Preparado para

KEEPER

Más allá de la bóveda:
elevando la gestión de acceso privilegiado en la empresa moderna

Documento técnico de EMA de julio de 2025,
por **Ken Buckler, CASP;** Director de Investigación,
Gestión de seguridad de la información, riesgos y cumplimiento

EMA™
IT & DATA MANAGEMENT RESEARCH, INDUSTRY ANALYSIS & CONSULTING

Tabla de contenidos

Introducción

En una era de amenazas cibernéticas implacables y rápida transformación digital, la gestión del acceso privilegiado (PAM) surgió como una disciplina de seguridad fundamental. Actualmente, las empresas exigen más que el almacenamiento de credenciales; requieren un marco integral que proteja los activos críticos, haga cumplir el acceso de privilegio mínimo y se integre sin problemas en entornos locales y en la nube.

La gestión del acceso privilegiado (PAM) efectiva comienza con una sólida verificación de identidad y autenticación multifactor para combinar tokens de hardware, aprobaciones móviles y verificaciones de biometría respaldadas por el cifrado de extremo a extremo y la seguridad de conocimiento cero. Los controles detallados basados en roles y el aprovisionamiento justo a tiempo dentro de una arquitectura de confianza cero garantizan que los usuarios reciban los privilegios mínimos necesarios, lo que reduce drásticamente el impacto de las violaciones. Simultáneamente, los registros de auditoría capturan cada sesión con privilegios, desde los comandos ejecutados hasta las reproducciones visuales y la duración de la sesión. Luego, los registros de auditoría alimentan motores de cumplimiento automatizados que alinean las prácticas con los estándares HIPAA, SOX y PCI DSS, al tiempo que las campañas de recertificación eliminan las cuentas huérfanas o excesivas.

La integración sin interrupciones con los servicios en la nube y las herramientas existentes es fundamental. La inyección de credenciales en scripts, canales y puertas de enlace de acceso remoto mantiene la productividad del usuario sin comprometer la supervisión. El análisis avanzado del comportamiento y la IA agéntica elevan a PAM a una defensa activa. Las alertas y acciones en tiempo real pueden eliminar amenazas y revocar privilegios de inmediato. Extender estos controles a terceros mediante el uso compartido limitado por tiempo y dispositivo, la rotación automática de contraseñas y los estrictos flujos de trabajo de aprobación mitiga aún más los riesgos de los contratistas y de la cadena de suministro.

En este documento técnico, analizaremos los desafíos a los que se enfrentan las organizaciones para cumplir con estas prioridades de PAM y evaluaremos cómo la plataforma KeeperPAM de Keeper Security se compara con las de la industria en general.

Confianza cero por diseño

Confianza cero y conocimiento cero

Incorporar los principios de confianza cero desde el principio ya no es opcional para la gestión del acceso privilegiado: es imperativo. Un marco de "confianza cero por diseño" trata cada solicitud de privilegios elevados como inherentemente no confiable, lo que requiere una verificación continua, una segmentación estricta y la aplicación del privilegio mínimo. Al cambiar de credenciales estáticas y todopoderosas a tokens de acceso efímeros y contextuales, las organizaciones pueden reducir drásticamente la superficie de ataque y limitar el movimiento lateral en caso de que se produzca una violación. Con un enfoque de confianza cero por diseño, cada decisión de acceso considera la identidad del usuario, la postura del dispositivo, la ubicación, la hora del día y el contexto de comportamiento. El aprovisionamiento justo a tiempo garantiza que los derechos privilegiados se otorguen solo por la duración exacta necesaria y que se revoquen automáticamente después. Los controles de acceso detallados y basados en roles minimizan el exceso de permisos, mientras que la autenticación multifactor y la supervisión continua de sesiones protegen contra el compromiso de credenciales y las amenazas internas.

"[Cuando se trata de la gestión del acceso privilegiado, nuestras prioridades son] la integración con la arquitectura de confianza cero y el marco de validación continua."
- Director de TI, 500-749 empleados, utilizando KeeperPAM

El enfoque de conocimiento cero de Keeper para el diseño de productos mejora aún más este enfoque, lo que garantiza que todo el cifrado y descifrado se realice localmente en su dispositivo; solo el texto cifrado viaja a la nube de Keeper. Una contraseña maestra y el material de claves derivadas nunca salen de un dispositivo elegido, lo que significa que los servidores de Keeper no pueden acceder ni almacenar datos sin cifrar ni las claves que los protegen. Incluso si su infraestructura fuera violada, los atacantes solo obtendrían una cadena ilegible de caracteres, lo que garantiza que existe una verdadera confidencialidad de extremo a extremo.

Los datos de la encuesta subrayan el impacto de este enfoque: el 60 % de los usuarios de Keeper Security consideran su implementación de PAM como "conocimiento cero" y "confianza cero por diseño", en comparación con solo el 34.9 % de los usuarios de todos los demás proveedores. Esta diferencia refleja una postura de seguridad proactiva: los clientes de Keeper hacen hincapié en la validación continua, la eliminación de cuentas compartidas y la gestión automatizada del ciclo de vida de los privilegios, frente a una mentalidad más reactiva e impulsada por el cumplimiento en otros lugares.

El PAM de confianza cero también acelera el cumplimiento y la preparación para auditorías. Cada sesión con privilegios se registra de extremo a extremo, completa con comandos ejecutados, reproducción visual y métricas de duración, lo que alimenta motores de cumplimiento automatizados que se alinean con los requisitos de HIPAA, SOX y PCI DSS. En la práctica, las organizaciones que integran la confianza cero en sus arquitecturas de PAM no solo fortalecen sus defensas, sino que también optimizan las operaciones, reducen los costos asociados con las cuentas huérfanas y demuestran mejoras medibles en la contención de violaciones.

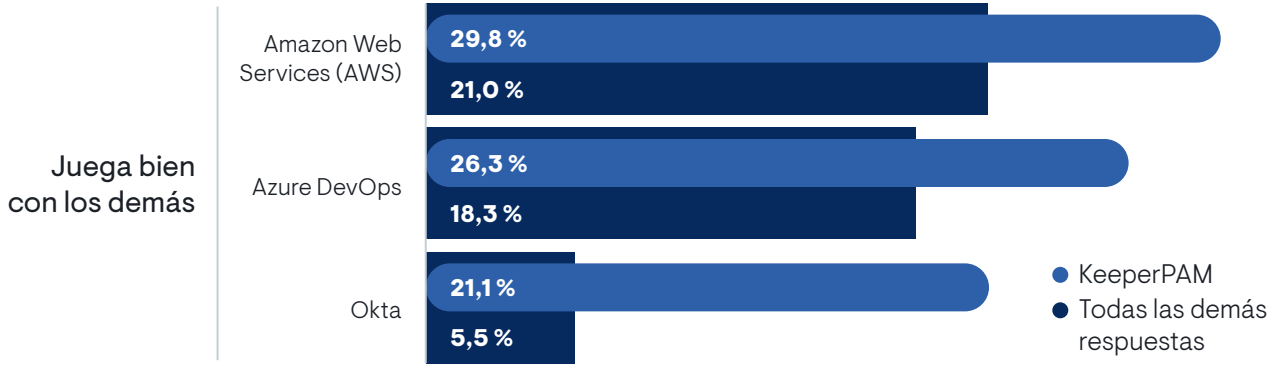
En última instancia, el enfoque de conocimiento cero y el diseño de confianza cero de Keeper transforman el acceso privilegiado de una posible responsabilidad en un proceso controlado y verificable, que se adapta en tiempo real a los riesgos cambiantes y garantiza que los sistemas críticos permanezcan seguros, conformes y resilientes.

Facilidad de implementación, configuración e integraciones

No existe un “botón fácil”, pero Keeper se acerca bastante

La facilidad de implementación, configuración e integración puede determinar el éxito o el fracaso del ROI de un proyecto de PAM. Según la encuesta de EMA, el 60 % de los clientes de Keeper Security calificaron la implementación inicial como “muy sencilla”, en comparación con solo el 22.1 % de los usuarios de otras plataformas de PAM. Por el contrario, el 10 % de los clientes de todas las otras soluciones calificaron la implementación como “algo difícil” o “muy difícil”, un punto débil totalmente ausente entre los usuarios de KeeperPAM. La migración de herramientas de PAM heredadas y locales a la nube sigue siendo un obstáculo para el 39 % de las organizaciones, una complejidad que la arquitectura nativa en la nube de Keeper elude. Los obstáculos de la integración afectan al 11 % de las implementaciones que no son de Keeper, en las que suelen requerirse conectores patentados y scripts manuales para integrarse en los canales de SIEM, emisión de tickets o DevOps. Las API modulares de KeeperPAM, los conectores plug-and-play y la perfecta orquestación en la nube aceleran el tiempo de obtención de valor y minimizan los problemas operativos.

Juega bien con los demás



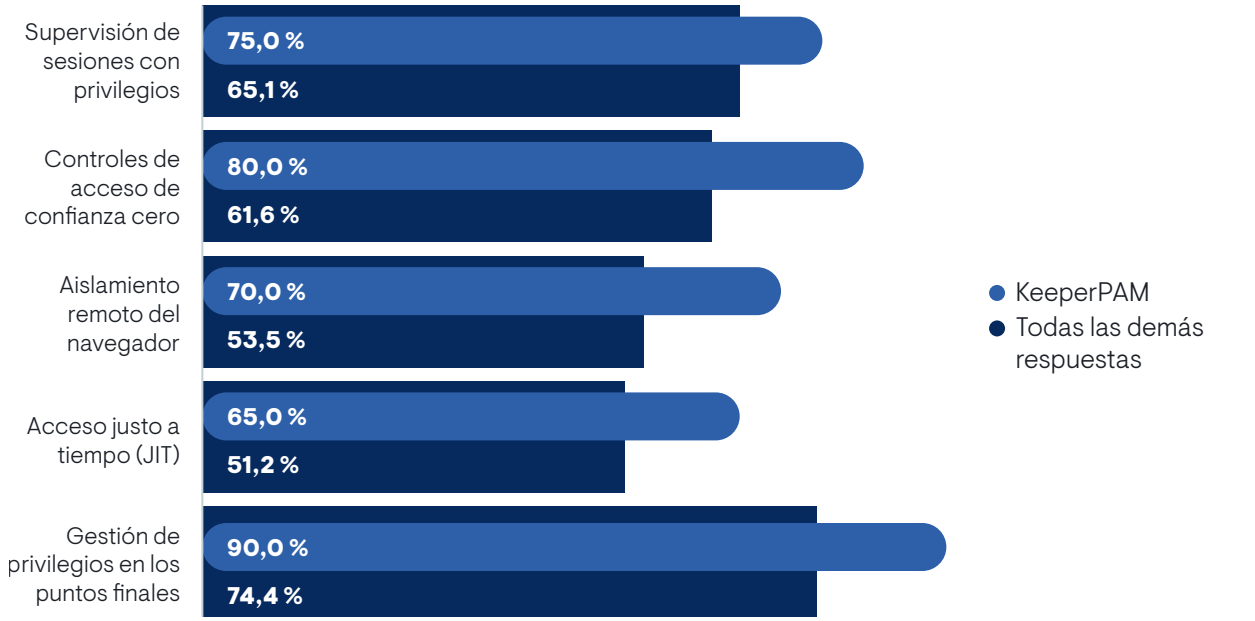
Las integraciones perfectas son una piedra angular de cualquier estrategia de PAM moderna, y Keeper también lidera en este aspecto. Los conectores listos para usar y las API permiten una integración rápida y bidireccional con las plataformas principales, ya sea que usted esté activando instancias de EC2 en Amazon Web Services, automatizando canales en Azure DevOps o centralizando la autenticación a través de Okta. Los usuarios de KeeperPAM informan de una adopción mucho mayor de estas integraciones en comparación con otras soluciones de PAM, lo que elimina la necesidad de realizar secuencias de comandos personalizadas o de mantenimiento manual de los conectores que consumen mucho tiempo. Al integrar la inyección de credenciales privilegiadas directamente en sus flujos de trabajo de CI/CD, consolas en la nube y proveedores de identidad, KeeperPAM minimiza la fricción, impulsa la productividad de los desarrolladores y asegura que los secretos permanezcan protegidos en cada capa.

Hacer Más con Menos Personal

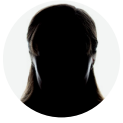
Los requisitos de personal para las implementaciones de PAM varían ampliamente según la plataforma. Solo el 15 % de los clientes de Keeper Security informan que necesitan personal específico para administrar la implementación, la configuración y la integración, gracias a la interfaz de usuario intuitiva de Keeper, a los asistentes de configuración guiada y a la documentación completa. Por el contrario, el 39.5 % de las organizaciones que utilizan otras soluciones de PAM requieren uno o más administradores a tiempo completo para mantener sus entornos en funcionamiento. Esos equipos suelen gestionar el mantenimiento complejo de dispositivos locales, la creación de scripts personalizados y las actualizaciones manuales de conectores, lo que incrementa el personal y agota los recursos de TI existentes. El diseño nativo de la nube de Keeper y las herramientas de autoservicio minimizan la dependencia de habilidades especializadas. Los administradores pueden incorporar nuevos sistemas, ajustar las políticas de privilegios e integrarse con canales de SIEM o DevOps, sin necesidad de hacer una gran personalización. En última instancia, una menor sobrecarga de personal se traduce en implementaciones más rápidas y operaciones a largo plazo más sostenibles y asequibles.

Más allá de la gestión de contraseñas y secretos

Capacidades avanzadas de PAM



La PAM moderna exige mucho más que almacenar credenciales: requiere un amplio conjunto de funciones que defienda, monitoree y se adapte activamente a las amenazas en evolución. KeeperPAM se destaca por ofrecer capacidades avanzadas que muchos proveedores heredados simplemente no ofrecen ni implementan a escala. La supervisión de sesiones con privilegios, por ejemplo, es crucial para capturar cada pulsación de tecla, comando y reproducción visual de actividades de alto riesgo. Los clientes de Keeper utilizan esta función con más frecuencia que sus pares, lo que permite la detección de amenazas en tiempo real y el análisis forense.



"El uso de PAM fortalece la integridad de nuestros datos y nuestra reputación."
- Vicepresidente de Desarrollo/Ingeniería, 1,000-2,499 empleados, usando KeeperPAM

El acceso a la red de confianza cero extiende los principios del privilegio mínimo más allá de las contraseñas para cada solicitud de acceso. Keeper incorpora verificaciones de políticas contextuales —postura del dispositivo, ubicación, hora y referencias de comportamiento—, lo que garantiza que incluso las sesiones autenticadas permanezcan bajo escrutinio continuo. Este control detallado de las operaciones con privilegios reduce significativamente la posible ventana de exposición en comparación con los modelos estáticos de todo o nada.

El aislamiento remoto del navegador (RBI) es otra área en la que Keeper supera a sus competidores. Las organizaciones que utilizan proxies para las consolas administrativas a través de navegadores aislados y seguros eliminan el acceso directo a los puntos finales para terceros y contratistas, lo que pone en cuarentena de manera efectiva el malware potencial o el robo de credenciales. Pocas otras soluciones de PAM integran RBI de manera tan fluida, en lugar de obligar a llevar a cabo soluciones manuales que socavan tanto la seguridad como la experiencia del usuario.

El aprovisionamiento justo a tiempo y la gestión automatizada del ciclo de vida de los privilegios completan el conjunto de herramientas avanzadas de Keeper. La elevación temporal y limitada en el tiempo evita que las cuentas permanentes con altos privilegios se acumulen, mientras que las campañas automáticas de desaprovisionamiento y recertificación aseguran la observancia a los mandatos de cumplimiento sin sobrecarga manual. Finalmente, la gestión de privilegios en los puntos finales —eliminar los derechos del administrador local mientras se otorgan privilegios delimitados a pedido— protege tanto contra ataques externos como contra el uso indebido interno.

Al mirar más allá de las contraseñas y los secretos, Keeper transforma la PAM en una plataforma de defensa activa: una que anticipa ataques, aplica confianza cero en cada capa y ofrece los controles avanzados que los entornos complejos de hoy exigen.

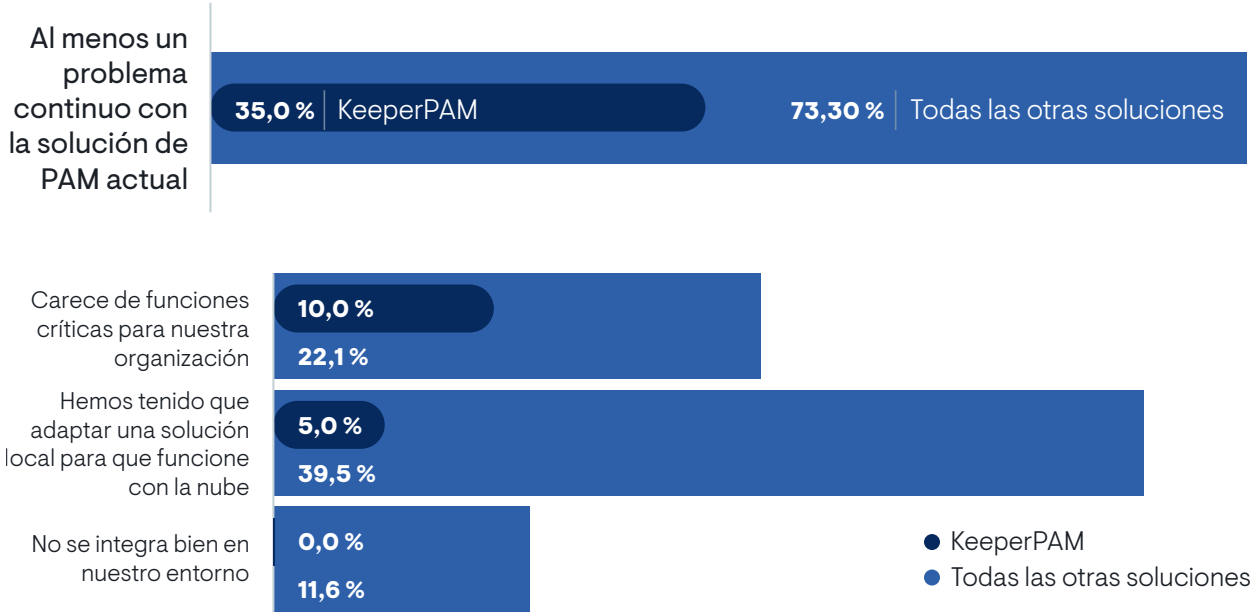
Satisfacción general

¿Su solución de PAM capea la tormenta?

La satisfacción del cliente es el barómetro definitivo del valor y la longevidad de una solución de PAM. Cuando el 5 % de las organizaciones que utilizan otras plataformas están buscando activamente un reemplazo, esto indica que hay diferencias críticas en la confiabilidad, la facilidad de uso o el soporte técnico. Por el contrario, ningún usuario de Keeper Security informó tener planes de abandonar su herramienta de PAM, lo que subraya la capacidad de Keeper para satisfacer las necesidades de seguridad y operativas en evolución.

Además, el 75 % de los clientes de Keeper dicen estar “muy satisfechos” en general, lo que supera con creces la calificación del 53.5 % de “muy satisfechos” entre los usuarios de proveedores de la competencia. La alta satisfacción se correlaciona con una adopción más rápida, una reducción de riesgos más efectiva y un menor costo total de propiedad, ya que los equipos satisfechos invierten en integraciones más profundas y funciones más avanzadas. En un entorno donde se ataca continuamente al acceso privilegiado, elegir una plataforma que deleite a sus usuarios no solo es un lujo, sino que es esencial.

Las funciones e integraciones son puntos problemáticos críticos



A pesar de su papel crítico, muchas implementaciones de PAM enfrentan obstáculos persistentes. El 73 % de las organizaciones que utilizan soluciones distintas de Keeper informan de al menos un problema significativo, en comparación con solo el 35 % de los clientes de Keeper. Los problemas críticos comunes incluyen la falta de capacidades esenciales, lo que obliga a los equipos a sumar herramientas de terceros, una integración deficiente en la infraestructura existente y el dolor de cabeza de adaptar las plataformas locales para admitir entornos en la nube. Los usuarios de KeeperPAM sufren estos problemas con mucha menos frecuencia, gracias a su completo conjunto de funciones, arquitectura nativa pensada para la nube y una extensa biblioteca de conectores. Al minimizar las diferencias en la funcionalidad y simplificar las implementaciones híbridas, Keeper no solo acelera el tiempo de creación de valor, sino que también reduce la carga de la resolución de problemas y las soluciones alternativas, lo que permite liberar a los equipos de seguridad para que se centren en la mitigación proactiva de riesgos, en lugar de combatir las limitaciones heredadas.

Mejor solución, mejores prioridades

Otras implementaciones de PAM no están a la altura de su potencial

Priority Area	Keeper Customers	Other PAM Solutions
Área prioritaria	Clientes de Keeper	Otras soluciones de PAM
Autenticación	Confianza cero continua	Basado en roles, MFA
Gestión de credenciales	Elimine las credenciales estáticas o compartidas	Control básico y monitoreo de acceso
Capacitación	Prioridad explícita	No enfatizado
Automatización	Enfoque en la mitigación de riesgos (porque el	Minimum regulatory compliance
el proceso ya es eficiente)	Enfoque en la eficiencia de los procesos	
Cumplimiento	Uso indebido de credenciales y enfoque de auditoría	Cumplimiento mínimo de las normativas

Keeper Security permite a las organizaciones pasar de un modo de mantenimiento impulsado por el cumplimiento a una postura proactiva que prioriza la seguridad. Los clientes de KeeperPAM eliminan las credenciales estáticas y compartidas de forma insegura a través de un motor de bóveda de conocimiento cero que emite secretos efímeros y de privilegios mínimos, lo que reduce significativamente tanto los vectores de ataque externos como el abuso interno, en comparación con los enfoques tradicionales en los que solo se cuenta con la bóveda. La autenticación continua y los controles de acceso de confianza cero, incluidas las verificaciones del estado del dispositivo, la geolocalización y el análisis de comportamiento, garantizan que cada sesión permanezca bajo escrutinio mucho después de un aviso único de MFA, lo que hace prácticamente imposible que los atacantes usen las credenciales robadas sin ser detectados. La automatización centrada en el riesgo de Keeper aborda todo el ciclo de vida de los

privilegios, desde el descubrimiento y la incorporación hasta la rotación y el desaprovisionamiento automáticos, lo que evita la proliferación de credenciales y de cuentas huérfanas, mientras que muchas otras soluciones solo automatizan los flujos de trabajo de aprobación o los informes de cumplimiento. Es importante destacar quve los clientes de Keeper integran explícitamente la capacitación y la concientización del personal como un control de seguridad central, reconociendo que los factores humanos son tan esenciales como la tecnología para fomentar la adopción y prevenir soluciones arriesgadas.

"Creo que el monitoreo constante de las cuentas privilegiadas me ayuda a dormir mejor por la noche."
– Vicepresidente de Desarrollo/Ingeniería, 2,500-4,999 empleados, usando KeeperPAM

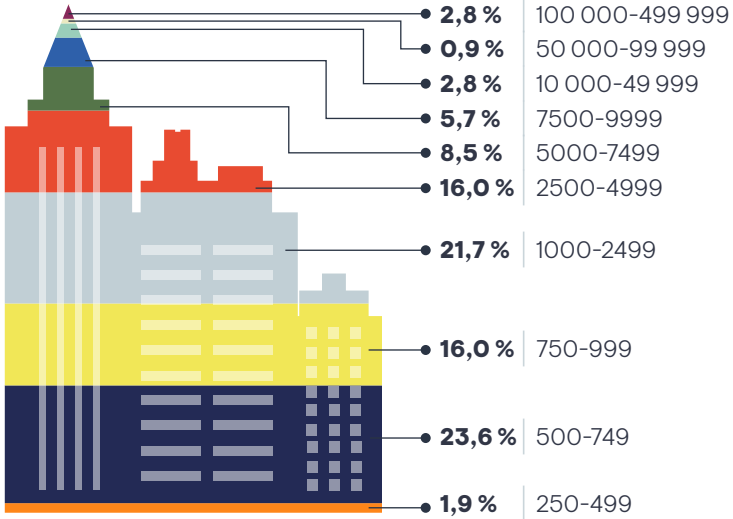
Por el contrario, los usuarios de otras herramientas de PAM suelen hacer hincapié en los controles tradicionales, como el acceso basado en roles, la auditoría posterior al acceso y la eficiencia operativa, lo que refleja una mentalidad reactiva que se enfrenta a diferencias en las funciones, las integraciones frágiles y la complejidad de adaptar soluciones locales para la nube. La arquitectura nativa de la nube de Keeper y su extensa biblioteca de conectores plug-and-play eliminan estos inconvenientes y permite llevar a cabo una rápida integración con plataformas SIEM, proveedores de identidad como Okta y canales de CI/CD en AWS o Azure DevOps. Las capacidades avanzadas, que incluyen la supervisión de sesiones con privilegios, el aislamiento remoto del navegador, el aprovisionamiento justo a tiempo y la gestión de privilegios en los puntos finales, son nativas de Keeper, lo que reduce la fricción en la implementación y las demandas continuas de personal.

Al combinar estas funciones de próxima generación con una experiencia de usuario perfecta, Keeper prepara a los equipos de seguridad para anticipar amenazas, aplicar una protección continua y verdaderamente fortalecer su entorno de acceso privilegiado.

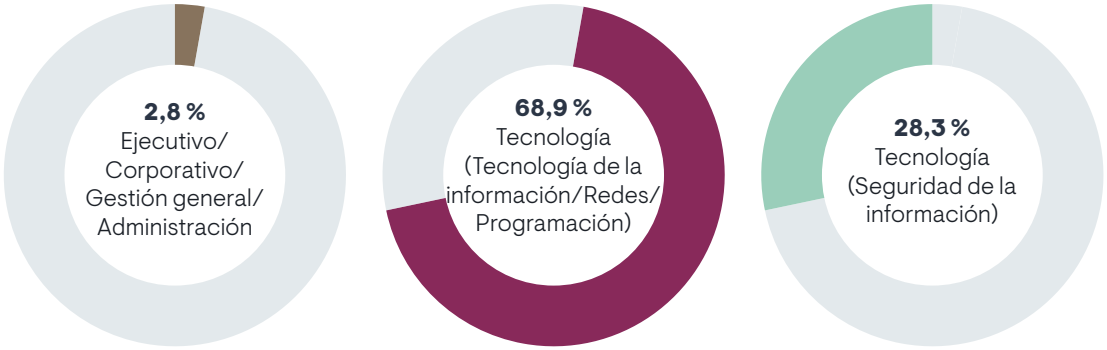
Metodología

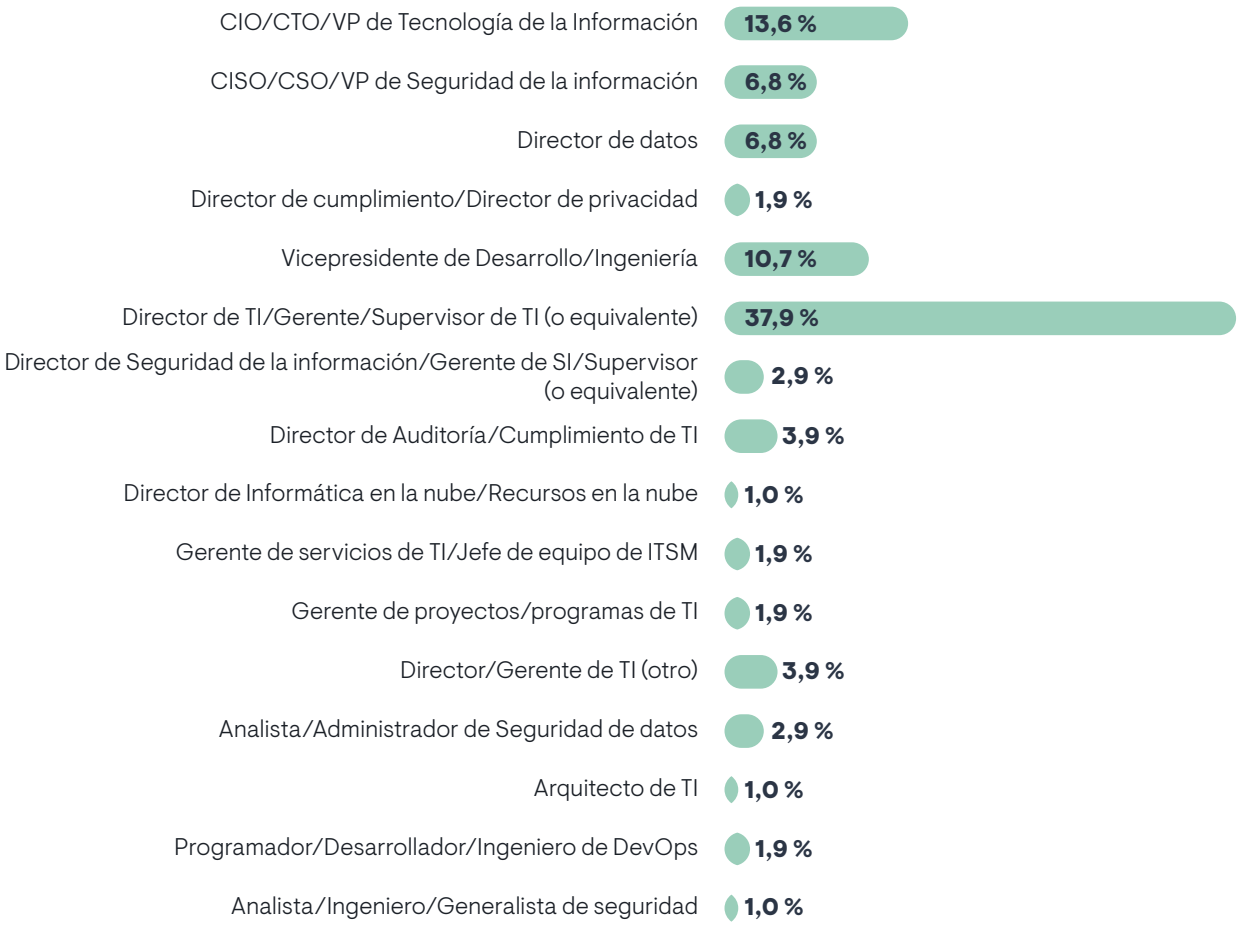
Un total de 106 profesionales que utilizan BeyondTrust, CyberArk, Delinea, Devolutions, Keeper Security, ManageEngine, One Identity o StrongDM a partir de junio de 2025. Todos los datos de este documento técnico se basan en las respuestas de la encuesta y en las respuestas abiertas sobre las prioridades y los desafíos de la gestión del acceso privilegiado en la empresa.

Tamaño de la organización



Rol del encuestado




CIO/CTO/VP de Tecnología de la Información
13,6 %
CISO/CSO/VP de Seguridad de la información
6,8 %
Director de datos
6,8 %
Director de cumplimiento/Director de privacidad
1,9 %
Vicepresidente de Desarrollo/Ingeniería
10,7 %
Director de TI/Gerente/Supervisor de TI (o equivalente)
37,9 %
Director de Seguridad de la información/Gerente de SI/Supervisor (o equivalente)
2,9 %
Director de Auditoría/Cumplimiento de TI
3,9 %
Director de Informática en la nube/Recursos en la nube
1,0 %
Gerente de servicios de TI/Jefe de equipo de ITSM
1,9 %
Gerente de proyectos/programas de TI
1,9 %
Director/Gerente de TI (otro)
3,9 %
Analista/Administrador de Seguridad de datos
2,9 %
Arquitecto de TI
1,0 %
Programador/Desarrollador/Ingeniero de DevOps
1,9 %
Analista/Ingeniero/Generalista de seguridad
1,0 %

Industria


Aeroespacial/Defensa 3,8 %
Automotriz 6,6 %
Servicios empresariales/Consultoría 1,9 %
Hardware de computadoras/Tecnología (dispositivos, chips, hardware de computadoras/redes) 2,8 %
Software de computación/tecnología (aplicación móvil, consumidor, personalizado, basado en la web) 11,3 %
Servicios de informática/tecnología (IaaS, SaaS, MSP, MSSP, proveedor de nube) 7,5 %
Informática/Tecnología: Otros 1,9 %
Educación (federal, estatal y local) 0,9 %
Finanzas/Servicios financieros/Banca/Cripto 3,8 %
Gobierno (federal, estatal y local) 1,9 %
Atención sanitaria/médica/farmacéutica 12,3 %
Fabricación 11,3 %
Sin ánimo de lucro/Sin fines de lucro 0,9 %
Petróleo/Gas/Productos químicos 1,9 %
Servicios profesionales (no técnicos) 1,9 %
Minorista/Mayorista/Distribución 6,6 %
Transporte/Líneas aéreas/Transporte en camiones/Ferrocarril 4,7 %
Viajes/Hospitalidad/Recreación 5,7 %
Servicios públicos/Energía 12,3 %

About Enterprise Management Associates, Inc.

Founded in 1996, Enterprise Management Associates (EMA) is a leading IT research and consulting firm dedicated to delivering actionable insights across the evolving technology landscape. Through independent research, market analysis, and vendor evaluations, we empower organizations to make well-informed technology decisions. Our team of analysts combines practical experience with a deep understanding of industry best practices and emerging vendor solutions to help clients achieve their strategic objectives. Learn more about EMA research, analysis, and consulting services at **www.enterprisemanagement.com** or follow EMA on **X** or **LinkedIn**.

2770 Arapahoe Road, Ste 132 - 544, Lafayette, CO 80026 +1 303.543.9500 **www.enterprisemanagement.com**

4577.081325-ES-LA