Delinea

Informe del estado del ransomware 2025

Adaptación ágil a un panorama de amenazas en constante evolución

Resumen ejecutivo

El panorama del ransomware está cambiando nuevamente a medida que los atacantes usan la IA para lanzar ataques más sofisticados, lo que obliga a las organizaciones a adaptarse con rapidez y reforzar sus defensas.

Los adversarios están aprovechando un vasto mundo clandestino de ciberdelincuencia para intercambiar las herramientas y los consejos más recientes, perfeccionando sus campañas con ingeniería social basada en deepfakes, evasión inteligente de detección y estrategias de ataque automatizadas. Cada vez con más frecuencia, las credenciales comprometidas son el principal vector de acceso inicial de los atacantes.

Para entender lo que realmente está ocurriendo más allá de los titulares, Delinea ha recurrido a quienes están en primera línea: responsables de TI y seguridad que trabajan incansablemente para proteger sus organizaciones. El estudio de este año recopila información de más de 1000 profesionales de la ciberseguridad en diversas regiones y ofrece una perspectiva más amplia sobre el estado de la ciberseguridad. El mensaje es claro: los ataques de ransomware están aumentando, aunque los pagos de rescates disminuyen, y las interrupciones comerciales pueden durar semanas. Es más, la extorsión ahora representa más de la mitad de los ataques de ransomware. Estos defensores de la red están adoptando IA, pero eso por sí solo no garantiza el éxito.

En este informe, aprenderá cómo los atacantes se están volviendo más agresivos y sofisticados, y cómo las organizaciones están adoptando medidas proactivas para detectar, mitigar y prevenir ataques de ransomware, lo que le permitirá tomar decisiones más fundamentadas sobre su propio programa de seguridad.

Conclusiones clave

- **Las vulneraciones por ransomware siguen aumentando, aunque cada vez paguen menos víctimas**
  - El ransomware está muy extendido: el 69 % de las organizaciones ha sufrido alguna vulneración y más de una cuarta parte ha recibido un ataque más de una vez.
  - El 60 % del ransomware ahora implica extorsión relacionada con el robo de datos.
  - Menos organizaciones (57 %) están pagando
  - Los atacantes siguen teniendo incentivos para actuar
- **Los ejecutivos muestran una preocupación creciente, pero las medidas de seguridad no están a la altura**
  - El ransomware está provocando un caos generalizado: el 75 % de las víctimas tarda dos semanas en recuperarse
  - El 90 % de los ejecutivos manifiesta preocupación por el ransomware
  - Las tácticas tradicionales contra el ransomware ya no están dando resultados
  - Solo un tercio de las organizaciones ha adoptado una política de mínimo privilegio, dejando abiertas rutas de acceso críticas para los atacantes
- **El uso de la IA está aumentando a medida que evolucionan las amenazas de ransomware**
  - La IA está dando más poder a los atacantes
  - Los grupos de ransomware son camaleónicos y persistentes
  - El 90 % de las afirma utilizar IA para combatir el ransomware

Conclusión clave 1:

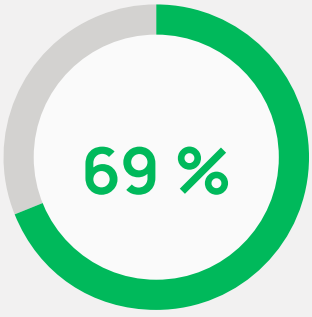
Las vulneraciones por ransomware siguen aumentando, aunque cada vez paguen menos víctimas

El ransomware está muy extendido

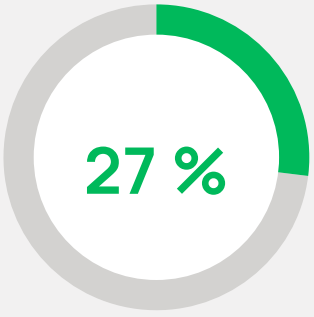
Los ataques de ransomware que consiguen tener éxito han aumentado. Más de dos tercios de los encuestados sufrieron vulneraciones por ransomware durante el último año; en Estados Unidos, estas vulneraciones aumentaron aproximadamente un tercio. Además, más de una cuarta parte de los encuestados fue víctima en más de una ocasión. Sea lo que sea lo que estén haciendo las organizaciones, no es suficiente para frenar el auge de la extorsión digital.

La mayoría de las empresas sufrió al menos una vulneración de seguridad durante el último año.

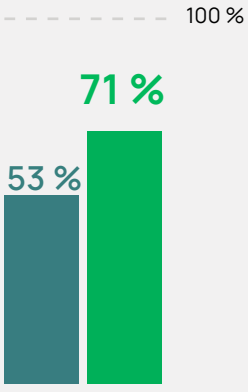
P: ¿Ha sido víctima su empresa de un ataque de ransomware en los últimos 12 meses?



de las organizaciones sufrieron vulneraciones por ransomware



de las organizaciones ha recibido más de un ataque

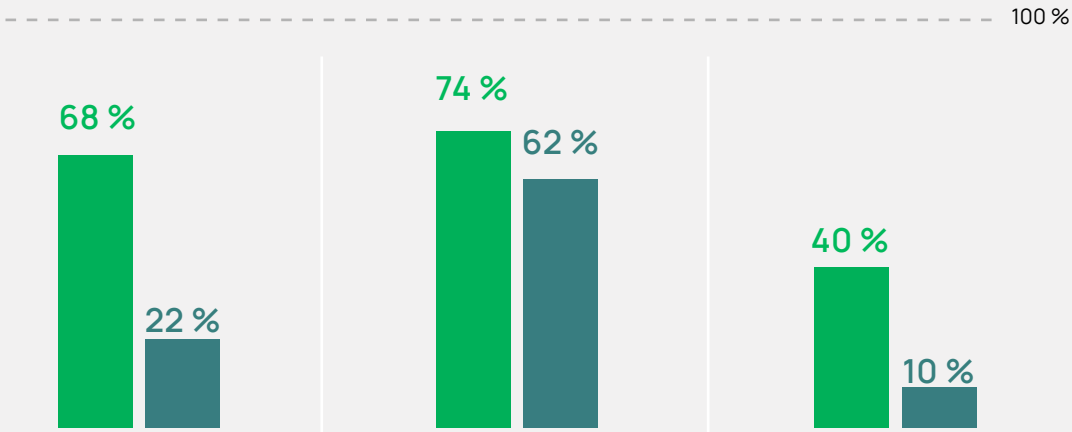


de las vulneraciones en EE. UU. aumentaron del 53 % al 71 % en 2023

En Estados Unidos, las organizaciones más grandes experimentaron el mayor aumento de vulneraciones. Las grandes empresas son señaladas como «objetivo de primera» y son blanco de sofisticados ataques «manuales» para obtener grandes recompensas. Sin embargo, las empresas más pequeñas no son inmunes y suelen considerarse presa fácil de campañas más simples y generalizadas.

Los ataques de ransomware en EE. UU. aumentaron el año pasado

P: ¿Ha sido víctima su empresa de un ataque de ransomware en los últimos 12 meses?



Gran empresa EE. UU. (más de 500 empleados): 68 % frente al 22 % en 2023

Mediana empresa EE. UU. (50-500 empleados): 74 % frente al 62 % en 2023

Pequeña empresa EE. UU. (1-49 empleados): 40 % frente al 10 % en 2023

¿Qué industrias están registrando el mayor aumento de amenazas? Según la encuesta de Delinea, la industria de TI y telecomunicaciones de EE. UU. sufrió el año pasado un 65 % más de ataques que el año anterior. Mientras que el comercio minorista, la hostelería y el ocio sufrieron un 57 % más de ataques, las organizaciones del sector sanitario siguen siendo un objetivo habitual: una de cada dos informó de ataques el año pasado. Aunque no hay dos organizaciones iguales, estos sectores comparten varias características clave, en particular su baja tolerancia a las interrupciones del servicio o el gran volumen de datos sensibles que gestionan de clientes y empleados.

¿Qué industrias son las más afectadas?

Según el equipo de investigación de Delinea Labs en su informe «La ciberseguridad y el panorama de amenazas de la IA», la tecnología, la manufactura y la sanidad estuvieron entre las industrias que más ataques sufrieron el año pasado. Estas industrias probablemente fueron seleccionadas por su baja tolerancia a las interrupciones del servicio y, por lo tanto, su mayor probabilidad de pago. El sector sanitario, en particular, es vulnerable debido a la naturaleza sensible de los datos de los pacientes, y las vulneraciones dejan al descubierto información confidencial y ponen en peligro vidas humanas.

Fuente: Delinea Labs, «La ciberseguridad y el panorama de amenazas de la IA», enero de 2025

La gran pregunta es ¿por qué sigue aumentando el número de ataques exitosos de ransomware? A continuación se presentan algunos factores clave:

- **El robo de credenciales no deja de aumentar.** Según el Informe de investigaciones sobre la filtración de datos de Verizon de 2025, el uso de credenciales robadas apareció en casi un tercio (32 %) de las vulneraciones el año pasado. Estas combinaciones robadas de nombre de usuario y contraseña facilitan a los atacantes eludir las defensas tradicionales e infiltrarse en las redes corporativas.
- **El ransomware como servicio (RaaS) se ha extendido.** El informe La ciberseguridad y el panorama de amenazas de la IA de Delinea Labs de 2025 indica que el modelo RaaS se ha vuelto más común, lo que amplía el acceso a ataques sofisticados para atacantes con menos conocimientos técnicos. El modelo RaaS suele tener como objetivo sectores como la tecnología, la manufactura y la construcción.
- **Los agentes de acceso inicial (initial access brokers o IAB) cada vez son más numerosos.** Delinea Labs considera que los IAB (atacantes especializados en comprometer accesos iniciales) están contribuyendo aún más al crecimiento de los ataques de ransomware. Algunos sitios vinculados a IAB incluso permiten a los compradores potenciales probar si las credenciales comprometidas funcionan antes de adquirirlas. Las credenciales de cuentas privilegiadas son especialmente valiosas, sobre todo aquellas que permiten acceder a sistemas de identidad corporativa como Active Directory, donde se almacenan las «llaves de la fortaleza».

Los grupos de ransomware son camaleónicos y persistentes

La investigación de Delinea revela que los cinco principales grupos de ransomware representaron el 36 % de los 5700 incidentes evaluados en el último año. Destaca la fluidez y persistencia del mundo clandestino de la ciberdelincuencia, con grupos que suelen cambiar de nombre para escapar al escrutinio y continúan operando a pesar de las acciones de las fuerzas del orden. Según el Informe de Delinea Labs, los cinco grupos principales por actividad son:

- **RansomHub:** versión renombrada de Knight, centrada en la extorsión principalmente a través del robo de datos; es un grupo RaaS de gran relevancia.
- **LockBit:** grupo RaaS muy conocido y prolífico desde 2019, que emplea sofisticadas técnicas de cifrado. Sigue activo, aunque con menor capacidad, a pesar de detenciones e intentos de desmantelamiento.
- **Play:** activo desde 2022, emplea cifrado intermitente como parte de sus tácticas de doble extorsión, lo que acelera la codificación de los archivos de las víctimas.
- **Akira:** grupo agresivo surgido en 2023 y vinculado al desaparecido grupo Conti.
- **Hunters International:** otro grupo RaaS, conocido por su sofisticado malware y que se cree que es una rama del grupo de ransomware Hive ya desmantelado

La mayoría del ransomware actual incluye extorsión mediante robo de datos

Los investigadores de Delinea afirman que la mayoría de los principales grupos de ransomware siguen ahora un modelo de doble extorsión. Así lo corrobora este estudio: el 60 % de las víctimas de ransomware encuestadas afirma haber sufrido robo de datos y el 85 % haber sido amenazado con la publicación o venta de sus datos.

Si hoy en día la extorsión se centra predominantemente en el robo de información, entonces las copias de seguridad suponen una estrategia de mitigación menos útil si se utilizan de forma aislada. Las organizaciones deben disponer, en cambio, de diversas técnicas de defensa. El énfasis debe ponerse en una seguridad proactiva y preventiva que impida que se produzca el robo de datos desde el principio.

Cada vez pagan menos empresas, pero aún queda mucho camino por recorrer

Más de la mitad de los encuestados declaró haber ignorado el consejo de las fuerzas de seguridad y de las autoridades, y haber pagado un rescate el año pasado para acelerar su recuperación. Aunque el año pasado pagaron menos empresas estadounidenses que el año anterior.

Pagar el rescate no siempre produce los resultados esperados. Aproximadamente uno de cada cuatro encuestados que pagaron rescate dijo que no recuperó todos sus datos, cifra que aumenta a uno de cada tres en el Reino Unido. Incluso si lo hacen, es probable que sus adversarios intenten seguir monetizando esos datos.

Pagar un rescate no garantiza la recuperación de los datos.

P: Si su empresa ha sido víctima de un ataque de ransomware en los últimos 12 meses, ¿pagó el rescate? Y si la empresa pagó el rescate, ¿recuperó los datos?

57 %

de las organizaciones pagó ransomware

60 %

de las organizaciones estadounidenses pagó ransomware frente al 76 % en 2023

54 %

de las organizaciones del Reino Unido pagó ransomware

26 %

de las organizaciones que pagaron un rescate no recuperaron sus datos (35 % en el Reino Unido; 18 % en los EE. UU.)

Mientras haya brechas de seguridad que investigar, víctimas dispuestas a pagar y regímenes que ofrezcan refugio al crimen organizado, la amenaza continuará. Ahora que la IA ofrece una nueva ventaja a los adversarios, los defensores de su red deben revaluar urgentemente su estrategia contra el ransomware.

Conclusión clave 2

Los ejecutivos muestran una preocupación creciente, pero las medidas de seguridad no están a la altura

El ransomware está causando caos y disrupción

Las organizaciones siguen viéndose duramente golpeadas por los ataques de ransomware. Descubrimos que casi la mitad de las víctimas tardaron hasta una semana (entre uno y seis días) en recuperarse de un ataque de ransomware. Tres cuartas partes de los encuestados afirmaron haber tardado hasta dos semanas. Pocos lograron recuperarse en menos de 24 horas. Y es probable que, en esos casos, los atacantes fueran descubiertos rápidamente antes de tener la oportunidad de robar datos o cifrar sistemas.

El tiempo de recuperación es lento

P: Si su empresa ha sufrido un ataque de ransomware, ¿cuánto tiempo le llevó restablecer las operaciones por completo?

46 %

de las víctimas tardó hasta una semana en recuperarse de un ataque de ransomware

(50 % de las empresas del Reino Unido y 42 % de las empresas de EE. UU.)

75 %

de las víctimas tardó hasta dos semanas en recuperarse

18 %

Solo el 18 % de las víctimas se recuperó en menos de 24 horas.

Muchas organizaciones no tienen tanta suerte. Hay varias etapas de respuesta y recuperación ante incidentes que debemos seguir. Primero se procede al aislamiento de los sistemas afectados y la determinación del alcance del ataque. Después, se elimina por completo cualquier malware y se reconstruyen los sistemas. A continuación, debe notificarse a todas las partes pertinentes. En algunos casos, también puede ser útil abrir un diálogo con los atacantes. Por último, deben restaurarse los datos cifrados desde la copia de seguridad. Todo ello requiere tiempo y dinero.

Aunque nuestro estudio revela que menos del 1 % de las organizaciones siguen recuperándose de un ataque pasado un mes, estos casos pueden tener un impacto enorme en los clientes y, a veces, incluso en comunidades enteras. Por ejemplo, en junio de 2024, un ataque de ransomware contra Synnovis, proveedor de servicios de laboratorio del sistema público de salud del Reino Unido (NHS), provocó el aplazamiento de miles de citas ambulatorias y procedimientos en Londres. Se realizó una llamada urgente para nuevos donantes de sangre. Incluso tres meses después, no todos los sistemas se habían restablecido.

De manera similar, los recientes ataques de ransomware contra los comercios minoristas del Reino Unido Marks & Spencer y Co-op interrumpieron significativamente las operaciones, afectando a los servicios y las cadenas de suministro. En el caso de algunas organizaciones, una vulneración grave de ransomware puede convertirse en una amenaza existencial. Con sede en Kettering (Reino Unido), el grupo logístico KNP se vio obligado a acogerse a un procedimiento concursal tras un ataque de ransomware en junio de 2023, lo que supuso la pérdida de 730 puestos de trabajo.

Según un estudio del Gobierno del Reino Unido, las organizaciones atacadas mediante ransomware podrían enfrentarse a:

- Pérdida de futuros beneficios
- Pérdida de oportunidades de negocio
- Costes de TI adicionales
- Daños a la reputación
- Pérdida de confianza en la dirección ejecutiva
- Impacto psicológico y físico adicional por estrés y ansiedad en el personal

Si su organización no cuenta con un programa sólido de continuidad del negocio y recuperación ante desastres que incluya un plan de respuesta ante incidentes bien diseñado y ensayado, pueden presentarse dificultades. Practicar escenarios pesimistas es fundamental para garantizar que cada parte implicada conozca su función e identificar posibles problemas ocultos. Podría tratarse de algo tan básico como decidir en qué orden restaurar los datos de las copias de seguridad. Los equipos de TI no deben dar por sentado que, por estar todo respaldado en la nube, la recuperación será sencilla.

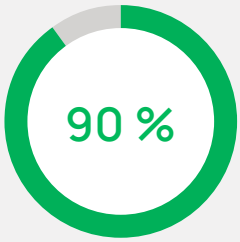
La gestión de accesos con privilegios (PAM) puede ayudar a reducir el tiempo de recuperación y los costes al limitar el movimiento lateral de los atacantes desde el inicio. Si disponen de un entorno más reducido en el que operar y causar daños, probablemente se llevarán menos datos.

La preocupación de los ejecutivos está justificada

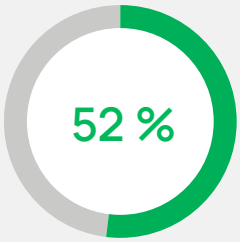
Dado el impacto potencial del ransomware en sus organizaciones, no sorprende que nueve de cada diez responsables de la toma de decisiones expresaran su preocupación ante esta amenaza. Y su inquietud va en aumento. Más de la mitad de los ejecutivos estadounidenses están ahora muy preocupados, frente a poco más de una cuarta parte en 2023. El mayor incremento se registró entre algunas de las empresas más grandes. Esto coincide con el aumento de víctimas entre empresas de ese tamaño y con el riesgo financiero y reputacional derivado de una vulneración grave.

Los líderes ejecutivos están cada vez más preocupados

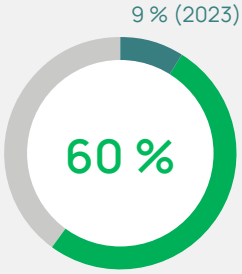
P: ¿Cuál de las siguientes afirmaciones describe mejor la preocupación de su junta directiva y del equipo ejecutivo ante el ransomware dirigido a su organización?



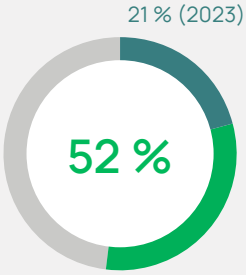
de los ejecutivos y juntas directivas está preocupado por la amenaza del ransomware



de las empresas estadounidenses está muy preocupado frente al 26 % en 2023



Empresas estadounidenses con ingresos de 250-499 millones USD: el 60 % está muy preocupado frente al 9 % en 2023

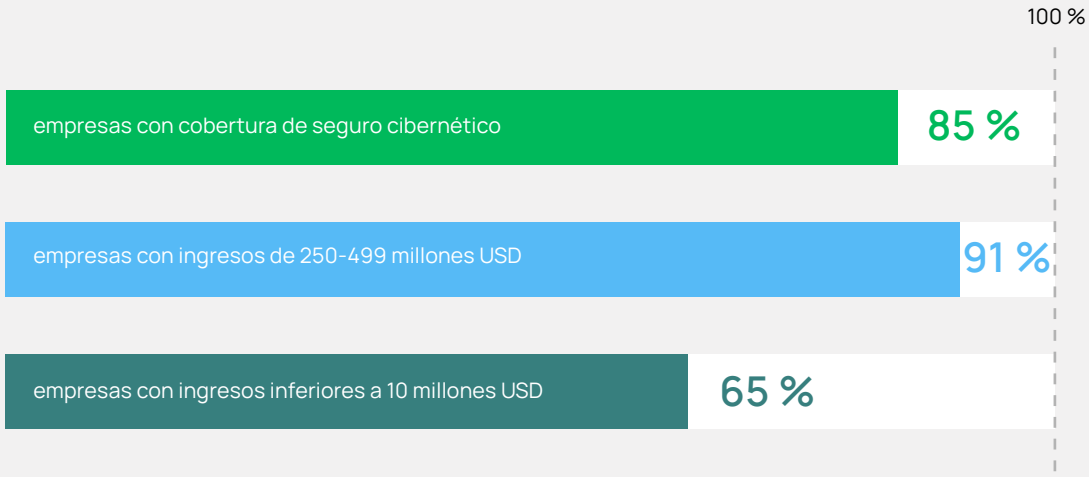


Empresas estadounidenses con ingresos de más de 500 millones USD: el 52 % está muy preocupado frente al 21 % en 2023

Estas inquietudes podrían traducirse en niveles relativamente altos de contratación de **ciberseguros**. De media, cuatro de cada cinco empresas afirman tener un ciberseguro. Las empresas más grandes tienen más probabilidades de contar con esa cobertura. Aunque las empresas más pequeñas tienen menores niveles de cobertura, deberían considerarla como una parte útil dentro de un enfoque integral de ciberseguridad.

Las empresas más grandes tienen más probabilidades de contar con un ciberseguro.

P: ¿Cuenta su empresa con un seguro que incluya cobertura ante ataques de ransomware?



Una póliza de seguro puede contribuir a mitigar el riesgo financiero derivado de un incidente. Pero cada vez más, las aseguradoras también exigen medidas de seguridad consideradas buenas prácticas como requisito previo a la cobertura, lo que puede ayudar a reforzar la postura de ciberseguridad corporativa. Algunas también ofrecen apoyo y recursos para medidas de seguridad preventiva y respuesta a incidentes, algo que puede ser especialmente útil para asegurados más pequeños.

Las tácticas tradicionales contra el ransomware no están dando resultados

Entonces, ¿cómo están respondiendo los ejecutivos ante el aumento de las amenazas de ransomware?

El número medio de encuestados con planes de respuesta ante incidentes activos es del 90 %, una cifra que, aunque se ha mantenido estable respecto al año anterior, sigue siendo tranquilizadora. También es destacable que las empresas más pequeñas (con menos de 50 empleados) registraron el aumento más significativo en respuesta a incidentes: del 60 % al 79 % en el transcurso de un año. Si el plan de respuesta se diseña de forma pragmática, incluye a todas las partes implicadas en la empresa y se practica con regularidad, puede ayudar a agilizar los esfuerzos de recuperación ante ransomware.

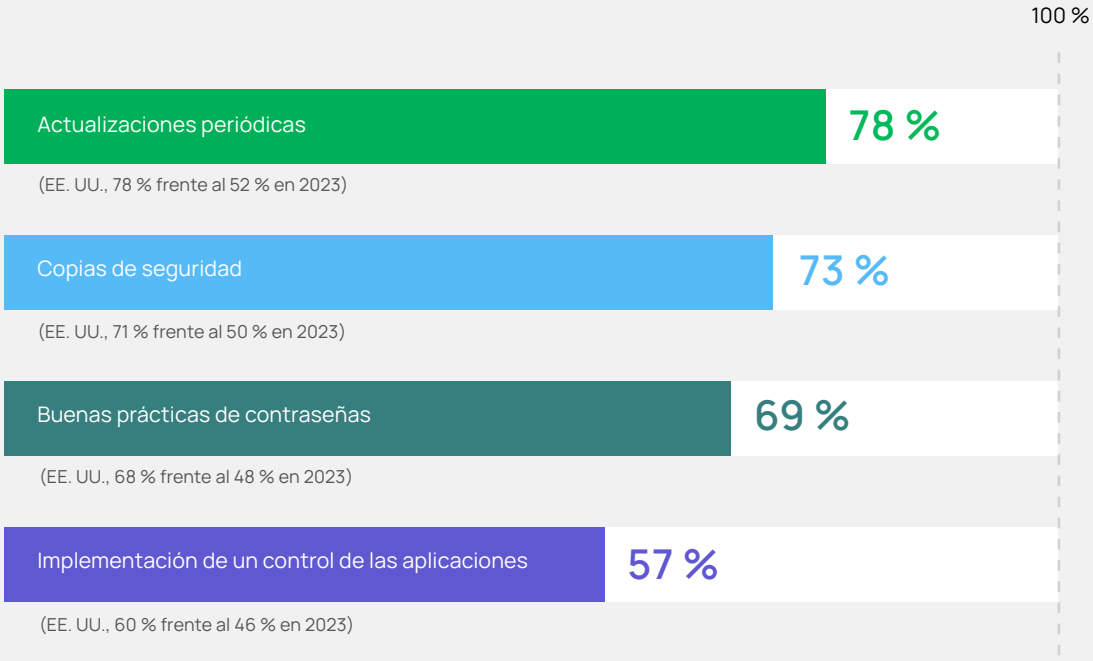
Ahora bien, resulta más eficaz centrarse en la prevención: una vez robados los datos, lo más probable es que los atacantes intenten monetizarlos. Estas fueron las cuatro medidas preventivas principales adoptadas por los encuestados el año pasado:

1. Actualización periódica de los sistemas y del software
2. Copia de seguridad de datos críticos
3. Aplicación de las prácticas recomendadas en materia de contraseñas
4. Implementación de un control de las aplicaciones

En Estados Unidos, la adopción de estas buenas prácticas registró un importante incremento con respecto al año anterior.

EE. UU. intensifica la aplicación de medidas preventivas

P: ¿Qué medidas, si las hay, ha tomado para evitar un ataque de ransomware? (Seleccione todas las que correspondan).



Sin embargo, por muy útiles que resulten estas buenas prácticas de ciberhigiene, basta con echar un vistazo a las cifras de víctimas de ransomware en la parte superior de este informe para ver que, claramente, no están funcionando. Una parte del problema es la enorme extensión de la superficie de ataque corporativa. Esta ha aumentado en los últimos años debido al trabajo remoto, las inversiones en activos en la nube, la proliferación de puntos finales del Internet de las cosas (IoT), las aplicaciones nativas en la nube desarrolladas internamente y el auge de la IA con capacidad de actuación.

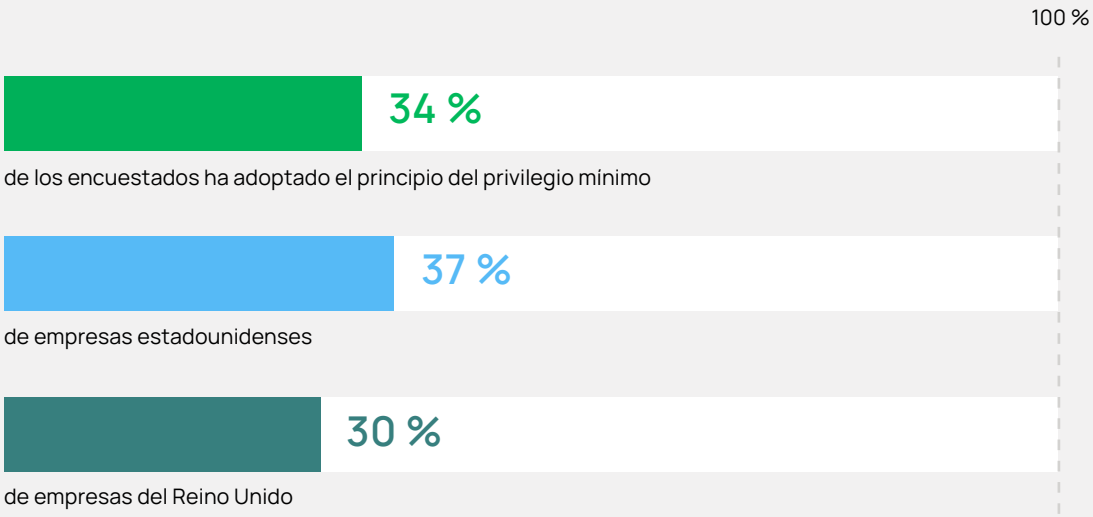
En la práctica, esto significa que los adversarios tienen un objetivo muy amplio y muchos vectores potenciales para sus ataques. Las ofertas de servicios preempaquetados contribuyen a reducir las barreras de entrada. Los IAB ofrecen acceso sencillo a redes corporativas y cuentas en la nube. Y existe un mercado ya consolidado en el que pueden vender los datos robados.

El principio de privilegios mínimos está lamentablemente infrarrepresentado

Otra de las razones por las que prosperan los actores de ransomware es la escasa atención que prestan las organizaciones a la gestión de la identidad. Aproximadamente uno de cada tres encuestados afirma haber adoptado una política de privilegios mínimos. Este principio de seguridad estipula que los usuarios y los sistemas solo reciben los permisos estrictamente necesarios para realizar sus tareas, nada más.

Pocas empresas aplican el principio de privilegios mínimos

P: ¿Qué medidas, si las hay, ha tomado para evitar un ataque de ransomware? (Seleccione todas las que correspondan).



¿Por qué es importante? En un contexto de ransomware, el principio de privilegios mínimos ayuda a reducir tanto la superficie de ataque como el radio de acción de los mismos:

- Evitando que los usuarios instalen aplicaciones no autorizadas o potencialmente inseguras, lo que podría permitir el acceso inicial a atacantes.
- Bloqueando los desplazamientos laterales y restringiendo así el acceso a usuarios, cuentas, aplicaciones y servicios.
- Limitando el acceso de terceros de riesgo potencial.

Cuando se combina con la segregación de funciones (SoD) y se complementa con la solución PAM, la autenticación multifactor (MFA) y análisis impulsados por IA, el principio de privilegios mínimos constituye un pilar esencial del modelo de confianza cero. Este principio de seguridad postula que ningún usuario ni sistema deben considerarse intrínsecamente fiable, y que todos deben autenticarse de forma continua según un modelo basado en el riesgo.

Sin embargo, en muchos entornos, aplicar este principio resulta más complejo: respaldar políticas sólidas o hacerlas cumplir puede explicar su escasa adopción entre los encuestados. Dependiendo del tamaño de la organización, puede ser necesario gestionar de forma continua miles de usuarios, aplicaciones y servicios.

Para llevarlo a cabo con éxito, es necesario un sistema de gestión de identidades y accesos (IAM) maduro, con funciones y responsabilidades bien definidas, vinculadas a los usuarios y auditadas periódicamente en todos los sistemas. La gestión de derechos en la nube (CIEM) y la detección y respuesta a amenazas de identidad (ITDR) también desempeñan un papel clave, ya que permiten identificar cuentas privilegiadas, supervisar el uso, investigar anomalías y responder a incidentes con controles eficaces. La gobernanza es un componente esencial en toda estrategia de IAM, ya que combina personas, procesos y tecnología en un único enfoque integrado.

Conclusión clave 3

El uso de la IA está aumentando a medida que evolucionan las amenazas de ransomware

La IA está otorgando nuevas capacidades a los actores de ransomware

El modelo de confianza cero, la solución PAM y la aplicación de privilegios mínimos son cada vez más importantes en un panorama de amenazas en rápida evolución. El Centro Nacional de Seguridad Cibernética del Reino Unido (NCSC) advirtió a principios de 2024 que la IA «casi con toda seguridad, aumentaría el volumen y agravaría el impacto de los ciberataques en los próximos dos años». Sus predicciones ya se están cumpliendo. Tengamos en cuenta, por ejemplo, al grupo de ransomware FunkSec, que se cree que utiliza IA generativa (GenAI) para crear su propio malware.

Los investigadores de Delinea Labs creen que los atacantes utilizarán GenAI en el futuro para imitar el estilo de escritura de empleados, clientes y proveedores, con el fin de aumentar la tasa de éxito de los ataques de phishing. También podrían crear sitios de phishing que reproduzcan el portal de una organización y usar voz o vídeo generados por IA para hacerse pasar por compañeros de confianza y convencer a los empleados de que descarguen malware.

El futuro de la IA se presenta con cada vez más capacidad de actuación: la IA funciona de forma autónoma y dinámica, resolviendo problemas y completando tareas sobre la marcha para alcanzar sus objetivos. Delinea ya observa ejemplos de esta tecnología incipiente, capaz de automatizar muchas de las etapas típicas de un ataque de ransomware, incluidas el reconocimiento, la explotación y la exfiltración. El riesgo es que esta tecnología reduce aún más las barreras de entrada para los potenciales actores asociados a redes de ransomware y les otorga la capacidad de lanzar ataques a gran escala contra objetivos muy específicos, con muy pocos recursos.

El verdadero desafío para su organización es que esto no solo podría aumentar el volumen de ataques, sino también acortar las fases iniciales de la cadena de ataque. Ello hace que la detección y la respuesta sean más difíciles, y desplaza el enfoque hacia la seguridad preventiva.

La IA se está adoptando de forma generalizada en la lucha contra el ransomware

La buena noticia es que el 90 % de los equipos de seguridad de TI con los que hablamos ya están utilizando IA para mantener a raya a sus adversarios. La están utilizando principalmente de tres maneras:

1. **En el centro de operaciones de seguridad (SOC)**

Los equipos del SOC se encuentran en la primera línea contra las ciberamenazas entrantes, incluido el ransomware. A menudo trabajan bajo presión y con recursos limitados, afrontando carencias de personal cualificado y una sobrecarga de alertas. Aquí es donde la IA puede brindar una ayuda muy necesaria: clasificando y enriqueciendo eventos con datos adicionales y luego enviándolos al analista adecuado para que pueda tomar decisiones mejor informadas. Los modelos más avanzados pueden realizar trabajo de analista de nivel 3 revisando datos de amenazas y brindando recomendaciones sobre cómo proceder. La inteligencia artificial con capacidad de actuación puede realizar de forma autónoma la búsqueda de amenazas para obtener información útil sobre posible actividad maliciosa dentro de la red.

2. **Para analizar indicadores de compromiso (IoC)**

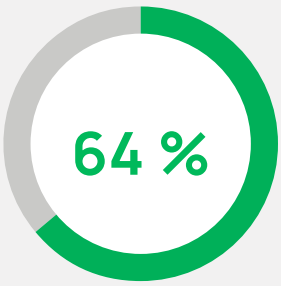
La IA es excelente para analizar grandes volúmenes de datos y buscar patrones que las personas podrían pasar por alto, y lo hace las 24 horas del día, los 7 días de la semana y los 365 días del año. Con este fin, resulta perfecta para ayudar a cribar los IoC, a menudo en un entorno SOC. Se podría programar una IA para recopilar una gran variedad de IoC de diferentes fuentes internas y externas. Se trata de liberar a los expertos humanos para que se concentren en tareas de operaciones de seguridad más valiosas, entregándoles información útil. Esto puede acelerar la detección y respuesta ante amenazas.

3. **Para prevenir el phishing**

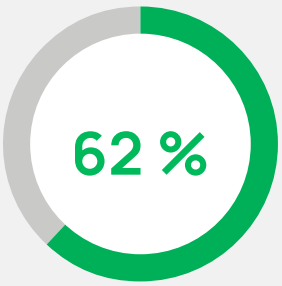
Puede entrenar algoritmos de IA para analizar correos electrónicos en busca de estilos de escritura sospechosos que no coincidan con el autor o comportamientos inusuales, como mensajes enviados a una hora extraña o con contenido poco habitual. La IA puede analizar enlaces, archivos adjuntos e imágenes, incluidos códigos QR. Incluso puede ayudar a crear ejercicios de simulación realistas para la capacitación del personal, así como a monitorizar las respuestas de los empleados.

Tres formas en que la seguridad informática utiliza la IA

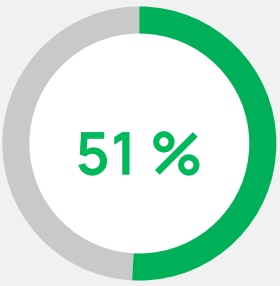
P: ¿Cómo utiliza su organización hoy la IA para protegerse contra ataques de ransomware? (Seleccione todas las que correspondan).



En el centro de operaciones de seguridad



Para analizar indicadores de compromiso (IoC)



Para prevenir el phishing

Otros casos prácticos de la IA

Además de estos usos, la tecnología también se está abriendo camino en herramientas IAM y PAM, con resultados impresionantes. Esto incluye:

- **Automatización de tareas rutinarias**

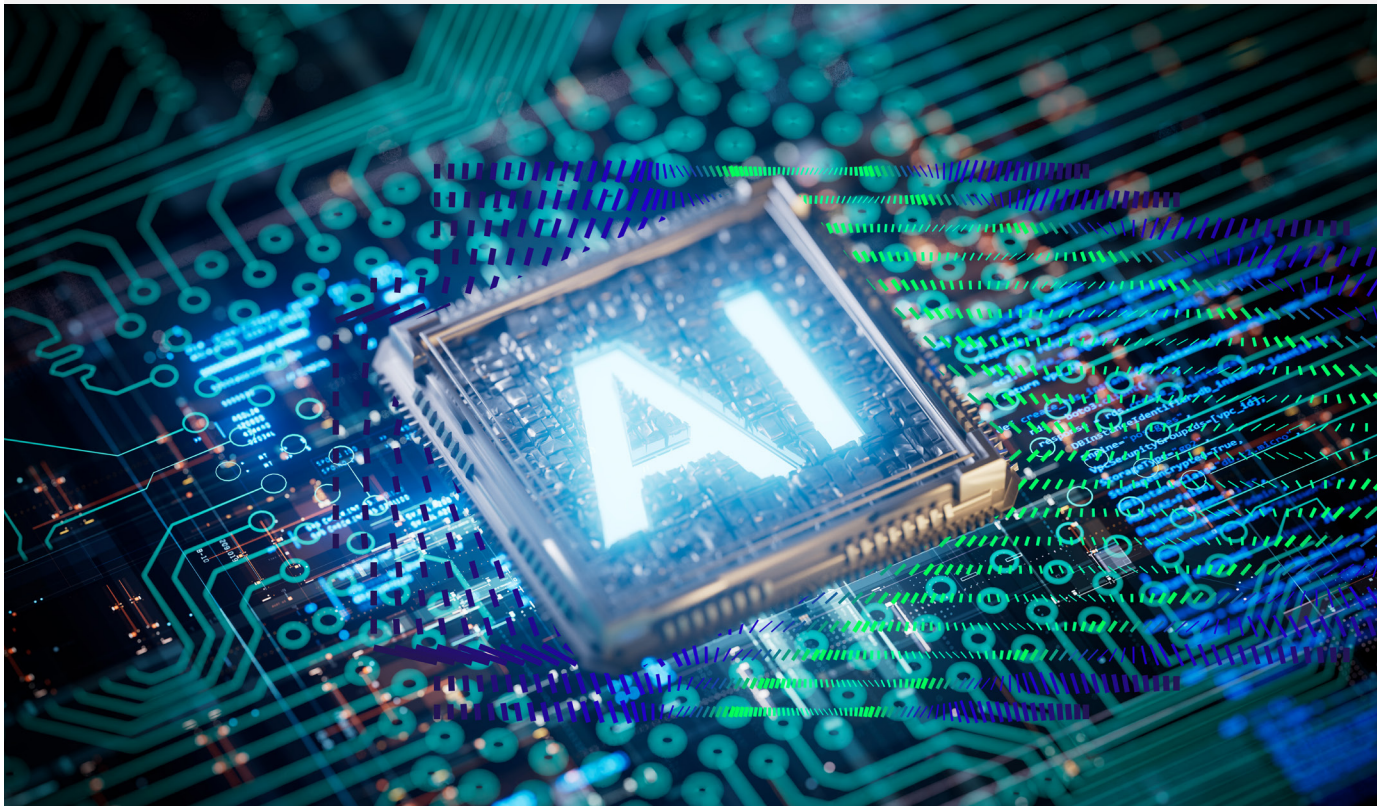
  Automatización del aprovisionamiento de cuentas, las revisiones de acceso de usuarios, el modelado de roles y otras tareas que consumen mucho tiempo y son propensas a errores humanos si se realizan manualmente, especialmente en organizaciones grandes.

- **Auditoría de sesiones**

  Uso de la IA para monitorizar sesiones y detectar problemas de seguridad, como identidades con demasiados privilegios o comportamiento privilegiado inesperado. Proporciona a los equipos un enfoque más eficiente, en comparación con las revisiones manuales de registros que consumen mucho tiempo.

- **Autorización inteligente para la defensa contra ransomware**

  La inteligencia artificial con capacidad de actuación define y optimiza las políticas de autorización y las aplica de forma automática. Esto significa que los usuarios no necesitan crear ni recordar contraseñas, y los equipos de TI no necesitan establecer permisos ni realizar un seguimiento de los cambios de políticas. Este tipo de autorización impulsada por IA será cada vez más crítica para la prevención del ransomware a medida que aumente el número de amenazas, las superficies de ataque, las brechas de habilidades en materia de ciberseguridad y la complejidad de los entornos.



Cómo pueden protegerse las empresas

Las credenciales robadas siguen siendo un factor principal en las vulneraciones de datos. No solo ayudan a los atacantes a obtener acceso inicial a las redes corporativas, sino que también aumentan los privilegios y se mueven lateralmente para causar el máximo daño.

Es una de las muchas razones por las que las vulneraciones de ransomware están aumentando. Dado que la IA ayuda a que los ataques sean más rápidos y exitosos, los ejecutivos están preocupados, y con razón. Ahora es el momento de convertir esa preocupación en acción.

Las defensas en capas son importantes. Deben incluir programas efectivos de capacitación y concienciación, parches basados en riesgos, copias de seguridad periódicas, controles de aplicaciones, antimalware, monitorización de red y un plan de respuesta ante incidentes probado periódicamente. Además, una estrategia de seguridad de la identidad sólida es absolutamente fundamental. La visibilidad y el control integrales y centralizados de todas las identidades de sus empleados y máquinas ayudarán a bloquear a los atacantes y limitar el daño que pueden causar si comprometen sus recursos.

Tómese su tiempo a la hora de evaluar a los proveedores. Elija una marca fiable que ofrezca capacidades mejoradas con inteligencia artificial, como monitorización de sesiones y autorización inteligente. Esto ayudará a minimizar los problemas, aumentar la resiliencia y optimizar la defensa contra el ransomware, al tiempo que allana el camino hacia la confianza cero.

Es la tranquilidad que necesita para desarrollar su negocio y aprovechar el potencial de su plantilla, sin comprometer la seguridad.

Obtenga más información sobre cómo una estrategia de seguridad de identidad sólida puede ayudar a combatir el ransomware en Delinea.com/es/.

Delinea

Securing identities at every interaction

Delinea es pionera en la protección de identidades humanas y de máquinas a través de una autorización inteligente y centralizada, permitiendo a las organizaciones gestionar sin problemas sus interacciones en entornos complejos. Al aprovechar la inteligencia impulsada por IA, la plataforma líder de seguridad de identidades nativa de la nube de Delinea aplica el contexto a lo largo de todo el ciclo de vida de la identidad en la infraestructura tradicional y en la nube, los datos, las aplicaciones SaaS y la IA. Es la única plataforma que permite descubrir todas las identidades (incluidos trabajadores, administrador de TI, desarrolladores y máquinas), asignar niveles de acceso adecuados, detectar irregularidades y responder a las amenazas en tiempo real. Con un tiempo de despliegue de semanas, en lugar de meses, un 90 % menos de recursos que gestionar que su competidor más cercano y un tiempo de actividad del 99,995 %, Delinea Platform ofrece seguridad sólida y eficiencia operativa sin complejidad. Obtenga más información sobre Delinea en **Delinea.com/es/**, **LinkedIn**, **X** y **YouTube**.

© Delinea RR2025-WP-0525-ES