Delinea

DOCUMENTO TÉCNICO

El futuro de las contraseñas en el lugar de trabajo:

no muerto, sino en evolución

Resumen ejecutivo

Con todo el revuelo en torno a la autenticación sin contraseña, es fácil creer que las contraseñas están muertas y enterradas. Google, Apple, Microsoft y los medios están impulsando la visión de un proceso de inicio de sesión automatizado que sea sencillo de utilizar para los consumidores y difícil de descifrar para los delincuentes. Es una propuesta convincente, teniendo en cuenta que el aumento de los robos de identidad y las filtraciones de datos suelen deberse a contraseñas débiles o fáciles de robar.

Gran parte de la historia se ha centrado en las contraseñas de los consumidores para sitios web y aplicaciones. Pero, como hemos visto en el pasado, la adopción de nuevas soluciones para el lugar de trabajo a menudo va a la zaga de la tecnología de consumo. Por ejemplo, avances como las interfaces fáciles de usar y la instalación con un solo clic han creado altas expectativas de los consumidores respecto de la tecnología, mientras que muchas personas todavía experimentan dificultades con herramientas y procesos obsoletos en el trabajo.

Con esto en mente, nos propusimos comprender cómo están evolucionando las contraseñas en el lugar de trabajo. Encuestamos a 300 líderes de TI y ciberseguridad en los Estados Unidos, que representan a empresas de diferentes tamaños y sectores. Compartieron sus perspectivas sobre el estado actual y futuro de las contraseñas, incluido el potencial de la autenticación sin contraseña.

Descubrimos que, adaptando una cita tristemente célebre, los informes sobre la muerte de la contraseña parecen haber sido muy exagerados.

En cambio, nuestros resultados muestran que las contraseñas están evolucionando hacia algo nuevo. Aunque es posible que las contraseñas nunca desaparezcan por completo, se complementarán con otras formas de autenticación mejores. La gestión de las contraseñas seguirá desempeñando un papel fundamental en la seguridad del lugar de trabajo en el futuro previsible.

Sigue leyendo para saber cómo:

- Las organizaciones gestionan actualmente el riesgo de las contraseñas con una combinación de soluciones
- Los requisitos de cumplimiento normativo y los seguros impulsan la demanda de gestión de las contraseñas
- Las empresas ven la experiencia de inicio de sesión del futuro
- La autenticación multifactor (MFA), la biometría y la inteligencia artificial respaldan la evolución de las contraseñas
- Las herramientas heredadas y los riesgos empresariales requieren estrategias de seguridad que la autenticación sin contraseña no puede resolver

Peligros de una mala praxis con las contraseñas

Acceso no autorizado
Las contraseñas débiles se descifran fácilmente, lo que facilita que los hackers malintencionados obtengan acceso no autorizado a cuentas, sistemas e información confidencial.

Vulneraciones de datos
Las contraseñas débiles pueden provocar vulneraciones de datos, en las que se expone o se roba información personal o empresarial confidencial.

Compromiso/adquisición de cuenta
Si las personas reutilizan contraseñas en varias cuentas y una se ve comprometida, los atacantes pueden usar la misma contraseña para acceder a otras cuentas.

Robo de credenciales
Los hackers malintencionados pueden utilizar credenciales robadas para hacerse pasar por personas en línea, accediendo potencialmente a cuentas financieras o cometiendo fraude.

Datos comprometidos
Una mala praxis de las contraseñas puede comprometer secretos comerciales o información de empleados o clientes, lo que puede tener consecuencias financieras y legales.

Distribución de malware
Los hackers malintencionados pueden obtener acceso a cuentas para difundir malware, utilizando la cuenta de un usuario como plataforma de lanzamiento para ataques a la organización.

Ataques de phishing
Las contraseñas débiles facilitan que los atacantes engañen a las personas para que revelen sus credenciales de inicio de sesión a través de correos electrónicos o sitios web de phishing.

Consecuencias legales y normativas
Algunos sectores y países cuentan con normativas que requieren políticas de contraseñas seguras. Su incumplimiento puede dar lugar a sanciones legales.

Daños a la reputación
Una vulneración de la seguridad debido a una mala praxis con las contraseñas puede dañar tu reputación ante socios, clientes y accionistas, y posiblemente dar lugar a demandas.

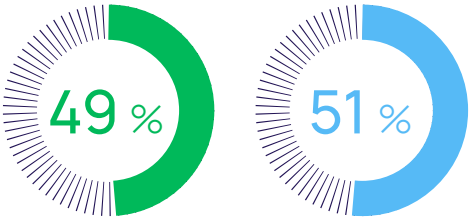
Pérdidas financieras
Las pérdidas significativas como resultado de una vulneración de la seguridad son comunes debido a muchos de los factores descritos anteriormente, incluidas multas elevadas, pérdida de clientes y demandas.

Estadísticas aterradoras de contraseñas relacionadas con el lugar de trabajo

480 $

Los empleadores gastan **480$ por empleado** en tiempo perdido debido a problemas con las contraseñas.

fuente: Más allá de la identidad

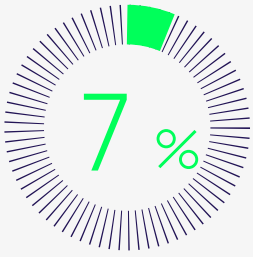


profesionales de seguridad informática

individuos

El 49 % de profesionales de seguridad de TI y el **51 % de individuos** comparten contraseñas con compañeros para acceder a cuentas comerciales.

fuente: Instituto Yubico y Ponemon



Si despiden con carácter urgente a un empleado, **solo el 7% de los responsables de seguridad de TI y ciberseguridad** confían plenamente en poder transferir contraseñas y credenciales, cancelar el acceso y mantener la continuidad del negocio.

fuente: Bravura Security

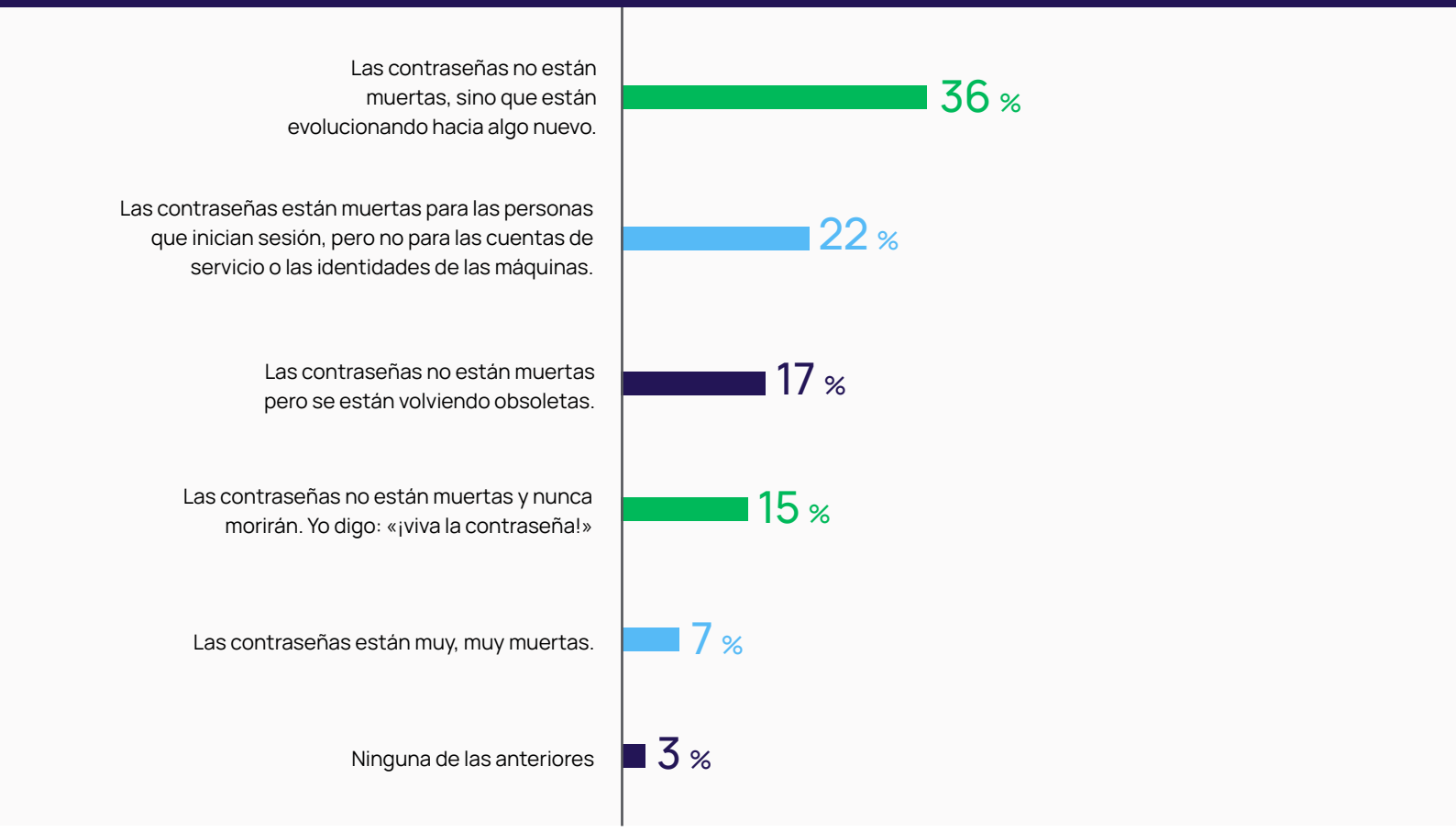
1 Las contraseñas en el lugar de trabajo no están muertas, sino que están evolucionando hacia algo nuevo

Los encuestados ya sienten los vientos del cambio, pero aún no están preparados para abandonar las contraseñas.

a. La mayoría afirma que las contraseñas están vivas y coleando

Un tercio de los encuestados cree que las contraseñas no están muertas sino que están evolucionando. En los extremos, algunos encuestados dicen que están contentos de haber dejado atrás sus contraseñas, mientras que otros dicen que nunca las abandonarán.
Uno de cada cuatro cree que las contraseñas están muertas para las personas, pero no para las máquinas. Según Gartner, las identidades de las máquinas se definen como contenedores, máquinas virtuales, aplicaciones, servicios, junto con dispositivos móviles, dispositivos IoT/OT, escritorios y firma de código. Las identidades de las máquinas están separadas de las identidades humanas y se utilizan para establecer confianza y autenticarse con otras máquinas en una red. Teniendo en cuenta que el número de identidades de máquinas ha superado con creces el de las identidades humanas, garantizar que estas conexiones sean seguras es una parte crucial de las estrategias de confianza cero y de seguridad que dan prioridad a la identidad.

Figura 1 | ¿Cuál de las siguientes opciones, si corresponde, describe MEJOR tu opinión sobre las contraseñas en el lugar de trabajo?

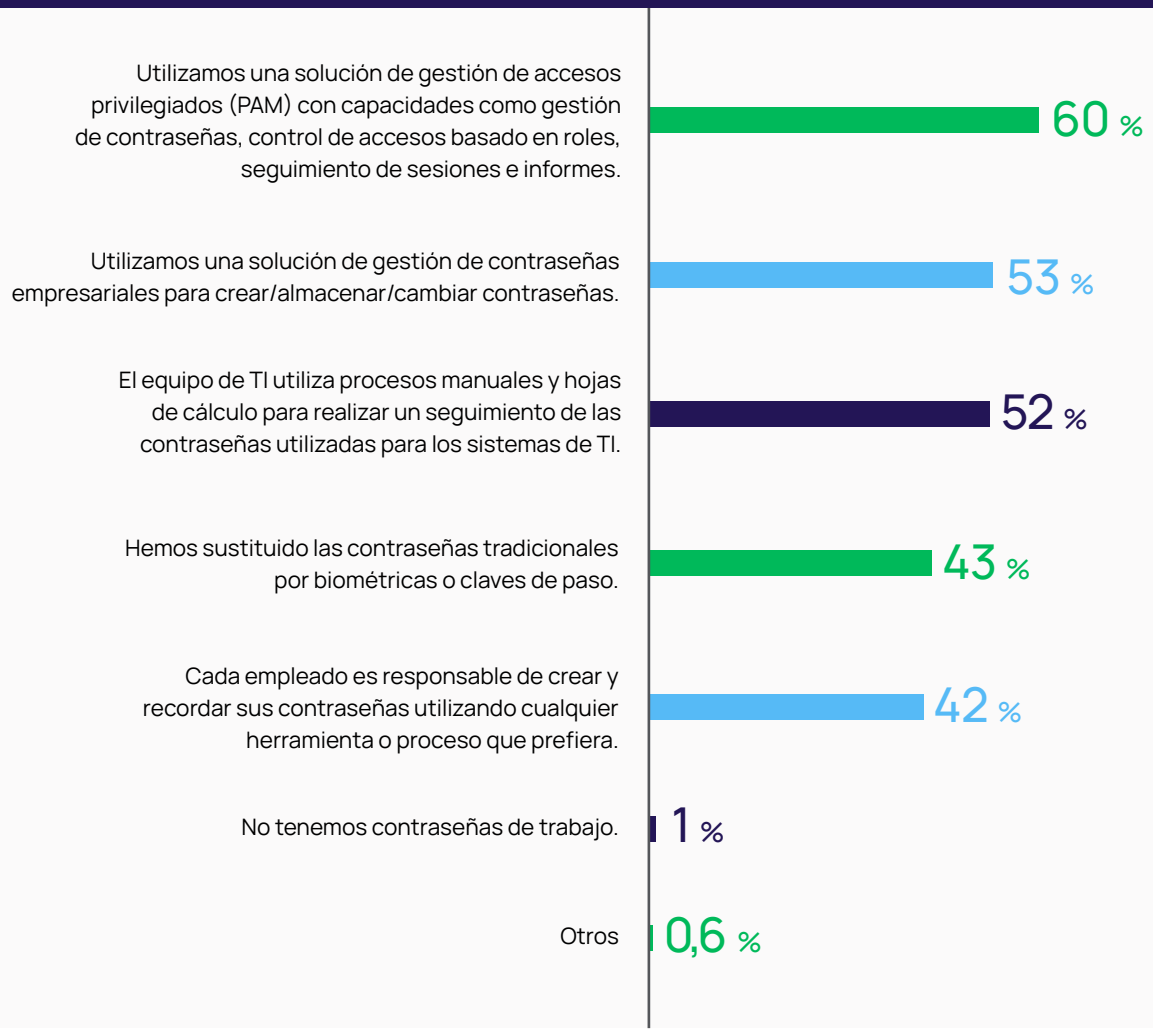


b. La mayoría de las organizaciones dependen de una combinación de soluciones de contraseñas para mitigar el riesgo

La buena noticia es que las organizaciones están tomando medidas para reducir los riesgos relacionados con una mala gestión de las contraseñas. La mayoría de los encuestados cuentan con múltiples soluciones. Descubrimos que:

- **La gestión de accesos privilegiados (PAM) lidera el grupo.** PAM, que incluye funciones como la administración de contraseñas, el control de accesos basado en roles (RBAC), la monitorización de sesiones y los informes, es más popular que las soluciones simples como los administradores de contraseñas, que están diseñadas principalmente para los consumidores.
- Desafortunadamente, más del 50 % de los encuestados respondieron que sus organizaciones todavía dependen parcialmente de **procesos manuales no seguros, como hojas de cálculo**, para crear, almacenar y cambiar contraseñas.
- Para el 43 % de los encuestados, sus organizaciones asignan **a sus empleados la responsabilidad** de administrar sus propias contraseñas utilizando las herramientas y métodos que prefieran. El riesgo interno aumenta con este enfoque, ya que es más probable que los usuarios cometan errores y no sigan las prácticas recomendadas, lo que hace que los equipos de TI y seguridad pierdan visibilidad y control.

Figura 2 | ¿Cómo gestiona actualmente tu organización las contraseñas de trabajo?

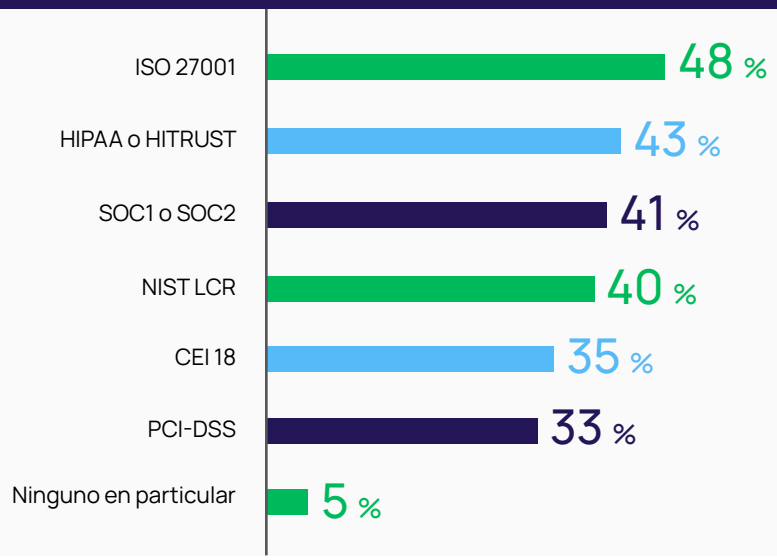


c. Los requisitos de cumplimiento normativo y los seguros impulsan la demanda de gestión de las contraseñas

Cualquier empresa evaluada por auditores o reguladores deberá demostrar que dispone de controles de gestión de contraseñas. Descubrimos que el 95 % de las empresas encuestadas deben cumplir al menos un conjunto de requisitos de cumplimiento normativo, y muchas tienen que cumplir más de un requisito.

Adaptarse a métodos sin contraseña sin dejar de cumplir con las normas puede ser complejo, ya que muchos marcos de cumplimiento normativo exigen requisitos de administración de contraseñas. Los auditores están acostumbrados a buscar controles observables basados en contraseñas. Incluso si eliminas las contraseñas de tu flujo de trabajo, deberás demostrar a los auditores que estás autenticando correctamente a los usuarios y proporcionándoles el nivel de acceso adecuado.

Figura 3 | ¿Qué marcos de cumplimiento normativo, si corresponde, debes cumplir actualmente?



El cumplimiento normativo rige la contraseña

Las prácticas comunes de seguridad de contraseñas requeridas por las regulaciones y estándares de cumplimiento incluyen:

- Aplicación de políticas de contraseñas seguras en cuanto a complejidad y longitud de caracteres
- Cambios periódicos de contraseña
- Implementación de la autenticación multifactor (MFA) para sistemas críticos
- Almacenamiento de contraseñas de forma segura mediante cifrado
- Supervisión y auditoría de actividades relacionadas con contraseñas
- Formación de los empleados sobre las mejores prácticas de seguridad de las contraseñas

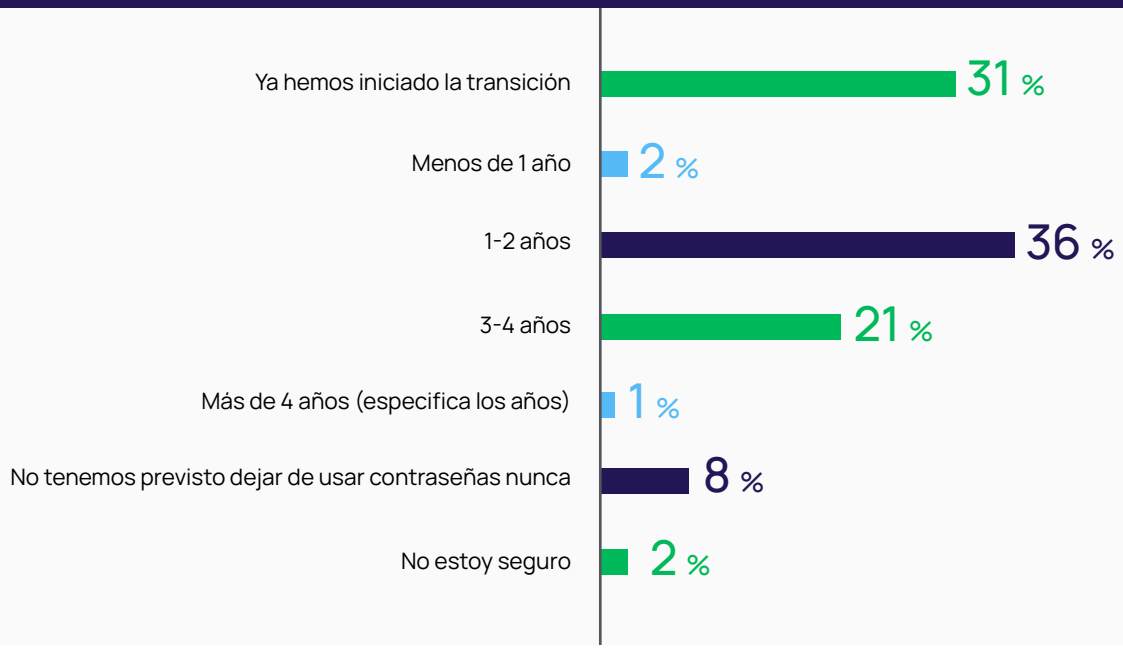
La mayoría de los organismos de cumplimiento normativo ofrecen orientación general y dejan los detalles al usuario. Otros son extremadamente específicos, como PCI, que aumentó los requisitos de caracteres de 7 a 12 en su última versión.

Obtén más información sobre los requisitos de cumplimiento normativo y auditoría en **https://delinea.com/es/solutions/security-compliance-audit**

d. La mayoría de los lugares de trabajo están a años de distancia de la autenticación sin contraseña

Eliminar las contraseñas no parece estar en la lista de prioridades de las empresas en este momento, tal vez debido a iniciativas competitivas y condiciones económicas cambiantes. Si bien el 30 % de los encuestados dice que ya ha comenzado la transición a la autenticación sin contraseñas, la mayoría prevé que no comenzará la transición hasta dentro de al menos un año, y algunos dicen que entre tres y cuatro años.

Figura 4 | ¿Qué plazo tiene su organización, si es que tiene alguno, para iniciar la transición hacia el abandono de las contraseñas?



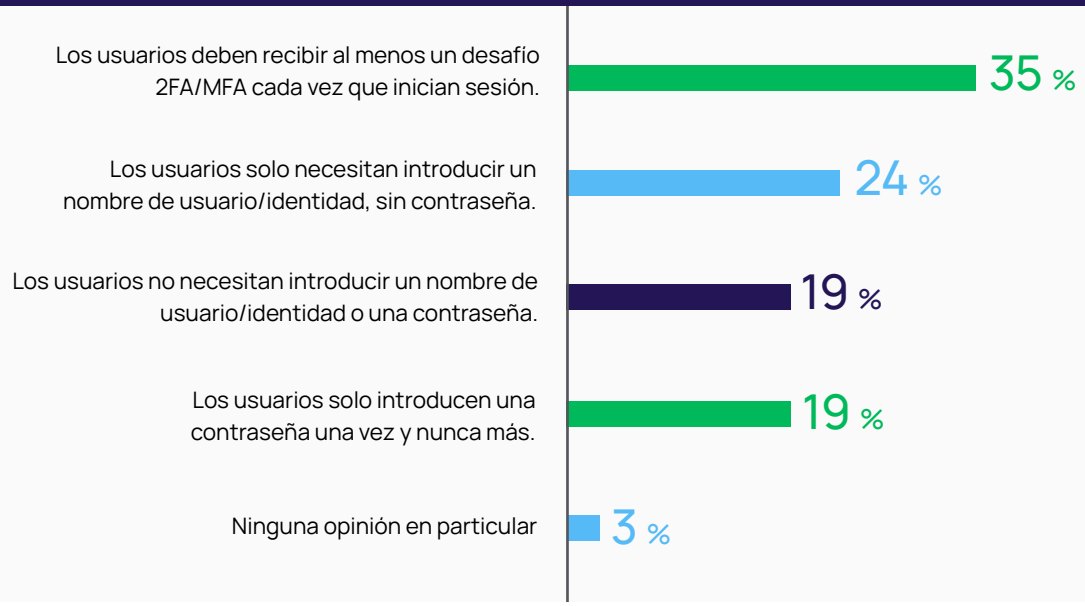
2 | La diferencia entre experiencia sin contraseña y despliegue sin contraseña

Por el momento, las empresas parecen tener una idea más clara de la *experiencia* sin contraseña que de cómo procederán con el *despliegue* sin contraseñas. Con una experiencia sin contraseña, las personas se autentican en recursos sin ningún secreto compartido. Aún cuando no se requiera que los usuarios introduzcan contraseña, la mecánica de autenticación de las contraseñas sigue produciéndose entre bastidores. El despliegue completo sin contraseñas, en el que el sistema de autenticación no mantiene ningún secreto compartido, es mucho más difícil de conseguir.

a. Esperar que la experiencia del usuario cambie

En el futuro, ¿qué deberías esperar al iniciar sesión en las herramientas del lugar de trabajo? Bueno, eso depende de dónde trabajes. Para algunas empresas, puede significar un proceso automatizado y totalmente independiente. Para la mayoría, implicará algunos pasos más para la verificación de la identidad.

Figura 5 | En tu opinión, ¿qué describe mejor la experiencia del usuario al obtener acceso a los sistemas del lugar de trabajo sin contraseñas?



b. Hay muchas esperanzas puestas en la biometría

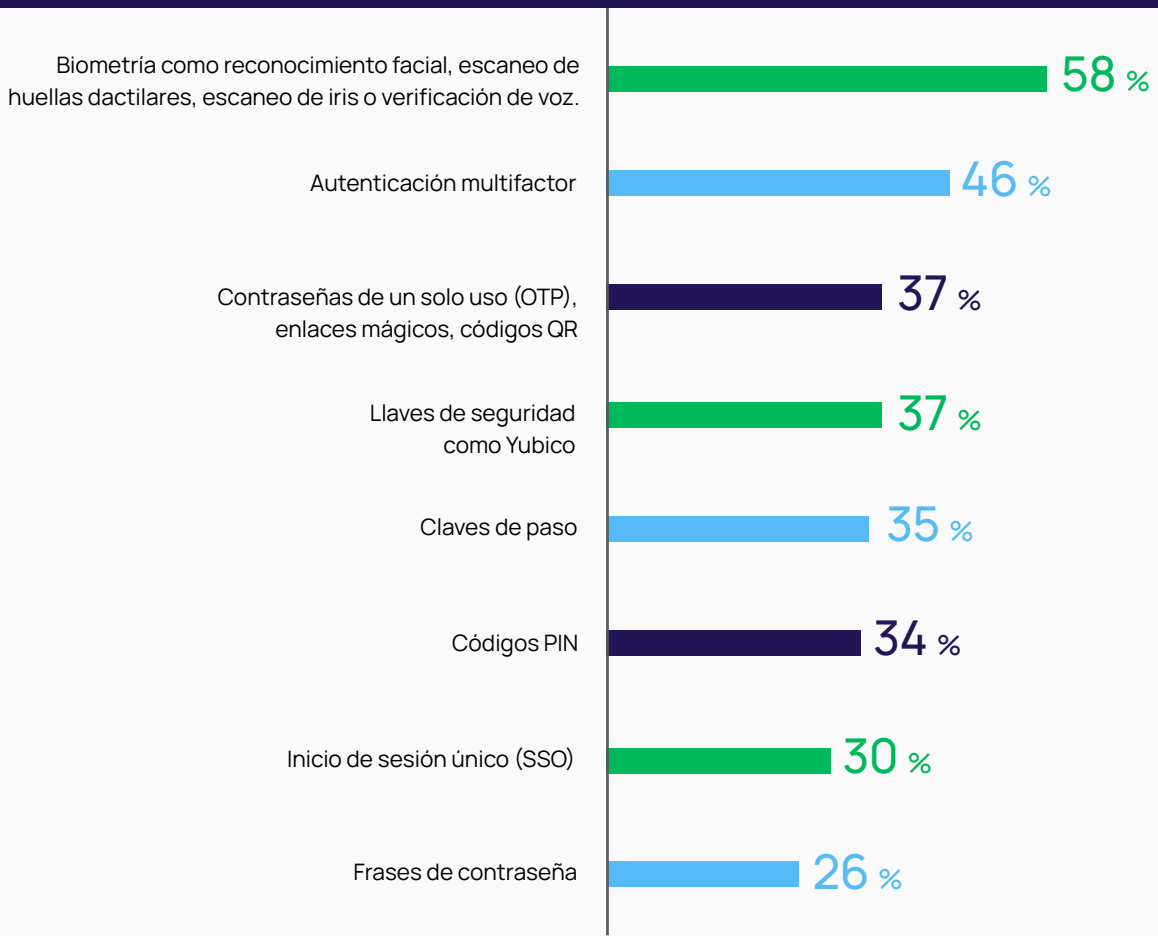
En lo que se refiere a la implementación técnica, existen muchas soluciones técnicas potenciales que compiten por reemplazar o complementar la contraseña tradicional. La mayoría de los encuestados espera que la biometría, como el reconocimiento de huellas dactilares, el reconocimiento facial e incluso la biometría conductual (por ejemplo, patrones de mecanografía), sea el camino a seguir.

Para que la autenticación basada en biometría sea una realidad en el lugar de trabajo, el software tendrá que demostrar una alta tasa de éxito. En pruebas independientes, muchos sistemas biométricos no cumplen actualmente sus promesas de precisión. En la práctica, cada empresa y proveedor de software deberá determinar lo estricta o indulgente que es la autenticación para equilibrar la facilidad de uso con la precisión.

Después de la biometría, muchos lugares de trabajo esperan confiar en la MFA como parte de la evolución de las contraseñas, exigiendo que las personas confirmen sus identidades con algo que tienen o saben. Es una noticia alentadora para las soluciones MFA que han estado luchando contra la fatiga de la MFA, en la que los usuarios rechazan pasos adicionales en el proceso de inicio de sesión.

Aunque las claves de paso basadas en FIDO2 son la solución técnica anunciada por los gigantes de la tecnología de consumo, curiosamente, los responsables de la toma de decisiones en TI y ciberseguridad no las calificaron como una de las mejores soluciones para la autenticación en el lugar de trabajo.

Figura 6 | ¿Con qué soluciones técnicas, si las hay, estás reemplazando o esperas reemplazar las contraseñas?

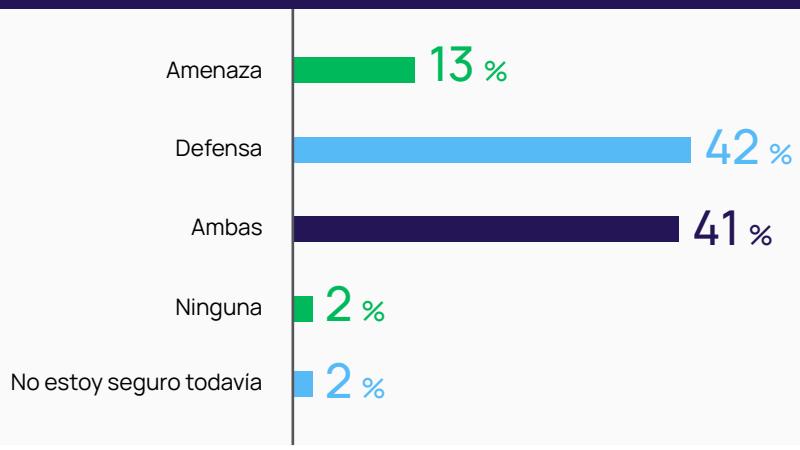


c. Más encuestados ven a la IA como una defensa, en lugar de una amenaza

Parece que todo el mundo tiene una opinión sobre cómo afectará la explosión de la IA generativa a la ciberseguridad. Por un lado, las capacidades de la IA están facilitando que los autores de amenazas creen correos electrónicos de phishing con apariencia realista para atrapar a sus víctimas, y el uso de herramientas públicas de IA en el lugar de trabajo aumenta el riesgo de que la información privada quede expuesta. Por otro lado, la IA tiene el potencial para que los equipos cibernéticos y de TI detecten amenazas con mayor facilidad y precisión, y respondan de inmediato.

En el caso del acceso con privilegios, más encuestados ven a la IA como una defensa que como una amenaza. Esto es particularmente cierto para las empresas grandes.

Figura 7 | ¿Crees que la inteligencia artificial es una amenaza o una defensa del acceso con privilegios?

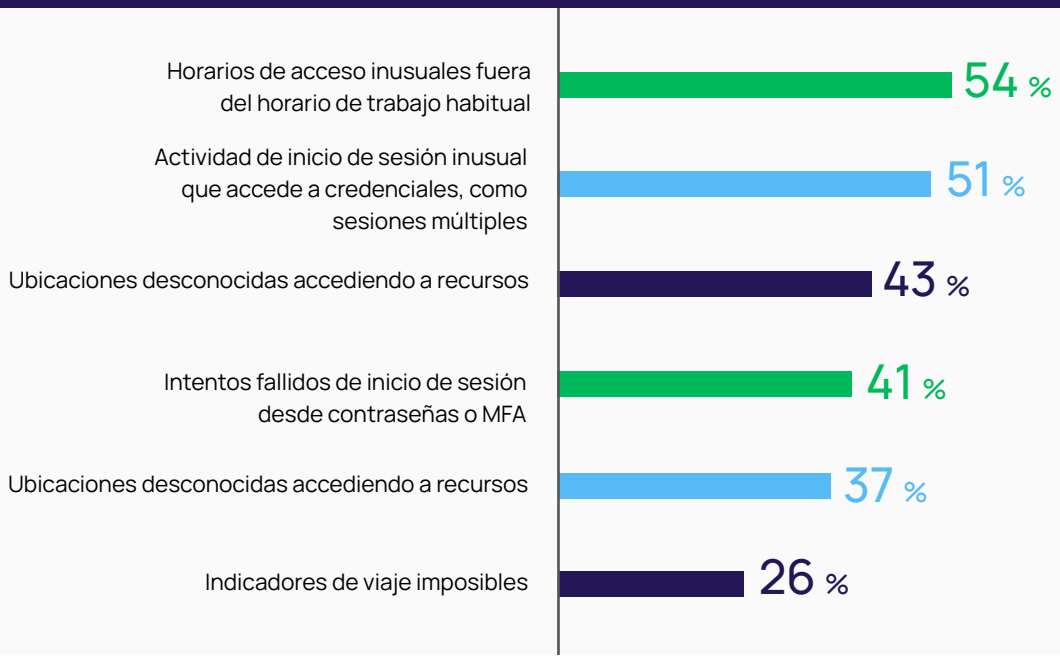


d. El análisis de comportamiento puede identificar ataques basados en credenciales

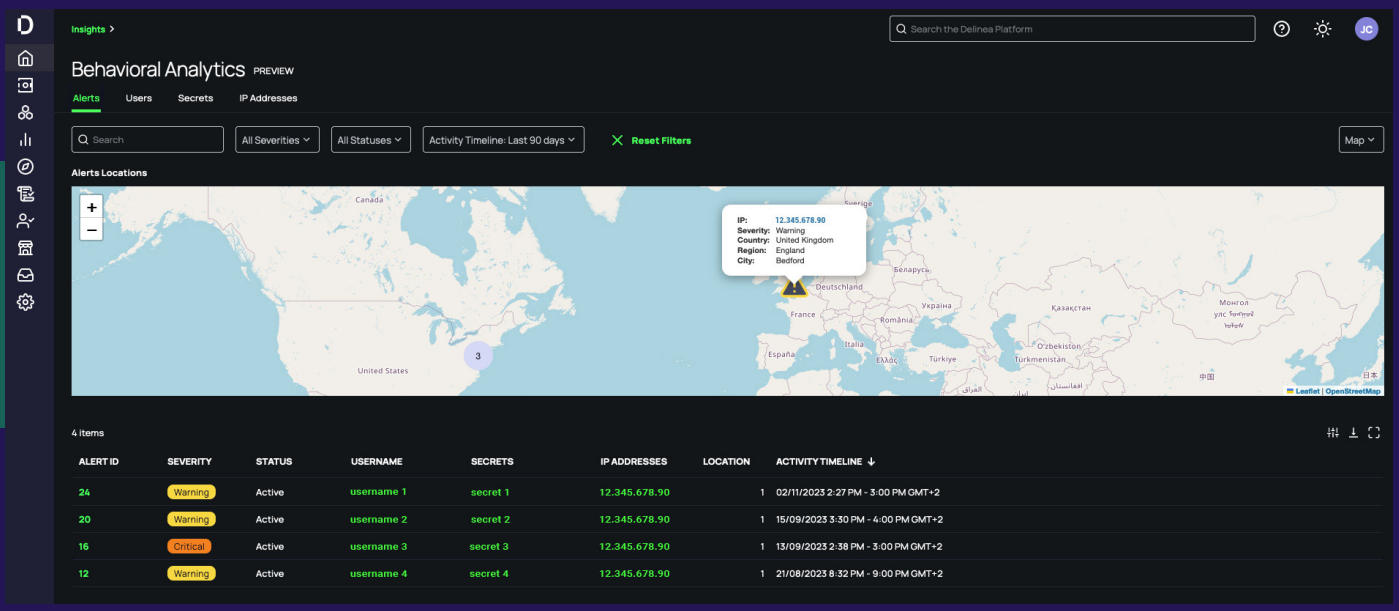
A medida que las contraseñas evolucionan, los responsables de la toma de decisiones reacios al riesgo van a necesitar una red de seguridad. Si bien los procesos de autenticación como la biometría y MFA brindarán algunas garantías, nada es seguro al 100 %. Seguirá habiendo casos en los que personas no autorizadas obtengan acceso.

Si eso sucede, las empresas deben conocer las señales de los ataques basados en credenciales para poder detener a los atacantes en seco. El análisis basado en el comportamiento puede identificar actividades de credenciales sospechosas y alertar a los equipos de seguridad para que investiguen las señales de alerta. Los encuestados dicen que hay muchos indicadores de compromiso que les gustaría conocer antes de que sea demasiado tarde.

Figura 8 | ¿Cuáles son, en todo caso, las mejores formas de ayudarte a detectar actividad de credenciales sospechosa?



¿Qué son las claves de paso basadas en FIDO2?



El estándar emergente para claves de paso es FIDO2, desarrollado por un consorcio de empresas de tecnología conocido como FIDO Alliance. FIDO2 está destinado a hacer que el proceso de autenticación de usuarios sea más seguro, con una solución que sea fácil de adoptar para las personas.

- El uso de cifrado de clave pública y datos biométricos hace que FIDO2 sea significativamente más seguro que los métodos tradicionales de autenticación basados en contraseñas.
- FIDO2 elimina la necesidad de que los usuarios recuerden contraseñas complejas y las cambien periódicamente.
- El diseño de FIDO2 lo hace resistente a los ataques de phishing, ya que las claves de autenticación están vinculadas a sitios web específicos y se requiere el consentimiento del usuario para cada intento de autenticación.
- Los usuarios pueden conservar sus credenciales de autenticación en sus dispositivos y no compartirlas con servicios en línea.

FIDO2 consta de dos componentes principales:

- **Autenticación web (WebAuthn):** WebAuthn, compatible con los principales navegadores, permite a las personas utilizar datos biométricos o dispositivos de seguridad externos, como claves de seguridad USB, para demostrar su identidad al iniciar sesión en servicios en línea.
- **Protocolo de cliente a autenticador (CTAP):** los dispositivos de seguridad externos interactúan con el ordenador o el dispositivo móvil de un usuario durante el proceso de autenticación, lo que garantiza que las claves privadas se almacenen de forma segura y nunca abandonen el dispositivo de seguridad.

3 | La evolución de la contraseña no será fluida

En comparación con la tecnología de consumo, los lugares de trabajo tienen requisitos y procesos de toma de decisiones más complejos que están vinculados a prácticas basadas en contraseñas. Los responsables de la toma de decisiones en materia de TI y cibernética deben considerar no solo el coste de adquisición de nueva tecnología, sino también los aspectos de gestión del cambio de la tecnología y la adopción de procesos, especialmente a medida que crecen sus organizaciones.

a. La tecnología heredada ralentiza el ritmo de evolución de las contraseñas

En el caso de la autenticación sin contraseña, descubrimos que los recursos no son un problema para la mayoría de las empresas encuestadas. La mayoría de los encuestados creen que tienen las habilidades y el presupuesto necesarios.

Los encuestados dicen que la tecnología heredada, así como la necesidad de procesos uniformes que se puedan gobernar en toda una organización, están definiendo el ritmo de la evolución de las contraseñas. La tecnología y los procesos heredados están frenando la carrera hacia la autenticación sin contraseña. Las organizaciones a menudo se vuelven dependientes de proveedores o tecnologías específicos, lo que puede limitar la flexibilidad para cambiar los procesos. Es posible que estos sistemas y aplicaciones heredados no tengan la infraestructura o las API necesarias para integrarse con soluciones modernas sin contraseña.

Garantizar una experiencia de usuario consistente en varios dispositivos y sistemas operativos puede ser un desafío, porque los métodos de autenticación sin contraseña pueden no ser compatibles con todos los dispositivos y plataformas.

Los problemas de sincronización son reales. Dado que los usuarios traen sus propios dispositivos, puede resultar difícil verificar las identidades de los usuarios en todos los sistemas.

Figura 9 | En tu opinión, ¿qué obstaculiza o podría obstaculizar que tu lugar de trabajo no tenga contraseñas?

b. La autenticación sin contraseña no es una solución mágica de seguridad

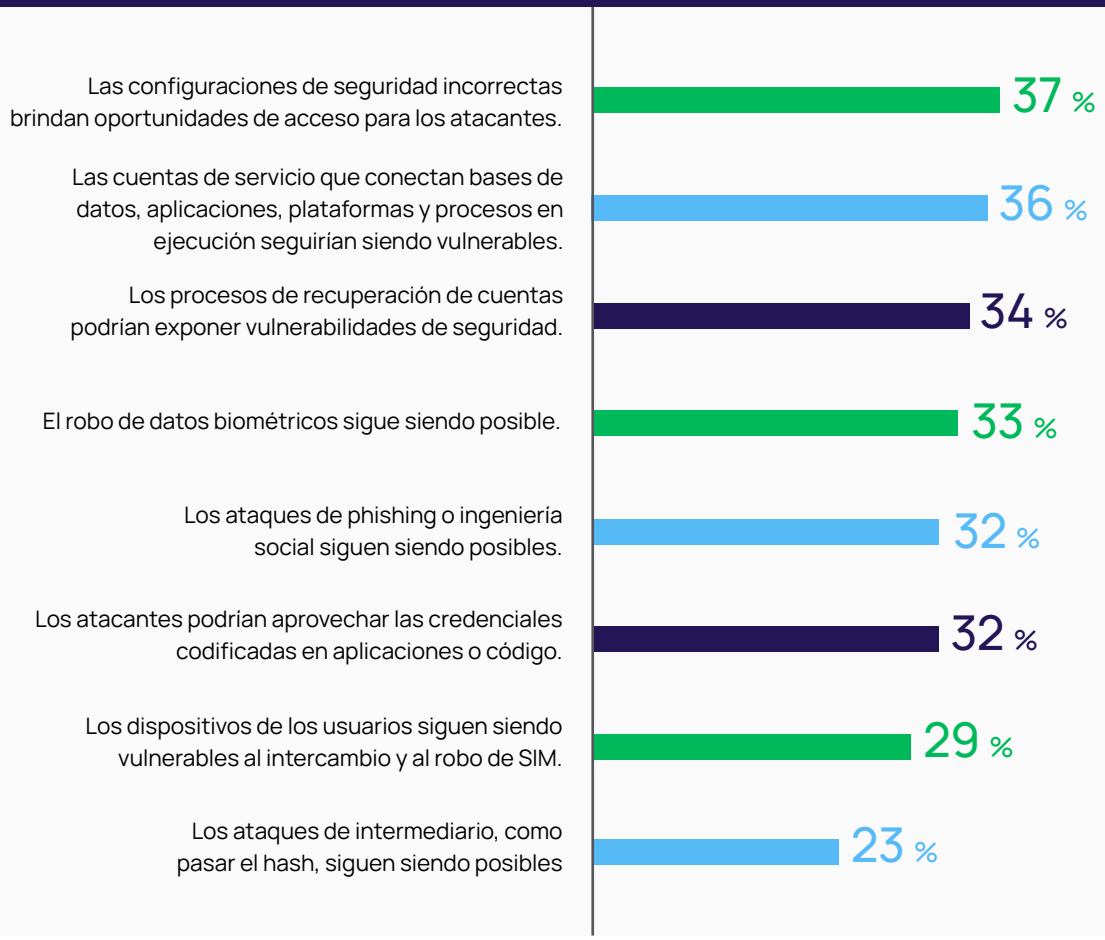
Aunque la autenticación sin contraseña puede mitigar algunos tipos de ataques, como el descifrado de contraseñas y la introducción de credenciales, los líderes de TI y ciberseguridad reconocen que no resolverá muchos desafíos críticos de seguridad.

El error humano sigue siendo una preocupación. Los encuestados están más preocupados por las configuraciones incorrectas que conducen a accesos no autorizados, por ejemplo, un depósito S3 que se deja abierto y accesible para todos.

Además del factor humano, a los encuestados también les preocupan las máquinas. Las identidades de las máquinas y las cuentas de servicio a menudo dependen de contraseñas y otros mecanismos de autenticación poco comprendidos o documentados. Si alguno de esos mecanismos falla debido a un cambio en el proceso de autenticación, las operaciones comerciales críticas pueden fallar.

Estos riesgos requerirán atención y recursos de seguridad, independientemente del camino de evolución de contraseñas que elijan las empresas.

Figura 10 | Si los usuarios ya no tuvieran que usar contraseñas, ¿qué riesgos de seguridad crees que seguirían afectando a tu organización?



Conclusión y recomendaciones

Los resultados de esta encuesta demuestran que las prácticas de gestión de contraseñas en el lugar de trabajo están evolucionando, aunque las organizaciones aún no se han alejado radicalmente de las contraseñas tradicionales. Esperamos que las soluciones automatizadas para la gestión de contraseñas sigan desempeñando un papel fundamental en el panorama de la seguridad durante algún tiempo y se vuelvan especialmente importantes a medida que superpongan controles para la autenticación, el acceso y la aplicación.

A medida que las marcas de tecnología de consumo y la Alianza FIDO crean una demanda de autenticación sin contraseña, las empresas seguramente escucharán que los empleados esperan el mismo tipo de experiencia fluida en el trabajo. A medida que la biometría se vuelva más precisa, la tecnología heredada sea reemplazada y la inteligencia artificial cree una red de seguridad más sólida, las empresas probablemente se sentirán más cómodas con un futuro sin contraseñas.

Puedes tomar medidas hoy y prepararte para que el ecosistema tecnológico y la plantilla de tu organización estén preparados para la evolución de las contraseñas.

#Eliminarlashojas

Si tu organización es como la mayoría y todavía usa contraseñas, asegúrate de almacenarlas en un almacén seguro de contraseñas cifradas, en lugar de hojas de cálculo y notas adhesivas. No hagas recaer en los usuarios la responsabilidad de elegir su propio proceso de administración de contraseñas. Terminarás con procesos manuales heterogéneos que dejan las contraseñas y las cuentas privilegiadas sin administrar y expuestas a ataques. Realiza la transición a un proceso automatizado que aplique contraseñas únicas y complejas, limita el uso compartido de contraseñas y las rote de forma regular e inesperada.

Aumenta la confianza en la autenticación

Aplica la autenticación multifactor (MFA) en toda la cadena de acceso desde el momento del primer inicio de sesión hasta la elevación de privilegios. La autenticación basada en riesgos responde de forma adaptativa a los cambios de estado. Por ejemplo, puede pasar a un estado de supervisión intensificado en momentos de riesgo, como reorganizaciones y despidos. La autenticación continua monitoriza el comportamiento del usuario durante una sesión. El acceso se puede revocar si se detecta actividad sospechosa o se puede requerir una verificación adicional.

Administra el acceso, no solo las contraseñas

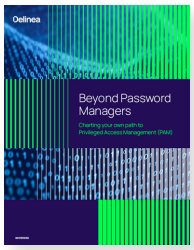
Las soluciones de gestión de accesos con privilegios (PAM) ofrecen un mayor nivel de seguridad que los administradores de contraseñas. Además de proteger contraseñas y otros secretos en un almacén seguro central, incluyen controles de acceso granulares. En lugar de un acceso amplio y permanente, los usuarios reciben un acceso de forma puntual y mínimo según sus funciones o responsabilidades.

Además del almacén seguro de contraseñas, PAM proporciona amplias capacidades de supervisión y auditoría. Esto ayuda a detectar y responder a incidentes de seguridad, así como a cumplir con los requisitos normativos. Las soluciones PAM pueden identificar actividades privilegiadas sospechosas o anómalas en tiempo real y activar alertas o respuestas automáticas, lo que te ayuda a abordar de forma proactiva posibles amenazas a la seguridad.

Mejora la conciencia cibernética

Incluso si cuentas con todas las soluciones de ciberseguridad adecuadas, sigue siendo fundamental invertir en formación para garantizar que los empleados comprendan la importancia de proteger las credenciales, verificar identidades y administrar el acceso. Con la educación y la formación práctica adecuadas, los empleados pueden pasar del eslabón más débil de la cadena de la ciberseguridad a una fuerza impulsora positiva.

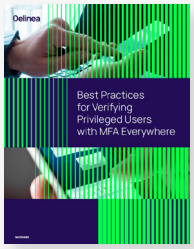
Recursos compartidos



Más allá de los gestores de contraseñas

Descubre por qué los administradores de contraseñas para consumidores no son suficientes para proteger las cuentas con privilegios en la empresa.

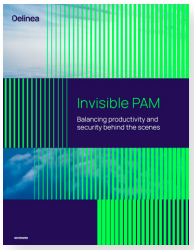
delinea.com/es/resources/password-managers-to-privileged-access-management



MFA En todas partes

El hecho de que alguien pueda presentar la contraseña correcta no garantiza que sea el usuario que crees que es. La autenticación multifactor (MFA) mitiga el riesgo en toda la cadena de puntos de control de acceso.

delinea.com/es/resources/verify-privileged-users-with-mfa-everywhere-whitepaper



Solución PAM invisible

Reduce la ciberfatiga y fomenta la satisfacción de los empleados Con las integraciones nativas, la gestión de los accesos con privilegios se sitúa entre bastidores y sincroniza todas las identidades, funciones, permisos y actividades con privilegios.

delinea.com/es/resources/invisible-pam-whitepaper

Privileged Access Management for Dummies (EN)

Una lectura rápida y sencilla para ponerse al día sobre la gestión de accesos privilegiados y los principios fundamentales de la seguridad

https://delinea.com/es/resources/privileged-access-management-for-dummies-pdf

Active Directory Weak Password Finder (EN)

Buscador de contraseñas débiles: descubre lo fácil que es descifrar contraseñas AD débiles y toma medidas para protegerlas.

delinea.com/resources/weak-password-finder-tool-active-directory

PRUEBA GRATUITA

Prueba la solución PAM líder en el sector, Secret Server, de forma gratuita durante 30 días.

delinea.com/es/products/secret-server#trial

Delinea

Defining the boundaries of access

Delinea es un proveedor líder de soluciones de gestión de accesos privilegiados (PAM) que proporciona seguridad sin fisuras a la empresa híbrida moderna. Delinea Platform amplía la capacidad y el rendimiento de las soluciones PAM proporcionando autorización para todas las identidades, controlando el acceso a la infraestructura de nube híbrida más crítica de una organización y a los datos sensibles. Su objetivo es ayudar a reducir el riesgo, garantizar el cumplimiento normativo y simplificar la seguridad. Delinea reduce la complejidad y controla los límites de los accesos para miles de clientes en todo el mundo. Nuestros clientes comprenden desde pequeñas empresas hasta las mayores instituciones financieras del mundo, organismos de inteligencia y empresas de infraestructuras críticas. **delinea.com/es/**