Delinea

DOCUMENTO TÉCNICO

La seguridad de la identidad es fundamental para obtener y mantener un ciberseguro

Informe de investigación sobre ciberseguros 2024

Resumen ejecutivo

El ciberseguro es un componente fundamental de un programa de gestión de ciberriesgos para garantizar la resiliencia y la recuperación. Ahora que tener un ciberseguro se ha convertido en una práctica estándar para organizaciones de todo tipo, el enfoque se ha desplazado hacia la aptitud para la concesión de dichos seguros, incluso cuando cambian los factores de riesgo.

A medida que los ciberincidentes han sacudido la industria, las aseguradoras están realizando evaluaciones de riesgos detalladas y es cada vez más difícil para los líderes informáticos demostrar el valor de su programa de seguridad y obtener una cobertura sólida. Las organizaciones deben proporcionar evidencia relevante para cerciorarse de que su seguro continúa y aumenta o se ajusta según sea necesario. Para organizaciones complejas e híbridas con perfiles de riesgo en constante evolución, recopilar información precisa y actualizada puede ser un trabajo increíblemente engorroso y que consume demasiado tiempo.

En este estudio de investigación de 300 tomadores de decisiones, analizamos cómo las empresas están abordando estos desafíos para obtener y mantener sus ciberseguros. En particular, exploramos cómo las organizaciones están adoptando tecnologías más novedosas como la inteligencia artificial para aumentar la eficiencia, escalar rápidamente y reducir los costes.

Conclusiones clave:

1. **Las brechas en la seguridad de la identidad son la causa más común de ciberincidentes que tienen como resultado reclamaciones a las aseguradoras. Las infracciones de identidad y privilegios representan el 47 % de los ataques que dan lugar a las reclamaciones a aseguradoras.**

2. **Las aseguradoras quieren evidencia de seguridad de la identidad antes de conceder pólizas. Más del 40 % de las aseguradoras exigen controles de acceso/autorización con el mínimo privilegio antes de conceder pólizas. Prácticamente todas las empresas estadounidenses (el 95 %) tuvieron que invertir en soluciones de seguridad de identidad antes de conseguir sus pólizas.**

3. **Si bien los costes generales de los ciberseguros están aumentando, la IA está brindando ventajas a los asegurados. La mitad de las empresas estadounidenses utilizan detección y monitorización de amenazas respaldadas por IA para reducir sus primas de ciberseguro.**

Continúe leyendo para comparar sus propias prácticas de seguridad de identidad y estrategias de ciberseguros. Lo que aprenda le ayudará a prepararse para su próxima evaluación de ciberseguro e identificar formas innovadoras de reducir su esfuerzo y sus costes.

47 %

Las infracciones de identidad y privilegios representan el 47 % de los ataques que dan lugar a reclamaciones de seguros

Conclusión principal 1

Las brechas en la seguridad de la identidad son la causa más común de ciberincidentes que tienen como resultado reclamaciones a las aseguradoras.

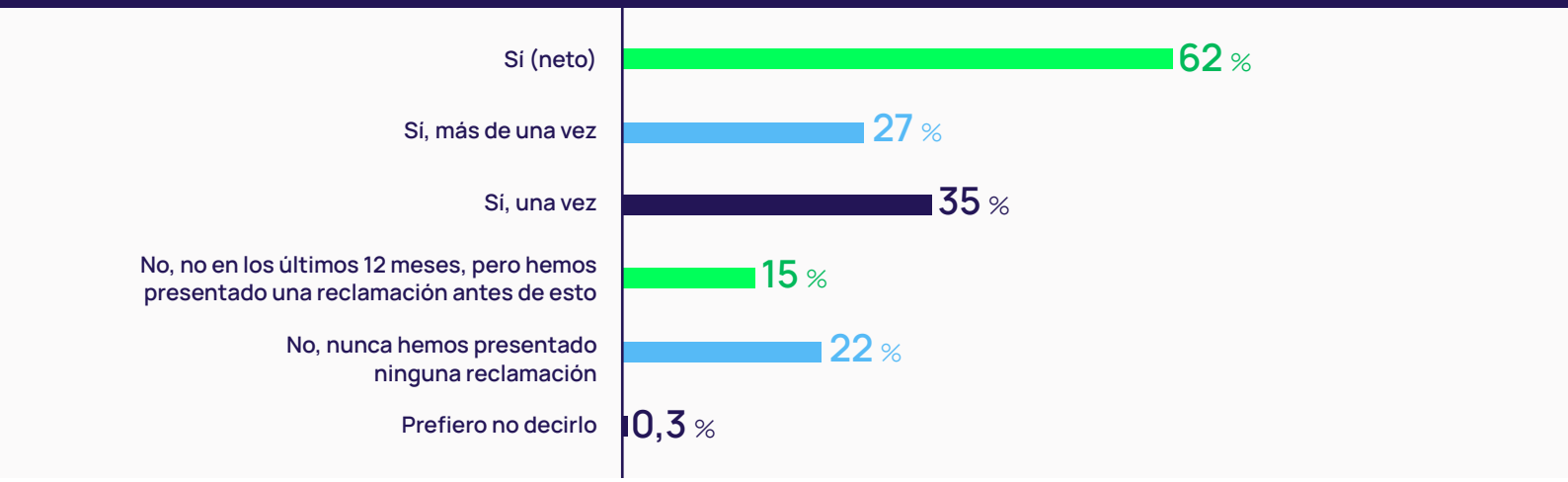
La frecuencia de reclamaciones por ciberseguros sigue siendo alta.

Una vez que las empresas obtienen un ciberseguro, lo utilizan.

Los datos muestran que el 77 % de las empresas con seguro han denunciando algún siniestro anteriormente. Esto coincide con los resultados de la encuesta de 2023 de Delinea, en la que el 79 % de los encuestados afirmó haber utilizado un ciberseguro en el pasado.

Solo en los últimos 12 meses, el 62 % de las empresas presentó una reclamación. Ha sido un año particularmente malo para más del 27 % de las empresas, que presentaron más de una reclamación durante los últimos 12 meses.

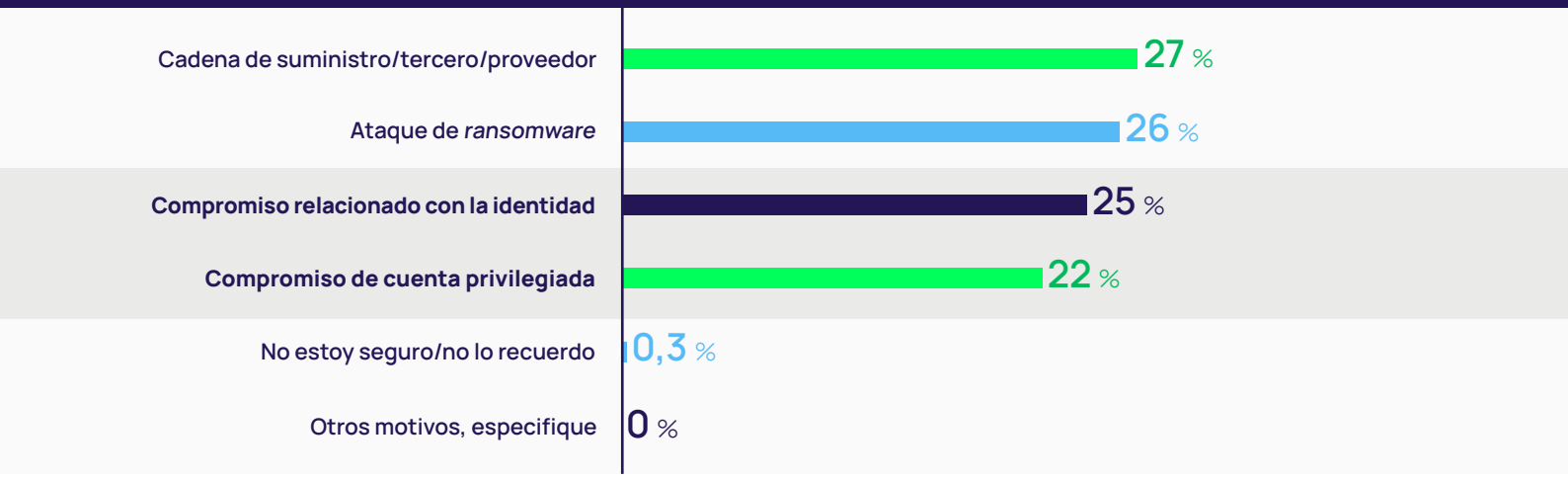
Figura 1 | ¿Ha presentado su organización alguna reclamación a su ciberaseguradora en los últimos 12 meses?



Las técnicas de ataque aprovechan identidades y cuentas privilegiadas.

En conjunto, dos vectores de ataques de identidad, la vulneración de la identidad y la vulneración de cuentas privilegiadas, causan más del 47 % de los ataques que causan reclamaciones a las ciberaseguradoras.

Figura 2 | ¿Qué causó el ciberincidente relacionado con la reclamación a la aseguradora de ciberseguridad?



Hoy en día, la mayoría de los ciberatacantes no necesitan colarse en una empresa: les basta con iniciar sesión. Los ataques relacionados con la identidad generalmente comienzan cuando un atacante utiliza credenciales válidas que ha robado o comprado. Pueden usar esas credenciales para hacerse pasar por una identidad autorizada o utilizar una cuenta privilegiada para poder desbloquear el acceso a recursos protegidos. Dependiendo del nivel de acceso asociado a esa identidad o cuenta privilegiada, el atacante puede descargar malware, manipular datos, apagar sistemas o más, todo lo cual conduce a posibles reclamaciones a las aseguradoras.

Como parte de la cadena de suministro, terceros como subcontratados, proveedores y partners, suelen tener acceso a datos confidenciales y sistemas de TI. Por ejemplo, los equipos de operaciones de TI suelen subcontratar tareas como la resolución de problemas, y los equipos de ingeniería normalmente escalan utilizando desarrolladores externos. Estos usuarios pueden acceder a los recursos utilizando una cuenta privilegiada compartida o una identidad individual. Con demasiada frecuencia, este tipo de usuarios operan sin suficiente supervisión y el acceso permanece activo mucho después de que se completen los proyectos, lo que deja vulnerabilidades que los actores maliciosos aprovecharán, dando lugar a posibles indemnizaciones por parte de las aseguradoras.

El *ransomware* suele comenzar a través de la ingeniería social o el phishing, animando a los usuarios con privilegios locales a hacer clic en un enlace que descarga *malware*. Una vez que logran establecerse, los atacantes puede cifrar datos y exigir un rescate por la clave de cifrado, o extraer datos y amenazar con publicarlos a menos que se pague un rescate.

Las empresas obtienen cobertura de los ciberseguros para respaldar sus requisitos de cumplimiento normativo y garantizar la continuidad del negocio.

Preguntamos a las empresas por qué buscaban cobertura de seguro *en el momento en que lo hicieron*. Los desencadenantes incluyen el cumplimiento de los requisitos regulatorios, directivas de la dirección ejecutiva o del consejo de administración y como reacción a ciberataques recientes, ya sea en su industria o que afecten directamente a su organización.

Los encuestados declaran que los requisitos de cumplimiento normativo constituyen *el principal motivo* para obtener un ciberseguro. Lo importante aquí no es que regulaciones como la PCI, la HIPAA y otros marcos de cumplimiento normativo requieran que las entidades cubiertas cuenten con ciberseguro. Tampoco se trata de que el ciberseguro sea una estrategia eficaz para pagar las multas por incumplimiento normativo, al menos para la mayoría de las empresas; la realidad es que las multas por incumplimiento normativo son el gasto ***menos común*** del que deben hacerse cargo las ciberaseguradoras.

Figura 3A | ¿Cuáles fueron sus principales motivos para solicitar un ciberseguro en el momento en que lo hizo?

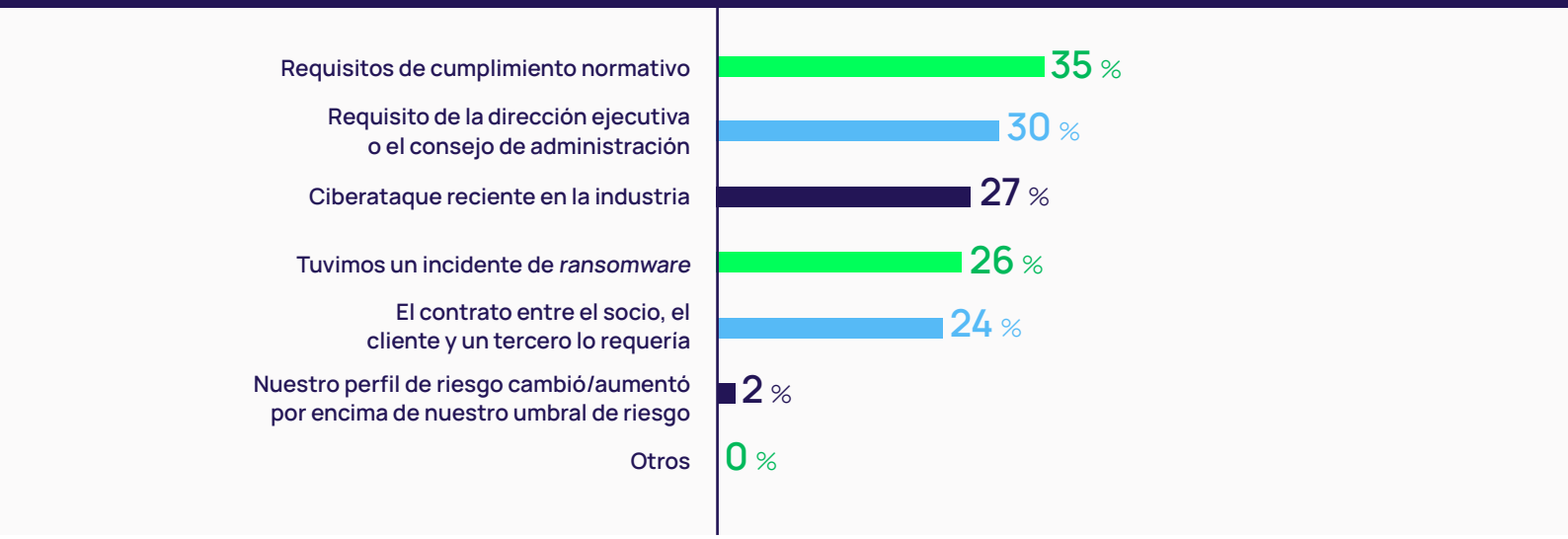
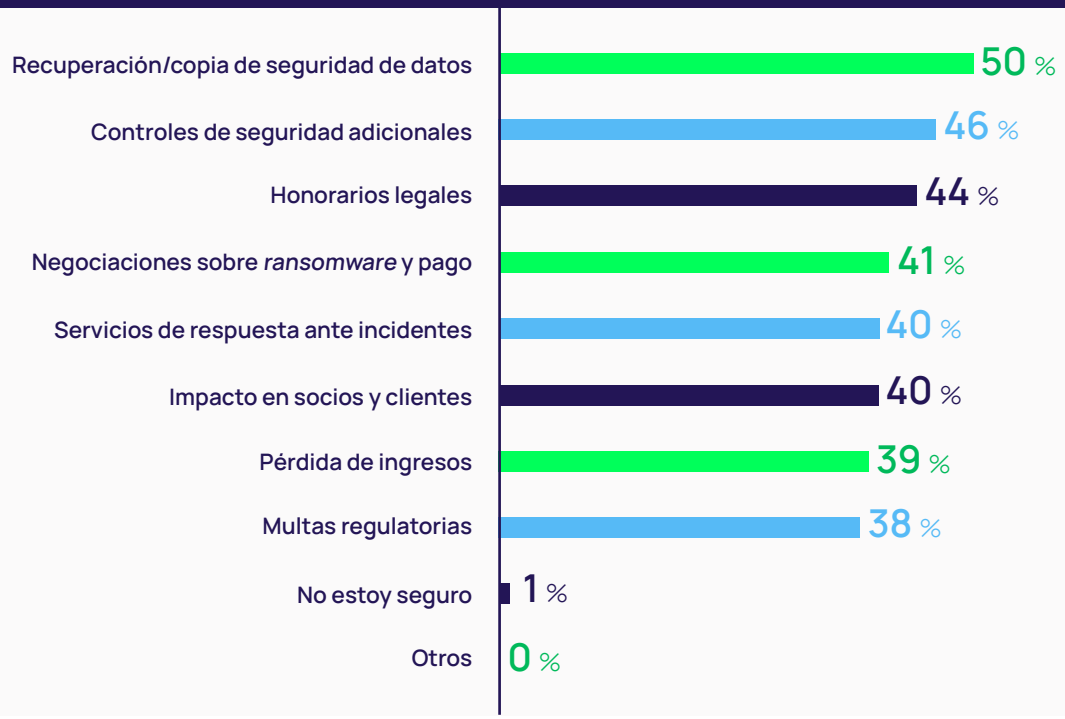


Figura 3 B | ¿Cuánto cubriría su póliza de ciberseguro?



Lo más probable es que las empresas que se rigen por regulaciones industriales se enfrenten a estrictas multas por incumplimiento normativo en materia de protección de datos. La recuperación y la copia de seguridad rápidas pueden ayudar a evitar multas y otros costes asociados con el incumplimiento normativo después de una vulneración de datos porque le permiten recuperar y proteger los datos rápidamente.

Los ciberseguros se centran principalmente en los servicios de recuperación y copia de seguridad de datos porque son esenciales para minimizar el tiempo de inactividad y las pérdidas financieras después de un ciberincidente. Al cubrir estos servicios, las aseguradoras apoyan la recuperación rápida y la resiliencia empresarial, lo que beneficia tanto al asegurado como a la aseguradora.

Tenga en cuenta también que el seguro es una estrategia de gestión de riesgos, no una estrategia de ciberseguridad. Muchas empresas utilizan marcos de cumplimiento normativo o ciberseguridad como NIST para guiar sus programas de seguridad, incluso si no son entidades cubiertas. Estos marcos exigen evidencia de controles de seguridad, al igual que lo harán las aseguradoras, porque se ha demostrado que reducen el riesgo. Si se establecen estos controles, se podrán satisfacer tanto a los reguladores como a las aseguradoras. Incluso si no está sujeto a regulaciones que impliquen posibles multas, no puede omitir esta parte sin más y esperar superar su próxima auditoría o evaluación de seguro.

La mitad de las empresas estadounidenses utilizan la detección y monitorización de amenazas respaldadas por IA para reducir sus primas de ciberseguros

Conclusión principal 2

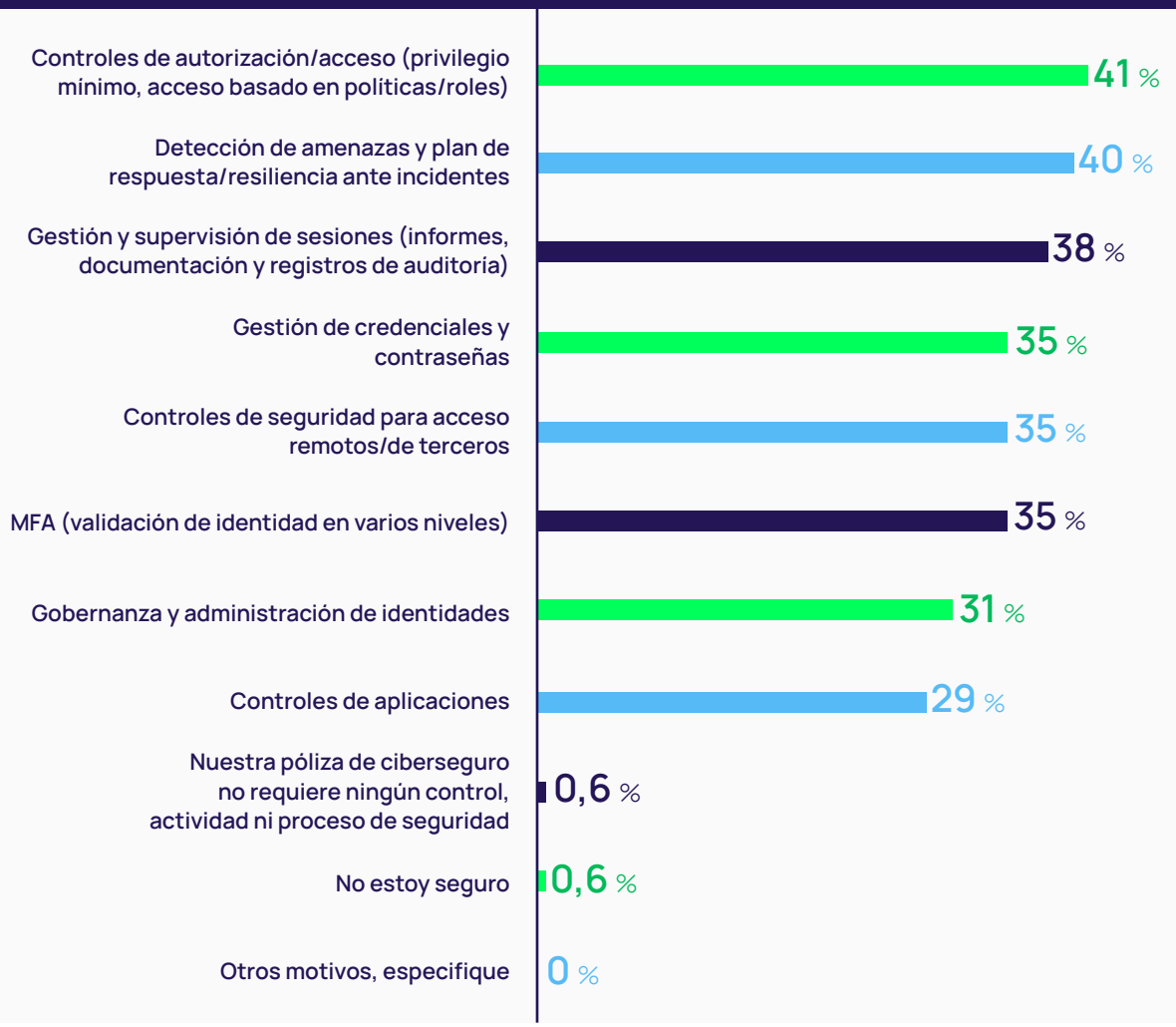
Las aseguradoras exigen pruebas de la seguridad de la identidad antes de conceder pólizas y el 41 % exige controles de autorización.

Las aseguradoras requieren controles, actividades y procesos de seguridad de la identidad.

Ahora que cuentan con más datos históricos que apuntan a la causa de los ciberataques, muchas aseguradoras exigen a los asegurados que minimicen la probabilidad y el impacto de los ciberincidentes, reduciendo así sus posibles pagos por reclamaciones. Casi todos los encuestados tienen algún tipo de requisito de seguridad de identidad exigido por su ciberaseguadora. La mayoría de los encuestados afirman que las pólizas de ciberseguro requieren diversos controles de seguridad de identidad.

Las aseguradoras generalmente exigen que los asegurados establezcan controles relacionados con la autorización/acceso con privilegios mínimos, seguidos de cerca por la detección y respuesta ante amenazas.

Figura 4 | ¿Qué controles, actividades y procesos de seguridad exige su póliza de ciberseguro?



Estos controles se alinean con las mejores prácticas de la industria y los requisitos normativos. Los controles de seguridad eficaces no solo ayudan a prevenir incidentes, sino que también garantizan que las organizaciones puedan responder con rapidez y eficacia, reduciendo el tiempo de inactividad y las pérdidas financieras. Al exigir controles de seguridad integrales, las aseguradoras pueden gestionar y predecir mejor las pérdidas potenciales, lo que se traduce en primas más estables y predecibles para los asegurados.

Definición de los controles de seguridad de identidad necesarios

Controles de acceso/ autorización

Los controles de acceso autorizan a qué sistemas y datos puede acceder una identidad y qué puede hacer con ese acceso. Las empresas normalmente gestionan la autorización a través de políticas como controles de acceso basados en roles o controles de acceso basados en atributos. Las mejores prácticas de privilegios mínimos requieren que las identidades tengan solo los permisos necesarios para realizar sus funciones, solo cuando los necesitan.

Controles de aplicaciones

Los controles de aplicaciones le ayudan a equilibrar las mejores prácticas con menos privilegios y la productividad del usuario. Las aplicaciones fiables se agregan a listas de permitidas para su instalación o ejecución automática, mientras que las aplicaciones maliciosas conocidas (*malware*) se incorporan a listas de denegación y se bloquean. Las aplicaciones desconocidas pueden quedar en un espacio aislado hasta que hayan sido revisadas y aprobadas.

Gestión de credenciales y contraseñas

Las credenciales incluyen nombres de usuario, contraseñas, *tokens* y otros secretos que desbloquean el acceso a sus sistemas y datos. Los ciberatacantes utilizan métodos como el robo de credenciales y el descifrado de contraseñas para robar credenciales. También pueden comprar credenciales a traficantes de accesos en la dark web. Para evitar robos, las credenciales deben ser difíciles de adivinar y estar siempre protegidas. Puede almacenar credenciales en un depósito seguro con cifrado de nivel militar. La gestión continua de credenciales, como la rotación y el vencimiento, garantiza que las credenciales tengan una vida útil limitada.

Gobernanza y administración de identidades (IGA)

IGA controla los permisos de las identidades durante todo su ciclo de vida, incluso cuando los usuarios se unen, se mueven o se van, y permite la supervisión de todas las identidades de su organización (humanas y máquinas), lo que facilita demostrar dicha supervisión a auditores, ciberaseguradoras y organismos de cumplimiento normativo.

Autenticación multifactor (MFA)

La autenticación multifactor valida la identidad humana al requerir que las personas proporcionen algo que tienen (como un código en un teléfono o una huella digital) o algo que saben (como preguntas de seguridad). Las mejores prácticas exigen la validación de la identidad en cada interacción que implique un alto riesgo, incluido el inicio de sesión inicial y la elevación de privilegios.

Controles remotos seguros/de terceros

Estos controles permiten que los empleados remotos y terceros accedan de forma segura a los recursos exactos que necesitan para completar su trabajo, al mismo tiempo que son monitorizados de cerca para una supervisión continua.

Gestión y grabación de sesiones

La gestión de sesiones y la monitorización continua detectan anomalías en las actividades y eventos de identidad, lo que ayuda en la prevención proactiva de incidentes y la respuesta rápida. Los registros de auditoría permiten identificar patrones, lo que resulta útil para predecir riesgos y acelerar el análisis forense posterior al evento. Además, los informes granulares le permiten realizar un seguimiento de las mejoras en su postura de seguridad de identidad, garantizar la responsabilidad y demostrar evidencia de los controles a las ciberaseguradoras.

Detección de amenazas y respuesta ante incidentes

La detección eficaz de amenazas y la respuesta ante incidentes son fundamentales para la resiliencia cibernética y la continuidad del negocio. Los controles incluyen mecanismos para detectar amenazas y un plan de respuesta estructurado para mitigar proactivamente los riesgos y contener y remediar los incidentes en curso. Esto incluye redundancias para garantizar que haya interrupciones mínimas o nulas durante un incidente.

La importancia de la seguridad de la identidad es compartida por expertos en seguridad y ciberseguros

C. J. Dietzman

Vicepresidente sénior de Servicio de Seguros Alliant

Cuando pienso en las expectativas de las aseguradoras y los suscriptores, la seguridad de la identidad se ha convertido en algo fundamental. La forma en que las ciberaseguradoras miden el riesgo se basa en incidentes, leyes y reclamaciones. A medida que realizamos ingeniería inversa de los ciberataques, a menudo encontramos puntos débiles en la gestión de la identidad. «Debe ofrecer un buen relato de los controles integrados y una historia holística sobre cómo mitiga el riesgo de acceso no autorizado y protege las identidades»

La mayor parte de los incidentes de ciberseguridad que han alcanzado el nivel de reclamación tienen su origen en la recopilación de credenciales, la vulneración de información privilegiada, el uso de un tercero que tenía acceso a los sistemas, etc., por lo que cuando se evalúa a las organizaciones para renovaciones, estas son las preguntas que se hacen».

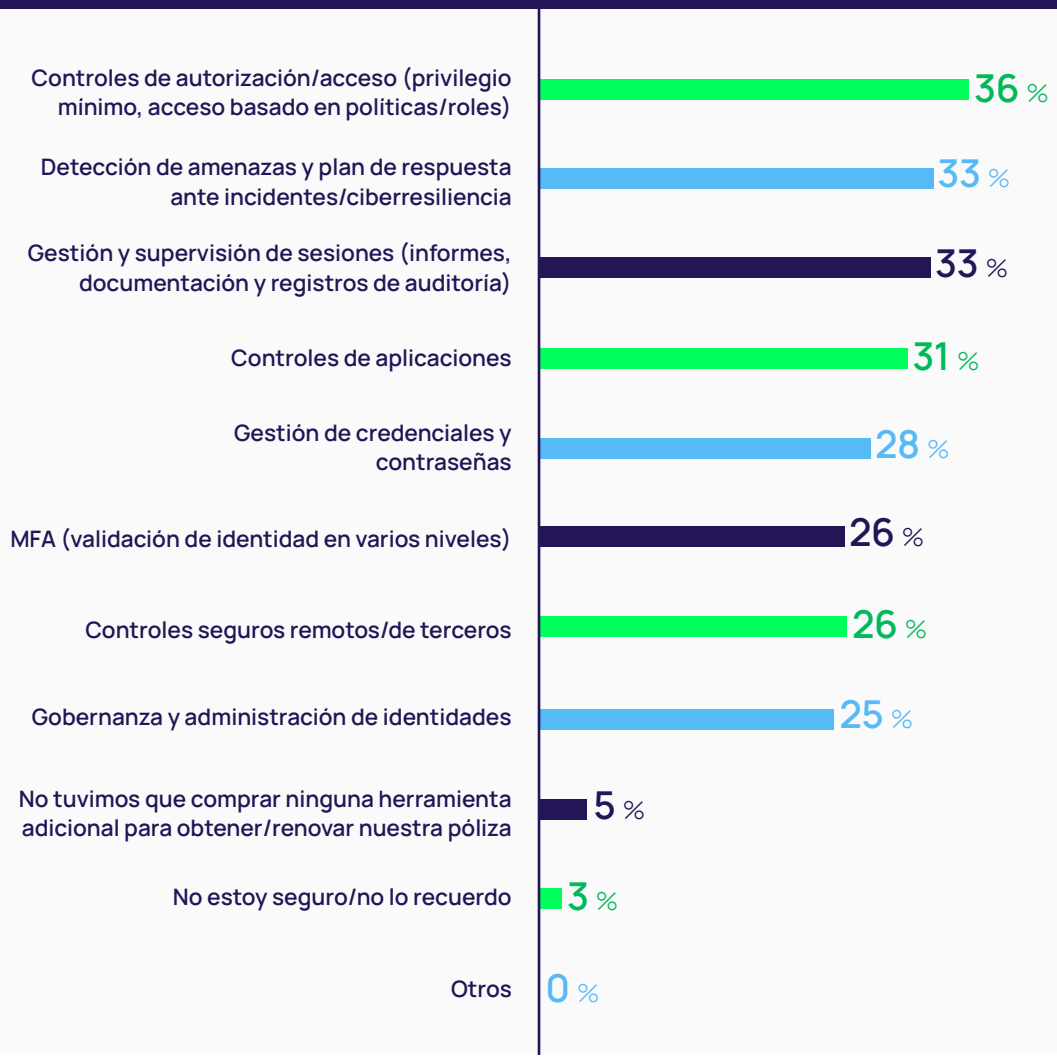
Myrna Soto

Directora ejecutiva de Apogee Executive Advisors y experta en ciberseguridad y gestión de riesgos.

La mayoría de las empresas encuestadas tuvieron que invertir en soluciones de seguridad de identidad antes de obtener o renovar su póliza.

Para satisfacer los requisitos de seguridad mencionados anteriormente, las organizaciones dicen que no pueden simplemente presentar procesos manuales a las potenciales aseguradoras y esperar recibir una póliza. En su lugar, necesitaban comprar soluciones de seguridad de identidad como parte de su conjunto de tecnología de seguridad.

Figura 5 | ¿Qué herramientas adicionales tuvo que adquirir para obtener/renovar su póliza?

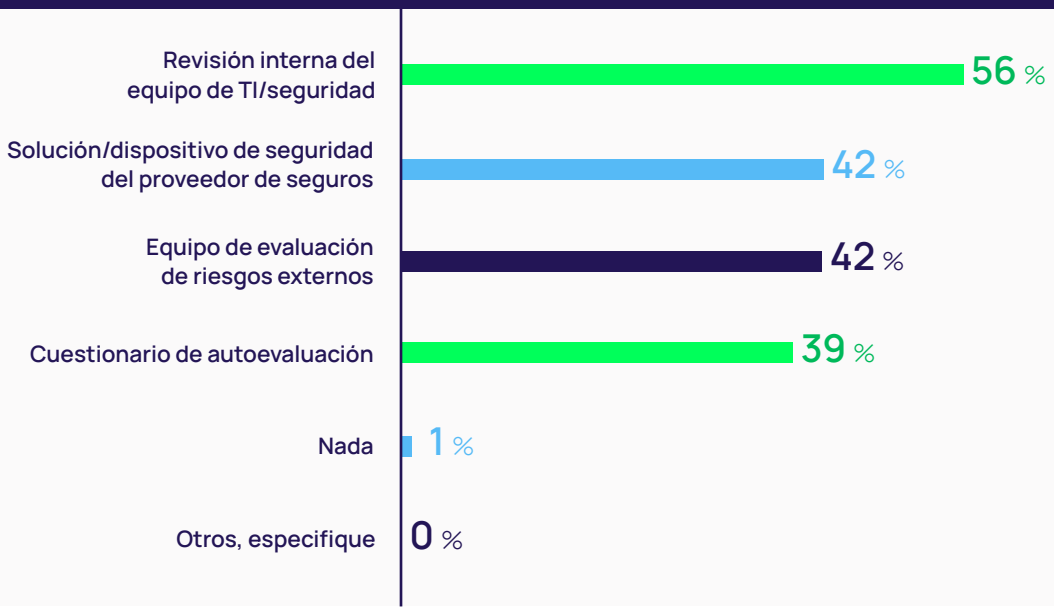


Estos resultados resaltan las diversas necesidades de seguridad de las organizaciones y los diferentes niveles de preparación con respecto a la infraestructura de ciberseguridad.

Las evaluaciones evalúan la postura de seguridad antes de que se otorguen las políticas.

Como reflejo de la creciente madurez de la industria de los ciberseguros, las aseguradoras ahora requieren evaluaciones detalladas de la postura de seguridad. La mayoría de los encuestados optan por realizar estas evaluaciones por su cuenta. Otros incorporan un equipo de evaluación de riesgos de terceros para complementar sus habilidades internas y proporcionar una visión imparcial de la postura de seguridad de una empresa.

Figura 6 | ¿Qué tipos de evaluaciones tuvo que hacer para obtener su póliza de ciberseguro?



Tanto si realiza estas evaluaciones por su cuenta o confía en un tercero, debe contar con que alejen a miembros capacitados del equipo de TI y seguridad de su trabajo diario y de sus proyectos más estratégicos.

41 %

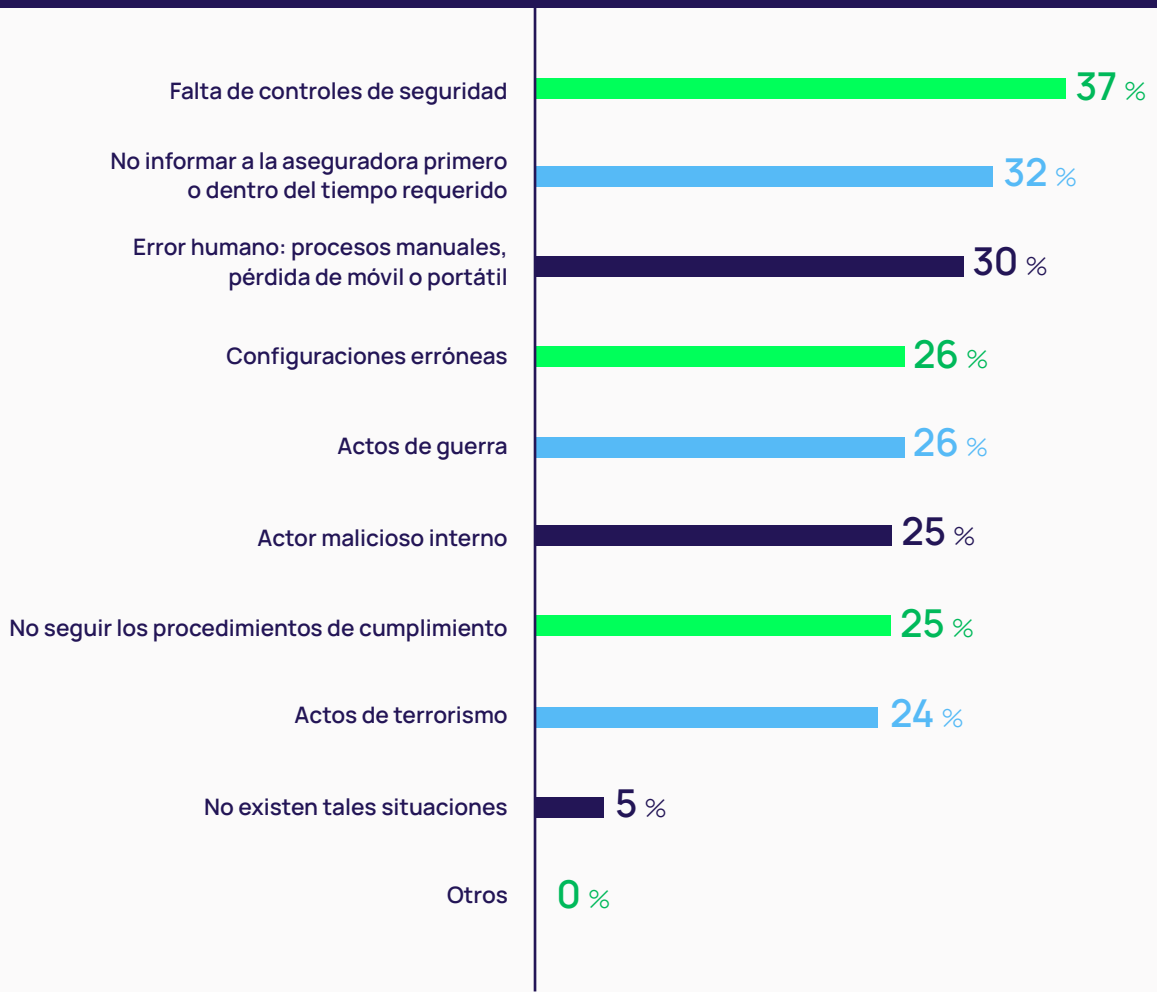
El 41 % de las aseguradoras exigen controles de acceso/autorización con privilegios mínimos antes de conceder una póliza

Los requisitos no terminan después de que se concedan las pólizas. Debe mantener controles de seguridad efectivos si espera que se paguen las reclamaciones.

Buenas noticias: adquirió soluciones de seguridad de identidad, demostró controles y aprobó su evaluación. ¡Su póliza de seguro ha sido concedida!

Sin embargo, los resultados de esta encuesta muestran que si no mantiene esos controles de seguridad y no los utiliza adecuadamente, es probable que su aseguradora rechace futuras reclamaciones. Tal como compartieron los encuestados, debe asegurarse de verificar que los controles de seguridad se apliquen a su organización en constante cambio, estén configurados correctamente y funcionen como se espera.

Figura 7 | ¿En qué situaciones, si las hay, su cobertura de ciberseguro sería nula?



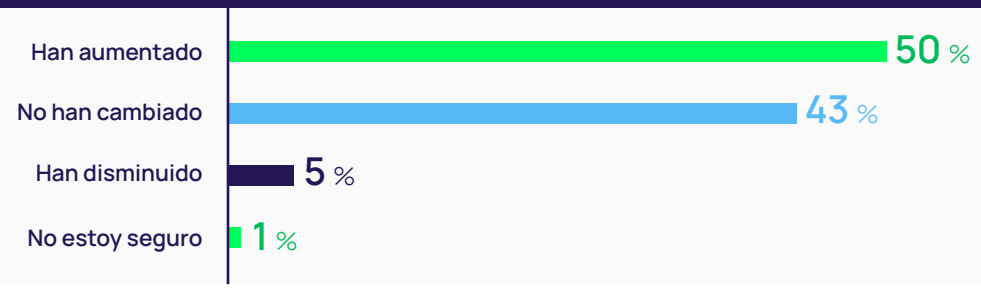
Su postura de seguridad no es «configúrela y olvídese». Su riesgo siempre está cambiando a medida que su entorno de TI se vuelve más complejo y las personas se unen, cambian de roles y abandonan la organización. Lo cierto es que las empresas no siempre siguen las políticas que orgullosamente comparten con un proveedor de seguros en su aplicación.

Conclusión principal 3

Aunque los costes generales del ciberseguro están aumentando, nuevas tecnologías como la IA están reduciendo las primas.

Los costes de los seguros continúan aumentando para muchas organizaciones.

Figura 8 | ¿Cómo han cambiado, si es que han cambiado, los costes de su ciberseguro desde que lo solicitó o desde la última vez que lo renovó?



Aunque más de la mitad informa de aumentos, una comparación interanual muestra que el aumento se está desacelerando. El año pasado, el 79 % de las empresas afirmaron que los costes del seguro aumentaron desde su última solicitud o renovación.

¿A qué se debe el aumento para algunos?

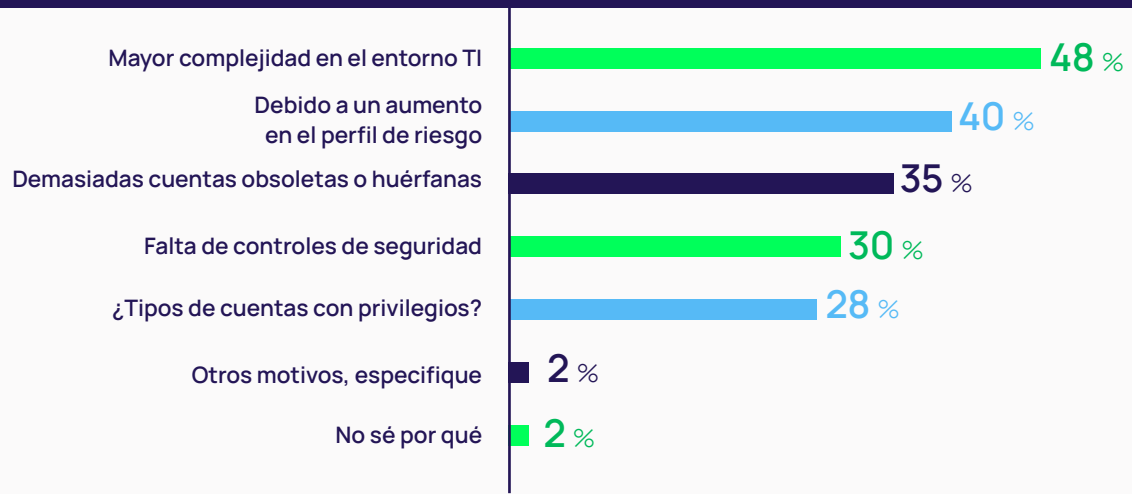
Considere el coste total de los recursos que se necesitan para completar las evaluaciones de seguros, abordar las brechas y demostrar evidencia de una ciberseguridad efectiva en un entorno de TI híbrido y moderno.

Los encuestados señalan la complejidad de las TI como factor determinante del aumento de los costes. A medida que aumenta el número de identidades, se requieren más recursos para realizar estas tareas. La complejidad del entorno de TI hace que las evaluaciones de seguridad de los ciberseguros sean más difíciles de completar. Además, las soluciones de auditoría e informes inconexas dificultan la agregación de los detalles y la medición del riesgo.

El aumento de los costes podría significar que los asegurados soliciten límites de cobertura más altos debido a un mayor perfil de riesgo. Reconocen el impacto comercial que deberán asumir si sufren un ciberataque y desean transferir ese riesgo.

En función de la complejidad del entorno TI y el perfil de riesgo, las aseguradoras pueden aumentar los precios para todos los asegurados a fin de garantizar suficiente liquidez en caso de que se presenten varias reclamaciones a la vez.

Figura 9 | ¿Por qué aumentaron los costes?



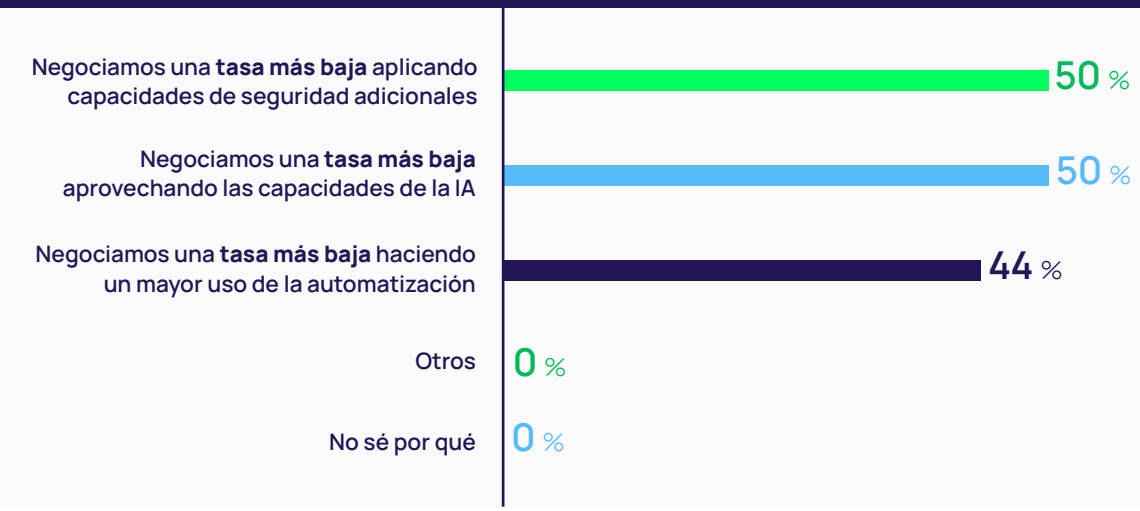
Las soluciones de ciberseguridad que evalúan de forma rápida e integral un entorno de TI complejo y brindan informes basados en riesgos que puede compartir con los proveedores de seguros son medios eficaces para reducir sus costes de ciberseguro.

La inteligencia artificial y los controles de seguridad ayudaron a las empresas con visión de futuro a reducir las tarifas de los seguros.

No todas obtienen la misma tarifa de seguro. Su tarifa se determina en función del riesgo que la aseguradora considere que usted representa, es decir, su perfil de riesgo. En el caso del ciberseguro, su riesgo está influenciado por factores como su ecosistema de tecnologías, sus controles de seguridad y su historial. Si puede demostrar visibilidad y controles que lo conviertan en un riesgo menor, podrá lograr reducir con éxito sus tarifas y, por ende, sus costes.

Los resultados de la encuesta muestran que las empresas con visión de futuro están aprovechando los beneficios de la IA para negociar tarifas más bajas y, por lo tanto, costes. Sin embargo, la mayoría aún necesita centrarse en adoptar y aplicar las bases de una seguridad de la identidad sólida.

Figura 10 | ¿Por qué disminuyeron sus costes de seguro?

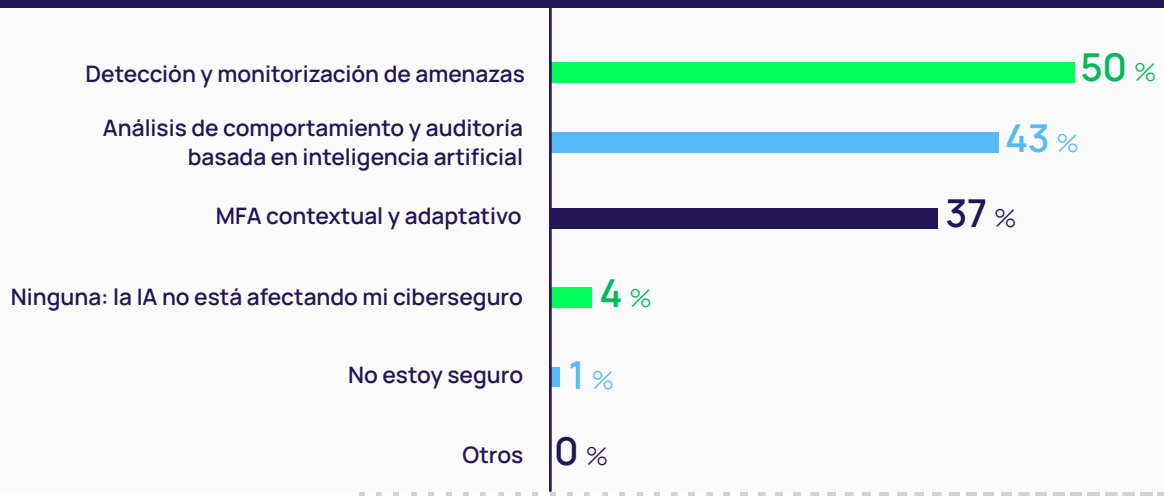


La inteligencia artificial, especialmente para la detección y monitorización de amenazas, es eficaz para reducir las primas de los ciberseguros

Las primas, el importe que paga una empresa para mantener activa una póliza de seguro, están determinadas por el tipo de seguro obtenido, los límites de la póliza y su deducible, entre otros factores. Cuanto más seguro esté de su postura y controles de seguridad, mejor podrá seleccionar el seguro adecuado para usted y negociar primas más bajas.

Las empresas están adoptando inteligencia artificial (IA) para garantizar que las soluciones y políticas de ciberseguridad funcionen como se espera y para contener los incidentes en curso, de modo que puedan reducir el tiempo de permanencia de los agentes de amenaza y el radio de explosión de los ataques, lo que a su vez puede reducir su perfil de riesgo.

Figura 11 | ¿Qué capacidades de IA, si las hay, está adoptando para reducir sus primas de ciberseguro?



Conclusión

La mayoría de las empresas estadounidenses encuestadas tuvieron que invertir en soluciones de seguridad de la identidad antes de obtener una póliza

Si bien el seguro es una herramienta esencial para la resiliencia cibernética, nunca podrá transferir todo tu riesgo. El ciberseguro debe funcionar en conjunto con controles y procesos de ciberseguridad sólidos, razonables y defendibles.

En particular, los proveedores de seguros esperan ver políticas de seguridad de identidad y soluciones efectivas antes de conceder una póliza. Necesitará compartir evidencia de los controles de seguridad de identidad en acción y asegurarse de mantener estos controles a medida que su superficie de ataque cambia y su perfil de riesgo aumenta.

La IA está ayudando a las organizaciones a capturar el conocimiento de expertos en la materia y actuar como «asistente del SOC» para identificar amenazas relacionadas con la identidad más rápidamente, reduciendo en última instancia el tiempo de permanencia, limitando el radio de explosión de un ataque y reduciendo el riesgo. Según los resultados de esta encuesta, la IA está preparada para ofrecer beneficios aún mayores a medida que las empresas negocian pólizas con las aseguradoras.

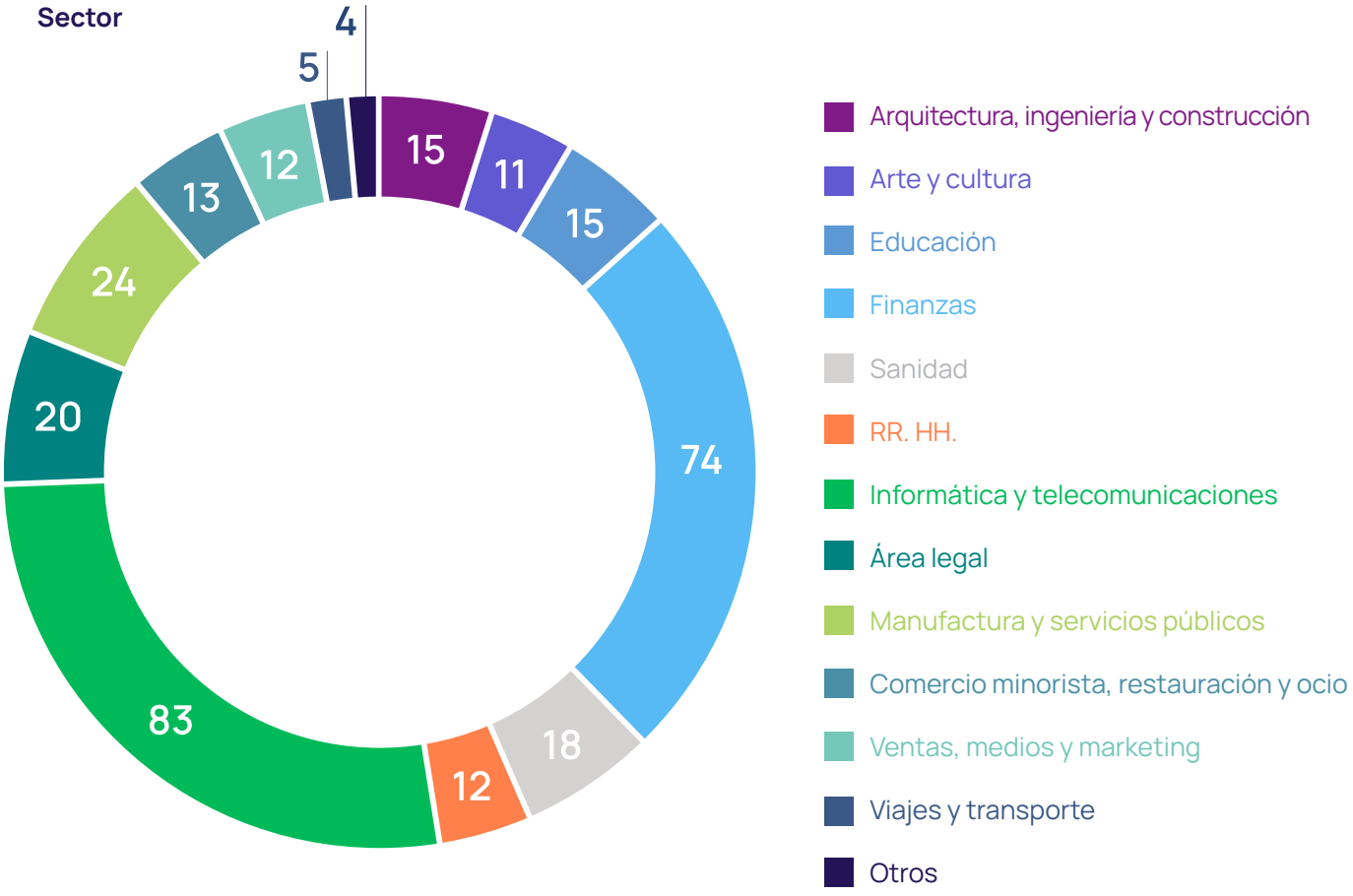
Como parte de sus evaluaciones de riesgos, los suscriptores querrán saber cómo está integrando la IA en sus esfuerzos de transformación digital, incluido el desarrollo de productos, la codificación, el desarrollo, las pruebas de control de calidad, etc. También debe esperar preguntas que examinen cómo su equipo de seguridad utiliza la IA para cuestiones como la gestión de identidad, la autorización, la detección y la respuesta. Cualquier control basado en IA debe ser fácilmente explicable de manera que su equipo, auditores y proveedores de seguros tengan confianza en cómo funcionan para reducir el riesgo.

Metodología

Esta encuesta en línea fue realizada en nombre de Delinea por Censuswide, quien, en junio de 2024, encuestó a 306 líderes con visibilidad del proceso de solicitud o renovación del ciberseguro de su organización. A todos los encuestados se les presentó el mismo conjunto de preguntas y las opciones de respuesta fueron aleatorias. Los resultados no fueron ponderados.

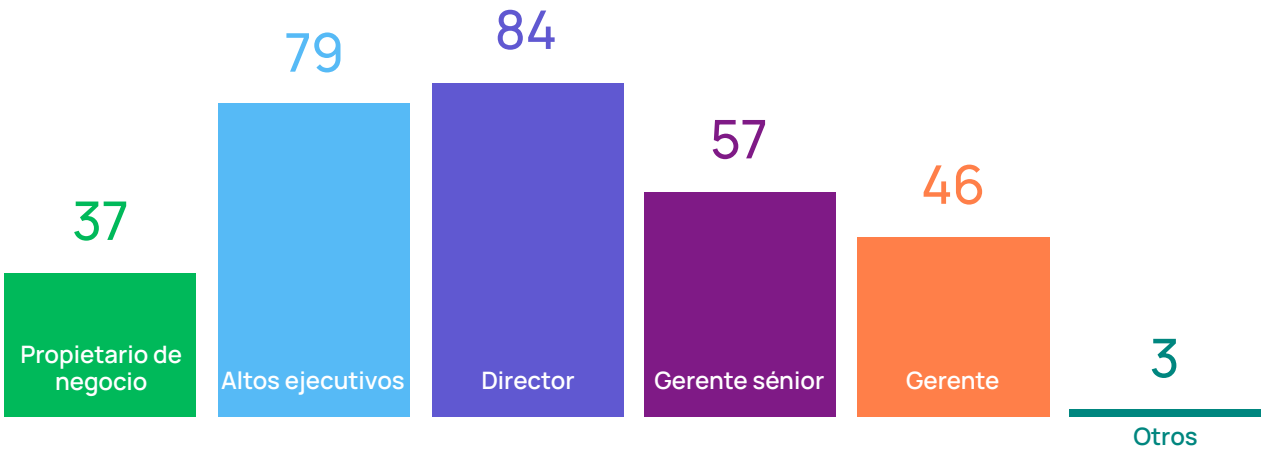
Desglose de 306 encuestados por recuento

Sector

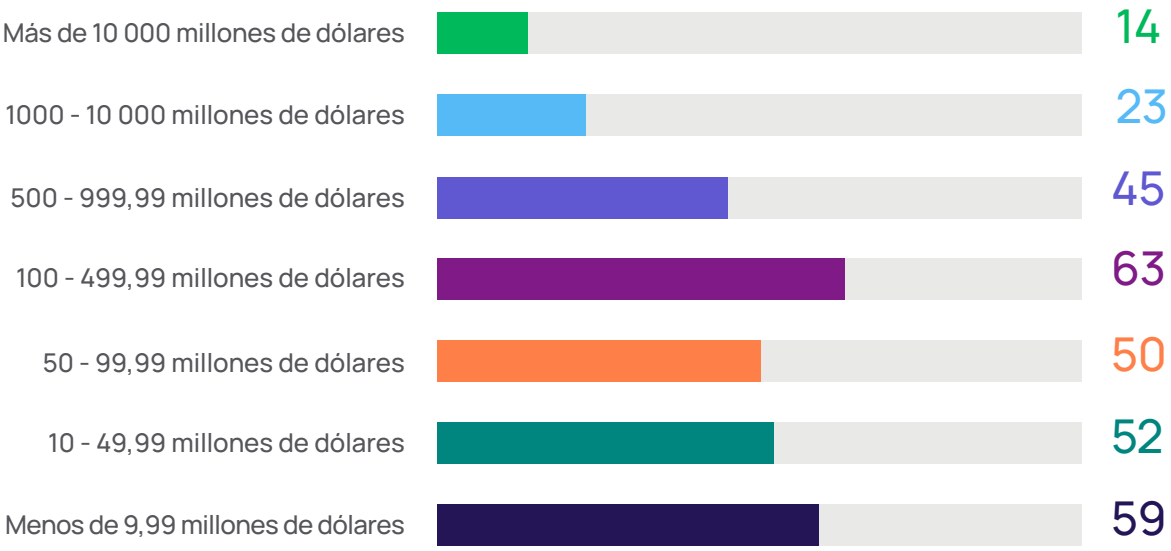


Roles

Cargos



Tamaño de la empresa



Recursos relacionados

SEMINARIO WEB

The Future of Cyber Insurance: Navigating the Impact of AI on Policy Holders

Escuche lo que dicen los expertos en ciberseguridad y seguros sobre cómo evaluar el lenguaje de la póliza para asegurarse de comprender su cobertura, las exclusiones y cómo su proveedor lo apoyará en caso de que ocurra un incidente.

Ver ahora (EN)

DOCUMENTO TÉCNICO

Perspectivas sobre los requisitos reforzados del seguro de ciberseguridad

Este informe reúne cuestionarios de las principales aseguradoras y destaca las preguntas más comunes. En concreto, examina los requisitos cada vez más estrictos de las aseguradoras en materia de seguridad de la identidad, incluida la autenticación multifactor (MFA), la gestión de contraseñas, el control de acceso, la elevación de privilegios, la gestión de sesiones, el mínimo privilegio y las políticas de confianza cero.

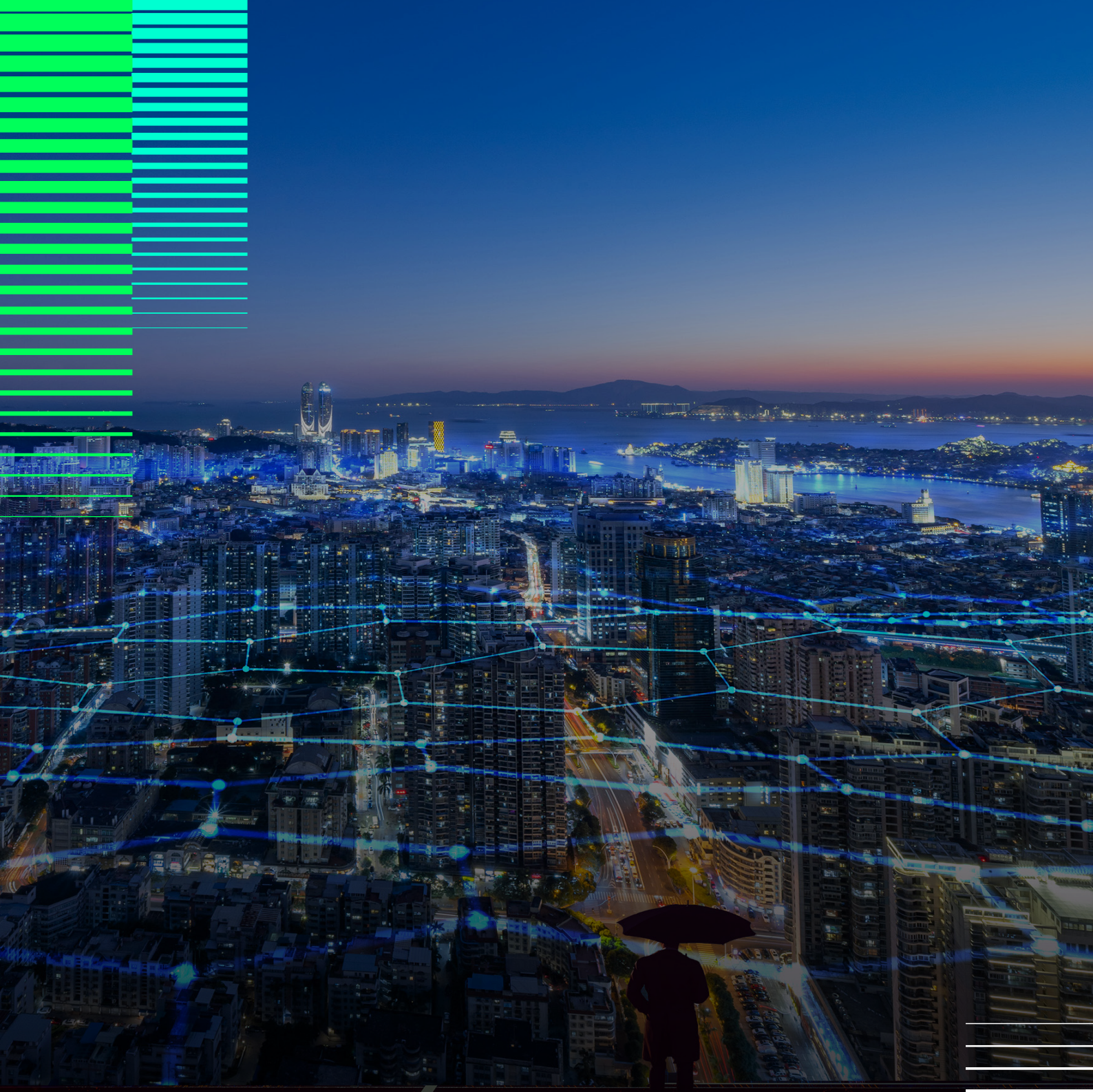
Descargar ahora

PODCAST

Cyber Insurance Trends for Risk Management with Joe Carson of Delinea and Dara Gibson of Optiv

Aprenda a mantener conversaciones sobre ciberseguros con su junta directiva.

Escuchar ahora (EN)



Delinea

Securing identities at every interaction

Delinea es pionera en la protección de identidades a través de la autorización centralizada, haciendo que las organizaciones sean más seguras al controlar sin problemas sus interacciones en toda la empresa moderna. Delinea permite a las organizaciones aplicar el contexto y la inteligencia en todo el ciclo de vida de la identidad a través de la nube y la infraestructura tradicional, los datos y las aplicaciones SaaS para eliminar las amenazas relacionadas con la identidad. Con la autorización inteligente, Delinea proporciona la única plataforma que permite descubrir todas las identidades, asignar niveles de acceso adecuados, detectar irregularidades y responder inmediatamente a las amenazas de identidad en tiempo real. Delinea acelera la adopción por parte de tus equipos al desplegarse en semanas, no en meses, y los hace más productivos al requerir un 90 % menos de recursos para su gestión que el competidor más cercano. Con un tiempo de actividad garantizado del 99,99 %, Delinea Platform es la solución de seguridad de identidad más fiable disponible. Obtenga más información sobre Delinea en **delinea.com/es/**, **LinkedIn**, **X** y **YouTube**.