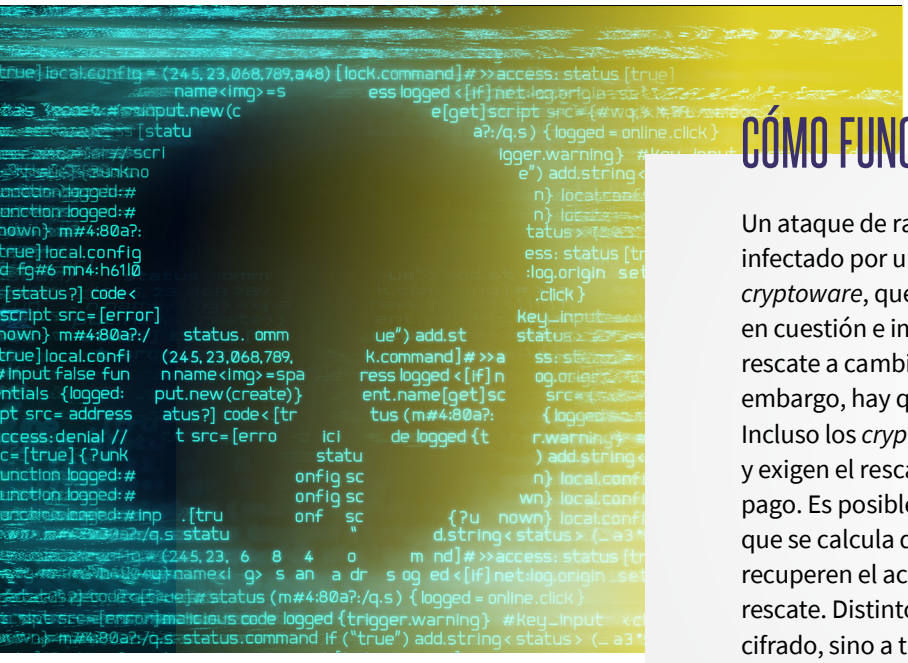
## CONOCER AL ENEMIGO

El estratega militar chino Sun Tzu sabiamente aconsejaba “Conozca a su enemigo”. Para desarrollar una estrategia que permita proteger los sistemas informáticos frente al ransomware, es necesario comprender la amenaza que representa. Por lo tanto, comencemos por explicar qué es el ransomware.

Los datos son el pilar básico de una empresa. Representan todas sus operaciones, ya que son transversales a todas las unidades de negocio. Permiten hacer un seguimiento de todo lo ocurrido, informar sobre el estado actual del negocio y también impulsar la toma de decisiones. Sin los datos, bien podríamos decir que una empresa no podría existir. Este es el fundamento sobre el que se basa el ransomware.

Se trata de un software malicioso que le impide acceder a sus sistemas informáticos o sus datos hasta que pague un rescate. Puede paralizar todas sus operaciones y, en casos de *leakware* o *extortionware*, también amenazar con filtrar y hacer públicos datos confidenciales.

Las empresas que tengan datos almacenados en ordenadores o redes están en riesgo. O sea, prácticamente todas. Los gobiernos estatales y locales, los organismos de seguridad, las administraciones de sanidad, los bancos y las empresas de crédito son los objetivos por excelencia: un sector impulsado por el robo de identidades, que solo en 2018 y según los informes sustrajo 14.700 millones de dólares a los consumidores. Tampoco es cuestión de tamaño: los ataques de ransomware afectan por igual a consumidores, grandes empresas y pymes.



# CÓMO FUNCIONA EL RANSOMWARE

Un ataque de ransomware ocurre cuando un ordenador se ve infectado por un virus. La mayoría del ransomware se trata de *cryptoware*, que cifra los archivos almacenados en el ordenador en cuestión e impide el acceso a ellos hasta que se pague un rescate a cambio de una clave que permita liberarlos. Sin embargo, hay que tener especial cuidado al pagar rescates. Incluso los *cryptoware* más peligrosos y falsos cifran los archivos y exigen el rescate, pero no entregan una clave después del pago. Es posible que las víctimas de este tipo de ransomware, que se calcula que se presenta en un 50 % de los casos, no recuperen el acceso a sus archivos, ni siquiera pagando el rescate. Distinto es el ransomware que no opera mediante cifrado, sino a través de una pantalla de bloqueo que no permite acceder a los datos (que no están cifrados).

El ransomware puede afectar a archivos específicos o a todo el sistema, mediante el registro de arranque maestro (MBR) de una unidad o el NTFS de Microsoft, lo que evita el arranque de los sistemas. Los ataques de ransomware suelen pasar desapercibidos gracias al uso de una red, como un tráfico cifrado por HTTPS o Tor. A diferencia de otros tipos de malware que operan en segundo plano, una vez que el ransomware se infiltra en el equipo objetivo, avisa de su presencia exigiendo el pago de un rescate en criptomonedas imposibles de rastrear.

Un ordenador puede infectarse con solo una pequeña e inocente acción del usuario, por ejemplo, hacer clic en un enlace malicioso. El ransomware suele transmitirse a través de correos de phishing, aunque los atacantes cibernéticos también recurren a muchas otras técnicas para infectar sus objetivos con ransomware. Esto suele ocurrir, en general, cuando el usuario abre un adjunto de un correo electrónico o hace clic en un enlace engañoso. Entre los vectores que suelen utilizarse para propagar el malware se encuentran los siguientes:

- **Correos electrónicos y mensajes de texto** que contienen enlaces de descarga de malware o un adjunto infectado con malware.
- **Sitios web** cuyo único propósito es atraer a los usuarios y lograr que hagan clic en una descarga o un enlace malicioso.
- **Publicidad fraudulenta (malvertising)** o maliciosa que engaña al usuario para que haga clic en enlaces que llevan a descargas no deseadas.
- **Redes sociales** que aparentan estar relacionadas con fuentes de confianza, pero que de forma rápida y engañosa redireccionan a un atacante cibernético. Las víctimas son objeto de las infecciones de manera directa e involuntaria desde una aplicación de red social o se sienten atraídas por un enlace o un anuncio malicioso.
- **Aplicaciones móviles** que los usuarios descargan voluntariamente en sus dispositivos sin darse cuenta de que son falsas y que transferirán el virus a su ordenador la próxima vez que se conecten.

Los hackers son cada vez más sofisticados: envían adjuntos infectados en correos que supuestamente provienen de contactos de la víctima. Si bien las políticas de uso y la formación son recursos útiles a la hora de reducir las conductas peligrosas por parte de los usuarios finales, es imposible erradicar esta vulnerabilidad por completo, ya que los puntos de contacto pueden no ser tan evidentes. Los contenidos maliciosos también pueden aprovechar las vulnerabilidades en navegadores o complementos y ejecutar código malicioso sin que el usuario se dé cuenta. Una vez establecida en un sistema huésped, la infección puede propagarse fácilmente hacia otros ordenadores de la misma red.

Además de engañar a los usuarios para que descarguen ransomware sin saberlo, los atacantes cibernéticos logran acceder a los sistemas a través de Internet cuando los usuarios no están en sus escritorios. No solo usan métodos violentos, sino también credenciales que adquieren en la Internet oscura (*dark web*) para obtener recursos y datos, aprovechándose del protocolo Remote Desktop Protocol y de las vulnerabilidades de software.

Según un informe elaborado en el año 2019, en el contexto de corporaciones y organizaciones gubernamentales, los ataques de ransomware suelen tener por objetivo activos de gran valor, como servidores, infraestructuras de aplicaciones y herramientas de colaboración. Aunque las empresas de TI priorizan, de manera acertada, las vulnerabilidades más críticas y actuales, aquellas más antiguas o de menor envergadura no deben dejarse de lado. En este informe, las vulnerabilidades antiguas (de hace 3 años o más) representaban más de un tercio de los ataques, de los cuales más de la mitad se servían de vulnerabilidades menos críticas[3].

**DE MEDIA, UN ATAQUE DE RANSOMWARE PROVOCA CASI 10 DÍAS DE INACTIVIDAD.[4]**

## ¿Cuáles son los efectos de una infección por ransomware?

Debido a las constantes noticias sobre ataques de ransomware y una avalancha de estadísticas atemorizantes, las empresas ya han tomado nota y están en busca de soluciones de seguridad o protección de datos que cumplan con sus necesidades. Un ataque tiene como efecto inmediato la interrupción masiva de las operaciones comerciales mientras los dispositivos y sistemas se desactivan para su desinfección, con la esperanza de lograr una restauración sin inconvenientes de los datos depurados, a partir de una estrategia eficaz de copia de seguridad y recuperación de desastres. De media, un ataque de ransomware provoca casi 10 días de inactividad[4].

Si bien el FBI recomienda no pagar rescates, en 2018 se informaron pagos por más de 2,57 millones de dólares[5]. De media, una empresa puede esperar un coste de 133.000 dólares por ataque, simplemente para volver a tener acceso a sus propios datos[6]. Por desgracia, algunas víctimas pagan sin garantía alguna de que recuperarán sus archivos y datos. Algunos estudios indican que los autores de ransomware suelen ganar más del doble que los desarrolladores que trabajan en proyectos legales[7]. Claramente, lo que es una ventaja para los atacantes es muy malo para las empresas y su personal de TI.

**2.57**
**mill.**
**DÓLARES PAGADOS EN RESCATES[5]**

**133,000**
**USD**
**COSTE MEDIO POR ATAQUE[6]**

Las empresas desean con todas sus ganas que sus defensas frente a ataques de ransomware funcionen. Pero incluso si logran evitar lo peor, al menos parcialmente, luego tendrán que lidiar con el riesgo de pérdida de datos asociado a los ataques. De media, los ataques suelen generar pérdidas cercanas al 8 % de los datos. Además de exigir el pago de un rescate, los atacantes pueden extraer datos de un ordenador o servidor infectado y exponer datos confidenciales, como nombres de usuario y contraseñas, información sobre medios de pago y direcciones de correo de los contactos. En los ataques modernos de ransomware, se hace una copia de los archivos en unidades compartidas de red e incluso se eliminan instantáneas de volumen en las estaciones de trabajo que impiden su restauración. Tanto el ataque como la pérdida de datos resultante forman un combo explosivo, y los riesgos de deterioro de la reputación de la marca pueden tener un impacto devastador a largo plazo que afecte gravemente la credibilidad.

> *"Los atacantes cibernéticos tienen técnicas cada vez más sofisticadas, y prácticamente ningún sector está a salvo del ransomware. Al poner a los sistemas de copias de seguridad en el punto de mira, los hackers tienen más probabilidades de que las empresas paguen por un rescate, debido a las graves consecuencias de la pérdida de datos y el tiempo de inactividad, que suelen ir más allá del coste económico. Los responsables de TI y del negocio deben considerar también el efecto adverso en la productividad de los empleados, la confianza de los clientes, la reputación de la marca y el cumplimiento normativo cuando sus sistemas y datos están en riesgo."*
>
> *- Oussama El-Hilali, CTO, Arcserve*

## ¿Cómo protegen los profesionales de TI a sus empresas frente al ransomware?

Estos son algunos de los métodos que se utilizan para detectar el ransomware y proteger los valiosos datos y sistemas:

- **Software antiransomware** que permite identificar posibles ataques y detectar y prevenir intrusiones en tiempo real.
- **Firewalls** que permite bloquear el acceso no autorizado a un ordenador o una red.
- **Filtros de archivos y correo no deseado** que permiten bloquear sitios web con supuesto malware y evitar que los adjuntos no deseados lleguen a la bandeja de entrada de los usuarios.
- **Software de políticas de grupo** que permite bloquear la ejecución de archivos desde carpetas locales que puedan infectar los sistemas.
- **Paquetes SIEM (Security Information and Event Management)** que permiten obtener estadísticas sobre el tráfico de red con el objetivo de detectar anomalías que indiquen una infracción de seguridad.
- **Software de copia de seguridad** que permite proteger los datos del negocio copiándolos desde servidores, bases de datos, ordenadores de sobremesa, portátiles y otros dispositivos.
- **Supervisión de la integridad de los archivos** que permite verificar la coherencia entre un archivo actual y un archivo validado.
- **Software antivirus y antimalware** que permite prevenir, detectar y eliminar malware.
- **Soluciones de gestión unificada de amenazas (UTM)** que permite hacer frente a diferentes amenazas a través de un único punto de defensa y una única consola.

Aunque cada uno de los distintos métodos para detectar ransomware y proteger los valiosos datos y sistemas son igual de útiles e importantes, recurrir a soluciones puntuales puede poner en un riesgo aún mayor a las empresas. En la actualidad, los atacantes cada vez son más sofisticados y cuentan con más recursos. Las estrategias de ataque suelen combinar diferentes técnicas para llegar a muchas partes de una red informática simultáneamente. Los ataques de ransomware emplean variantes de malware para sortear los programas antivirus. Entonces, ¿cuáles son los obstáculos que presentan las estrategias tradicionales de protección contra el ransomware?


## Muchos sistemas, pocas funcionalidades importantes

Era más sencillo hacer frente al malware cuando existía una tecnología antivirus basada en firmas para cada exploit. A medida que evolucionan las amenazas y se configuran distintos ataques contra vulnerabilidades comunes, es más difícil identificar las amenazas utilizando tecnologías basadas en firmas.

Asimismo, muchos proveedores de protección de datos se han subido al tren del ransomware, haciendo hincapié en "funcionalidades" de seguridad cibernética que, en realidad, solo son capaces de detectar anomalías que podrían o no estar relacionadas con el ransomware. Una vez identificadas, lo que hacen es mostrar una alerta, pero no toman ninguna medida para resolver el problema.

## Las soluciones individuales son difíciles de administrar, lo que aumenta la vulnerabilidad

Muchas empresas recurren a varias herramientas y proveedores para acceder a diferentes funciones de seguridad frente al ransomware; por ejemplo, es posible que tengan dos proveedores de firewall, otro de DLP o filtrado web, de copia de seguridad y recuperación de desastres, copias en la nube, centros de datos y también otro para copias móviles.

El hecho de que una empresa tenga varios dispositivos y proveedores para las distintas tareas de seguridad dificulta aún más el seguimiento y la prevención de ataques. Las herramientas y los distintos programas de software requieren cierto nivel de administración y actualizaciones, lo que dificulta adaptarse a los tipos más recientes de malware. Gestionar varios proveedores y soluciones aumenta el riesgo, las vulnerabilidades y los errores. Esto tiene consecuencias negativas tanto en la productividad como en los costes.

Hoy en día, es posible transformar las complejas herramientas de antiransomware heredadas y pertenecientes a múltiples proveedores gracias a una única solución de defensa avanzada que ofrece funcionalidades integrales de copia de seguridad y recuperación de datos, protección de endpoints y redes neuronales contra malware, exploits y ransomware, tanto si son conocidos como si no.

## Los profesionales de TI también requieren prácticas de administración de TI

Las soluciones de tecnología son clave para la seguridad cibernética y la protección contra el ransomware, como las tecnologías de seguridad de correos electrónicos y firewall, y los sistemas de prevención y detección de intrusiones. Proteger una empresa depende en gran medida de soluciones avanzadas de protección y seguridad integradas de datos. La adopción de prácticas adecuadas de administración de TI es también esencial.

Resulta importante reconocer que las conductas de los usuarios finales representan la mayor amenaza. Las empresas necesitan implementar controles de administración de TI que permitan detectar si un empleado no cumple alguna política o procedimiento. Estas prácticas deberían contemplar la participación activa de los usuarios, es decir, informar cómo se deben ajustar las conductas en pos de la seguridad.

Los profesionales de TI también deben considerar la totalidad de su portfolio de TI para evaluar los riesgos. Si bien es cierto que cualquier sistema es vulnerable, los atacantes se interesan más por datos valiosos que no están protegidos de manera adecuada. Es necesario que las empresas prioricen la protección de sus recursos y hagan una administración proactiva de su TI, por ejemplo, usando objetivos de punto de recuperación (RPO) para conocer qué nivel de pérdida de datos es aceptable en caso de error y también para reforzar las defensas. Deben conocer los recursos con los que cuentan y cómo están configurados, además de controlar de cerca todos los cambios que ocurran.

Las referencias, como la Biblioteca de Infraestructura de Tecnologías de la Información (ITIL), pueden ayudar a las empresas a implementar mejores prácticas en el ámbito de la administración de TI. La ITIL ofrece prácticas relacionadas con la administración de configuraciones, cambios y versiones en forma de procesos clave que las empresas pueden dominar para defenderse contra las amenazas de ransomware y seguridad cibernética.


## ¿ES POSIBLE UN FUTURO LIBRE DE RANSOMWARE?

Eludir un polifacético ataque de ransomware requiere una defensa coordinada que combine la tecnología adecuada con prácticas responsables de administración de TI. La solución ideal consiste en una solución multicapa de seguridad y protección de extremo a extremo. Si una empresa de TI logra implementar una primera y última línea de defensa contra el ransomware, podrá prácticamente eliminar la amenaza y transformar la manera en que protege sus datos frente a extorsionistas, hackers y malhechores.

Según una encuesta mundial reciente de profesionales de TI, dos de cada tres encuestados opinan que es esencial encontrar soluciones que combinen seguridad con protección de datos. Incluso lo consideran más importante que encontrar soluciones que incorporen la inteligencia artificial (IA) para predecir desastres o que automaticen las tareas de cumplimiento[10].

# ESTRATEGIAS DE PROTECCIÓN FRENTE AL RANSOMWARE

A continuación, presentamos cinco estrategias de protección contra el ransomware que pueden ayudar a que su empresa vaya más allá de los enfoques reactivos de seguridad e integre tecnologías antiransomware y otras de prevención de amenazas con funcionalidades de recuperación de desastres y alta disponibilidad para neutralizar los ataques cibernéticos.

## 1 Administrar el acceso de manera activa

**Desarrolle los controles y procedimientos necesarios para proteger las aplicaciones y los sistemas frente a los usuarios no autorizados.**

- Restrinja el acceso a puntos habituales de entrada de ransomware, como cuentas personales de correo electrónico y sitios de redes sociales, y utilice filtros web en gateways y endpoints para bloquear los intentos de phishing contra usuarios que involuntariamente hacen clic en enlaces maliciosos.
- Use una autenticación de varios factores y estándares avanzados de contraseñas, además de exigir contraseñas cuando los usuarios se comuniquen con sitios web que no están clasificados por el proxy o firewall.
- Implemente servidores proxy y software de bloqueo de anuncios, y restrinja los permisos para instalar y ejecutar aplicaciones de software.
- Examine y supervise a terceros que tienen acceso remoto a la red de la empresa y a sus conexiones con terceros para garantizar que estén aplicando las mejores prácticas de ciberseguridad.
- Use listas de aplicaciones autorizadas para permitir que solo se ejecuten programas aprobados en una red.

## 2 Administrar la configuración de los sistemas en todos los vectores de ataque

**Desarrolle sistemas y procesos de administración centralizada que aborden todo el espectro de amenazas de ransomware.**

- Evalúe y clasifique los datos confidenciales del negocio e implemente la separación física y lógica de servidores, redes y almacenes de datos.
- Garantice que las soluciones de antivirus y antimalware estén habilitadas para su actualización automática y analice los correos electrónicos entrantes y salientes a fin de detectar intentos de phishing, evitar la suplantación de correos y filtrar archivos ejecutables.
- Use un sistema de administración centralizada de parches para blindar todos los endpoints a medida que se descubre una vulnerabilidad, incluso en dispositivos móviles, sistemas operativos, software y aplicaciones, ubicaciones en la nube y el Internet de las Cosas (IoT).
- Despliegue el aprendizaje profundo sin firma y tecnologías antiransomware y antiexploits para detectar tanto el malware conocido como el desconocido.
- Despliegue tecnologías integradas de protección de endpoints y continuidad del negocio para acelerar la prevención frente a amenazas y permitir la inmediata restauración de datos.
- Asegure las aplicaciones y servidores web usando firewalls para aplicaciones web.
- Deshabilite los scripts de archivos de Microsoft Office enviados por correo electrónico y considere el uso del software Office Viewer para abrir los archivos de Office.

- Realice auditorías de red para los sistemas usando el Protocolo de Escritorio Remoto, cerrando los puertos que no se utilizan y usando autenticación de doble factor.
- Detecte y clasifique comportamientos maliciosos, como el cifrado masivo de archivos, para bloquearlos.
- Incorpore advertencias en correos electrónicos provenientes de fuentes externas para recordar a los usuarios sobre el peligro de hacer clic en enlaces y abrir adjuntos.
- Use equipos UTM que combinan firewall, antivirus en gateway, así como capacidades de prevención y detección de intrusiones para bloquear el acceso a direcciones IP maliciosas.

## 3 Combinar soluciones de seguridad y protección de datos

**Incorpore, pruebe y mantenga una protección integral de datos y seguridad cibernética para obtener una protección de extremo a extremo.**

- Proteja los repositorios de copias de seguridad frente a los ataques de malware, ransomware y día cero.
- Detenga y elimine amenazas como malware y ransomware en las copias de seguridad.
- Conserve las copias de seguridad de datos en dispositivos separados y use almacenamiento fuera de línea para que los dispositivos infectados no puedan acceder a ellos.
- Realice copias de seguridad de máquinas virtuales, almacenamiento en la nube y sistemas operativos con RPO, teniendo en cuenta qué cantidad de pérdida de datos sería aceptable en caso de fallo.
- Use un sistema que permita guardar varias iteraciones de copias de seguridad, en caso de que alguna copia incluya archivos cifrados o infectados.
- Integre equipos para la recuperación de desastres y disponibilidad de las aplicaciones, y aproveche la inteligencia artificial para la protección de endpoints.
- Use el escaneo de vulnerabilidades, el cifrado SSL y demás controles técnicos para confirmar que las copias de seguridad se están realizando correctamente.
- Use la regla 3-2-1: cree tres copias de los datos, almacénelas en dos medios diferentes y guarde uno de ellos fuera del sitio.
- Realice pruebas periódicas de las copias de seguridad para verificar la integridad de los datos y garantizar su operatividad.
- Realice pruebas periódicas de los datos y los procesos de recuperación de desastres para garantizar que su empresa se encuentra preparada.

## 4 Implicar a los usuarios con formación y comunicaciones

**Brinde a sus usuarios la formación y las pautas que necesitan para protegerse frente a las amenazas de ransomware.**

- Ofrezca formación y comunicaciones periódicas de concientización para que todas las personas de su empresa comprendan la amenaza del ransomware y estén familiarizadas con las técnicas de seguridad.
- Establezca políticas de seguridad y prevención de ransomware para los usuarios finales.
- Oriente a los usuarios para que no abran correos electrónicos sospechosos, ni hagan clic en enlaces o abran archivos adjuntos, que presten atención a la hora de visitar sitios desconocidos y también cierren su navegador cuando no lo estén usando.
- Asegúrese de que los empleados sepan dónde y cómo denunciar actividades sospechosas.

## 5 Mantener y probar un plan de continuidad del negocio y recuperación de desastres

**Establezca, pruebe y mantenga las prácticas, los procedimientos y las herramientas tecnológicas necesarias para garantizar que las aplicaciones y los datos puedan recuperarse por completo en caso de desastre.**

- Elabore planes de contingencia y rehabilitación que son fundamentales para la recuperación y la continuidad del negocio, independientemente de cuál haya sido el origen del error.
- Realice una evaluación de riesgos que clasifique los tipos de desastres que podrían ocurrir y establezca prioridades para la recuperación y la continuidad del negocio.
- Despliegue soluciones de recuperación de desastres, copias de seguridad y alta disponibilidad tanto dentro como fuera de las instalaciones.
- Cuente con un plan de respuesta ante incidentes que incluya los pasos que deben seguirse en caso de que suceda un ataque de ransomware como, por ejemplo, desconectar el sistema infectado de la red para evitar que se propague la infección y determinar la confidencialidad de los datos involucrados.
- Pruebe el plan, incluidos los equipos y sistemas de tecnología, para garantizar que se está brindando una protección completa. Denuncie cualquier infección ante las autoridades correspondientes.

# ¿ESTÁ LISTO PARA HACER FRENTE AL RANSOMWARE?

Descargue la **evaluación de preparación frente al ransomware** que le permitirá medir sus capacidades y allanar el camino hacia un futuro libre de ransomware.

# UNA NUEVA TECNOLOGÍA PROMETE UN FUTURO LIBRE DE RANSOMWARE

Durante años, los profesionales de TI han buscado sin éxito una solución multicapa de protección/seguridad de datos de extremo a extremo que les permita obtener resiliencia de TI y prevención frente al ransomware. ¡Buenas noticias! Ahora existe una solución que ofrece exactamente eso: una primera y última línea de defensa contra la amenaza del ransomware.
Esta solución combina los productos Arcserve Appliance Series con Sophos Intercept X Advanced for Server para aplicar un enfoque multicapa que brinda seguridad y protección de datos integrales, todo en una sola plataforma unificada.

Los usuarios pueden beneficiarse de una completa gama de funcionalidades de sistemas autónomos que permiten eliminar la necesidad de recurrir a componentes individuales. Con una interfaz central para procesos de copia de seguridad, herramientas e infraestructura se obtiene una solución integral. Los productos Arcserve Appliance Series combinan almacenamiento deduplicado acelerado por flash, procesamiento sólido de servidores y redes de alta velocidad, todo con hardware altamente redundante y servicios en la nube.

A todo esto se suma la protección de endpoints de la mano de Sophos Intercept X Advanced for Server. Finalmente, obtendrá una solución de extremo a extremo que ofrece detección de malware basada en firmas y sin firmas, redes neuronales e inteligencia artificial avanzadas (deep learning), tecnología antiexploits y tecnologías antiransomware que brindan protección frente a la más amplia gama de amenazas contra endpoints.

¿El resultado? Una solución “todo en uno” sin precedentes: ciberseguridad de principio a fin, copia de seguridad de datos, recuperación de datos y alta disponibilidad, todo en una única plataforma que satisface las necesidades de cualquier infraestructura.

# RESUMEN

Si bien el ransomware representa un riesgo comercial significativo y una amenaza desafiante, el futuro no es tan pesimista. Hoy en día, las empresas pueden:

- **Implementar soluciones integradas de protección en profundidad** para obtener funcionalidades avanzadas de copia de seguridad, recuperación de desastres, alta disponibilidad y seguridad cibernética.
- **Habilitar prácticas de TI** mediante la participación efectiva de los usuarios, administración de datos y prácticas de recuperación de desastres que permitan un retorno de la inversión (ROI).
- **Ofrecer una primera y última línea de defensa** que acelere la detección de amenazas y permita la restauración inmediata de los datos respaldados.

Entonces, ¿por qué sentarse a esperar? ¿Por qué conformarse con un mundo donde los extorsionistas cibernéticos, los hackers y los malhechores recurren al ransomware para obtener injustamente ingresos de empresas que solo quieren trabajar y prosperar? Defiéndase. Mantenga sus datos seguros. Use tecnologías actuales de protección de extremo a extremo y prácticas adecuadas de administración de TI para garantizar que finalmente usted y su empresa puedan disfrutar de un futuro libre de ransomware.

## ACERCA DE ARCSERVE

Arcserve ofrece soluciones extraordinarias que permiten proteger los valiosos activos digitales de las empresas que necesitan una protección de datos integral y completa. Fundada en 1983, Arcserve es el proveedor con más experiencia del mundo en soluciones de continuidad del negocio que permiten proteger infraestructuras de TI de varias generaciones, con aplicaciones y sistemas en cualquier ubicación, en local y en la nube. Empresas de más de 150 países confían en la experiencia y las tecnologías increíblemente eficientes e integradas de Arcserve para eliminar el riesgo de pérdida de datos y los largos periodos de inactividad, con hasta un 50 % de ahorro en costes y complejidad en copias de seguridad y restauración de datos.

## ACERCA DE SOPHOS

Más de 100 millones de usuarios en 150 países confían en Sophos, que brinda la mejor protección contra amenazas complejas y la pérdida de datos. Sophos es una empresa comprometida a brindar soluciones de seguridad completas que son fáciles de implementar, administrar y usar, y que ofrecen el coste total de propiedad más bajo del sector. Sophos ofrece soluciones premiadas de cifrado y seguridad de endpoints, web, correos electrónicos, dispositivos móviles, servidores y redes, con el respaldo de SophosLabs, una red global de centros de inteligencia de amenazas.

## RECURSOS


1 https://cybersecurityventures.com/global-ransomware-damage-costs-predicted-to-reach-20-billion-usd-by-2021/

2 https://www.javelinstrategy.com/coverage-area/2019-identity-fraud-report-fraudsters-seek-new-targets-and-victims-bear-brunt
https://www.aarp.org/money/scams-fraud/info-2019/survey-identity-fraud-decline.html

3 https://risksense.com/press_release/risksense-spotlight-report-exposes-top-vulnerabilities-used-in-enterprise-ransomware-attacks/

4 https://healthitsecurity.com/news/fbi-alerts-to-rise-in-ransomware-attacks-urges-victims-not-to-pay

5 https://pdf.ic3.gov/2018_IC3Report.pdf

6 https://www.sophos.com/en-us/press-office/press-releases/2018/01/businesses-impacted-by-repeated-ransomware-attacks-according-to-sophos-global-survey.aspx

7 https://twitter.com/CarbonBlack_Inc/status/925348051782373382

8 https://healthitsecurity.com/news/fbi-alerts-to-rise-in-ransomware-attacks-urges-victims-not-to-pay

9 Encuesta Arcserve EMEA, 31 de julio de 2019

10 Encuesta Arcserve EMEA, 31 de julio de 2019


Para obtener más información sobre Arcserve, **visite arcserve.com/es**