Informe exclusivo de investigación

Patrocinado por Keeper Security

Pollfish

 | keeper.io/malpracticereport

Introducción

La mala higiene de las contraseñas en el lugar de trabajo ya era una amenaza para la ciberseguridad de las organizaciones incluso antes de la pandemia de la COVID-19. Cuando la COVID-19 obligó a las organizaciones de todo el mundo a desplegar y asegurar rápidamente la capacidad de trabajo a distancia de sus empleados, los equipos comenzaron a conectarse a los recursos de la organización a distancia, en entornos que sus empleadores no controlaban, muchas veces utilizando sus propios dispositivos.

Los encuestados en el informe del Instituto Ponemon titulado **Ciberseguridad en la era del trabajo a distancia: un informe global de riesgos**, encargado por Keeper Security en 2020, expresaron su gran preocupación por la seguridad de las contraseñas en sus organizaciones:

- El 60 % de los encuestados dijeron que sus organizaciones habían sufrido un ciberataque en los últimos 12 meses.
- Más del 50 % de estos ataques incluyeron credenciales robadas.
- El robo de activos informáticos causó daños por valor de 5 millones de dólares o más en el 25 % de las empresas.

La pandemia empujó a las organizaciones a desplegar rápidamente una serie de nuevas tecnologías para mantener a los teletrabajadores conectados, colaborando y trabajando. Desde Zoom hasta Google Workspace y Slack, los empleados tuvieron que registrarse en más cuentas en línea, y mantener un registro de más contraseñas.

Keeper quería averiguar hasta qué punto había cambiado la seguridad de las contraseñas desde que las empresas pasaron a trabajar en entornos remotos. ¿Estaban los empleados que trabajan a distancia siguiendo las mejores prácticas para proteger sus contraseñas, o estaban cayendo en la «fatiga de las contraseñas» y adoptando malos hábitos que conducen a importantes riesgos de ciberseguridad? Por ello, Keeper se asoció con Pollfish para realizar la Encuesta sobre imprudencias en el uso de contraseñas en el trabajo.

Mientras que Ponemon realizó una encuesta a los líderes de las organizaciones, nosotros decidimos ir directamente a los empleados para esta encuesta, y preguntamos a 1000 trabajadores a tiempo completo en Estados Unidos sobre sus hábitos de uso de las contraseñas. La encuesta finalizó en febrero de 2021, y estaba compuesta únicamente por personas que utilizaban contraseñas para iniciar sesión en cuentas online relacionadas con el trabajo.

A continuación se exponen las conclusiones más importantes de la encuesta. Los datos completos también pueden consultarse en la página 6.

Conclusión 1: Los empleados estadounidenses están organizando y almacenando sus credenciales de acceso de forma insegura

Nuestra encuesta reveló que los empleados estadounidenses no siguen las mejores prácticas a la hora de almacenar y organizar sus contraseñas relacionadas con el trabajo, lo que supone importantes riesgos de ciberseguridad para sus empleadores.

- Más de la mitad de los encuestados (57 %) admite haber anotado las contraseñas online relacionadas con el trabajo en «notas adhesivas», y dos tercios de ellos (67 %) admiten haber perdido estas notas. Además de dejar la información sensible de la empresa a la vista de cualquier otra persona que viva o visite su casa, esto perjudica la eficiencia de la organización. Las notas adhesivas perdidas significan contraseñas perdidas, lo que resulta en tickets de asistencia para restablecer dichas contraseñas.

- El 62 % de los encuestados almacena las credenciales de acceso en un cuaderno o diario, y la abrumadora mayoría (82 %) afirma que guarda estos cuadernos al lado o cerca de sus dispositivos de trabajo, donde puede acceder a ellas cualquier otra persona que viva en su casa o esté de visita.

Utilizar un bolígrafo y un papel para anotar las contraseñas se ha vuelto aún más problemático en el mundo del trabajo a distancia. La mayoría de los trabajadores (66 %) dice que es más probable que anoten las contraseñas relacionadas con el trabajo cuando trabajan desde casa que cuando trabajan en la oficina.

Incluso cuando utilizan métodos digitales para organizar y almacenar sus contraseñas, los empleados estadounidenses están llevando a cabo prácticas de seguridad de contraseñas deficientes.

- Casi la mitad de los encuestados (49 %) guarda las contraseñas relacionadas con el trabajo en un documento en la nube.

- Algo más de la mitad (51 %) afirma que actualmente guarda estas contraseñas en un documento guardado en su ordenador.

- El 55 % guarda las contraseñas relacionadas con el trabajo en su teléfono.

Almacenar las contraseñas en archivos no encriptados es extremadamente arriesgado. Lo único que necesita un ciberdelincuente es vulnerar el almacenamiento en la nube, el ordenador o el dispositivo móvil, y podrá acceder a todas las contraseñas de los empleados.

Conclusión 2: Los empleados estadounidenses están creando contraseñas débiles y fáciles de adivinar

Una contraseña segura consiste en una cadena aleatoria de letras mayúsculas y minúsculas, números y caracteres especiales. Sin embargo, muchos de los encuestados admitieron que utilizan contraseñas que contienen datos personales, que los ciberdelincuentes pueden encontrar fácilmente en los canales de las redes sociales.

- Más de un tercio (37 %) de los encuestados ha utilizado el nombre de su empleador en una contraseña relacionada con el trabajo.

- Más de un tercio (34 %) ha utilizado el nombre o el cumpleaños de su pareja.

- Casi un tercio (31 %) ha utilizado el nombre o el cumpleaños de su hijo.

La reutilización de contraseñas entre las cuentas personales y las relacionadas con el trabajo se ha convertido en un gran riesgo de ciberseguridad para las empresas, ya que el 44 % de los encuestados admite que reutiliza las contraseñas en sus cuentas personales y en las relacionadas con el trabajo y el 53 % admite que mantiene cuentas personales protegidas por contraseña en sus dispositivos de trabajo.

Conclusión 3: Los empleados estadounidenses comparten contraseñas relacionadas con el trabajo con personas no autorizadas

Muchos empleados estadounidenses no tienen cuidado de con quién comparten sus contraseñas relacionadas con el trabajo. Esto pone a las organizaciones en riesgo de sufrir una filtración si estas contraseñas acaban en manos de alguien imprudente o con intenciones maliciosas.

- En el último año, el 14 % de los encuestados ha compartido sus contraseñas relacionadas con el trabajo con su pareja o cónyuge.
- El 11 % de los encuestados ha compartido contraseñas relacionadas con el trabajo con otro miembro de la familia.

Incluso en ausencia de una filtración de datos, un empleador podría ser declarado culpable de incumplimiento y se le impondrían sanciones muy importantes, si se descubriera que partes no autorizadas han visto información protegida por el cumplimiento normativo.

Conclusión 4: Los empleadores estadounidenses no están cumpliendo su parte para garantizar que las contraseñas se compartan de forma segura y/o sólo con las partes autorizadas

Nuestra encuesta reveló que las contraseñas compartidas en el lugar de trabajo son comunes.

- Casi la mitad de los encuestados (46 %) afirma que su empresa comparte las contraseñas de las cuentas que utilizan varias personas.
- Más de un tercio (34 %) ha compartido contraseñas relacionadas con el trabajo con compañeros del mismo equipo.
- Casi un tercio (32 %) ha compartido las contraseñas relacionadas con el trabajo con sus jefes.
- El 19 % ha compartido sus contraseñas con su equipo ejecutivo.

Lo mejor es dar a cada usuario una contraseña única para cada cuenta o aplicación relacionada con el trabajo, lo que puede hacerse de forma práctica mediante el uso de una plataforma de gestión de contraseñas de empresa (EPM). Compartir las contraseñas en el lugar de trabajo es seguro si las contraseñas se comparten de forma segura y únicamente con personas autorizadas. Los resultados de nuestra encuesta indican que muchos empleadores estadounidenses no están aplicando estrategias de mitigación de riesgos para ayudar a garantizar que se compartan las contraseñas de forma segura.

- La mayoría de los encuestados (62 %) afirman haber compartido una contraseña relacionada con el trabajo a través de un mensaje de texto o un correo electrónico, que podría ser interceptado en tránsito por los ciberdelincuentes.

- Casi un tercio de los encuestados (32 %) admite haber accedido a una cuenta en línea perteneciente a un antiguo empleador, lo que indica que muchos empleadores no desactivan las cuentas cuando los empleados dejan la empresa.

Conclusión

La adopción e implementación de una plataforma de gestión de contraseñas para empresas como Keeper Enterprise solucionaría las imprudencias en el uso de contraseñas descubiertas en esta encuesta. La encriptación de contraseñas de conocimiento cero y el marco de confianza cero de Keeper proporcionan una gestión avanzada de contraseñas, un uso compartido seguro y otras funcionalidades de seguridad. Los administradores y responsables de TI obtienen una visibilidad y un control completos de las prácticas de contraseñas de los empleados, incluyendo:

- Modelo de seguridad exclusivo de conocimiento cero y sistema de marco de confianza cero; todos los datos en tránsito y en reposo están encriptados; no pueden ser vistos por los empleados de Keeper Security ni por ninguna parte externa.

- Despliegue rápido en todos los dispositivos, sin costes iniciales de equipamiento o instalación.

- Integración personalizada y soporte y formación 24 horas al día, 7 días a la semana, por parte de un especialista de soporte.

- Soporte para RBAC, 2FA, auditoría, reporte de eventos y múltiples estándares de cumplimiento, incluyendo HIPAA, DPA, FINRA y RGPD.

- Provea a los equipos de carpetas compartidas, subcarpetas y contraseñas seguras.

- Autenticación única (SAML 2.0)

- Habilite el acceso al almacén sin conexión cuando el SSO no esté disponible.

- Provisión dinámica de bóvedas a través de SCIM.

- Configurable para Alta Disponibilidad (HA).

- Autenticación avanzada de dos factores/múltiples factores.

- Sincronización de Active Directory y LDP.

- Aprovisionamiento de SCIM y Azure AD.

- API para desarrolladores para la rotación de contraseñas y la integración del backend.

Resultados de la encuesta

ELIGE UNA RESPUESTA

PU1. ¿Está actualmente empleado a tiempo completo?

#	Respuestas	Respuestas (%)	Suma
A1	Sí	100,00%	1000
A2	No	0,00%	0

ELIGE UNA RESPUESTA

PU2. ¿Utiliza actualmente contraseñas para acceder a las cuentas online relacionadas con el trabajo?

#	Respuestas	Respuestas (%)	Suma
A1	Sí	100,00%	1000
A2	No	0,00%	0

ELIGE UNA RESPUESTA

P1. ¿Tiene actualmente alguna contraseña online relacionada con el trabajo anotada en una nota adhesiva?

#	Respuestas	Respuestas (%)	Suma
A1	Sí	57,30%	573
A2	No	42,70%	427

ELIGE UNA RESPUESTA

P2.Si es así, ¿ha perdido alguna vez esa nota adhesiva?

#	Respuestas	Respuestas (%)	Suma
A1	Sí	66,55%	382
A2	No	33,45%	192

ELIGE UNA RESPUESTA

P3. ¿Es más probable que anote las contraseñas online relacionadas con el trabajo cuando trabaja desde casa?

#	Respuestas	Respuestas (%)	Suma
A1	Sí	66,00%	660
A2	No	34,00%	340

ELIGE UNA RESPUESTA

P4. ¿Tiene actualmente un cuaderno o un diario en el que guarda los datos de acceso y las contraseñas?

#	Respuestas	Respuestas (%)	Suma
A1	Sí	62,10%	621
A2	No	37,90%	379

ELIGE UNA RESPUESTA

P5. En caso afirmativo, ¿tiene ese cuaderno al lado o cerca de su dispositivo de trabajo?

#	Respuestas	Respuestas (%)	Suma
A1	Sí	81,79%	512
A2	No	18,21%	114

ELIGE UNA RESPUESTA

P6. ¿Guarda actualmente las contraseñas relacionadas con el trabajo en un documento en la nube?

#	Respuestas	Respuestas (%)	Suma
A1	Sí	48,90%	489
A2	No	51,10%	511

ELIGE UNA RESPUESTA

P7. ¿Guarda actualmente las contraseñas relacionadas con el trabajo en un documento en su ordenador/escritorio?

#	Respuestas	Respuestas (%)	Suma
A1	Sí	50,60%	506
A2	No	49,40%	494

ELIGE UNA RESPUESTA

P8. ¿Guarda actualmente las contraseñas relacionadas con el trabajo en su teléfono?

#	Respuestas	Respuestas (%)	Suma
A1	Sí	54,70%	547
A2	No	45,30%	453

ELIGE UNA RESPUESTA

P9. ¿Ha compartido alguna vez una contraseña relacionada con el trabajo a través de un mensaje de texto o un correo electrónico?

#	Respuestas	Respuestas (%)	Suma
A1	Sí	38,10%	381
A2	No	61,90%	619

VARIAS RESPUESTAS POSIBLES

P10. ¿Con quién ha compartido sus contraseñas relacionadas con el trabajo durante el último año (elija todas las que correspondan)?

El porcentaje (encuestados) se calcula dividiendo el recuento de cada respuesta por el total de encuestados únicos.

El porcentaje (de respuestas) se calcula dividiendo el recuento de cada respuesta por el recuento total recogido.

#	Respuestas	Encuestados (%)	Respuestas (%)	Suma
A1	Compañeros del mismo equipo	34,40%	18,86%	344
A2	Compañeros de todos los departamentos	13,10%	7,18%	131
A3	Directivos	31,70%	17,38%	317
A4	Equipo directivo	18,50%	10,14%	185
A5	Antiguos compañeros	6,90%	3,78%	69
A6	Pareja o esposo/a	14,40%	7,89%	144
A7	Hijo/-a	7,90%	433%	79
A8	Otro miembro de la familia	10,60%	5,81%	106
A9	Amigo con el que no trabajo	4,70%	2,58%	47
A10	Ninguna de las anteriores	37,60%	20,61%	376
A11	Otra	2,60%	1,43%	26

ELIGE UNA RESPUESTA

P11. ¿Ha entrado alguna vez en una cuenta en línea que pertenece a su anterior empleador después de haberse marchado?

#	Respuestas	Respuestas (%)	Suma
A1	Sí	32,40%	324
A2	No	67,60%	676

ELIGE UNA RESPUESTA

P12. Al crear una nueva contraseña para una cuenta relacionada con el trabajo, ¿ha utilizado el nombre de su empresa?

#	Respuestas	Respuestas (%)	Suma
A1	Sí	36,70%	367
A2	No	63,30%	633

ELIGE UNA RESPUESTA

P13. ¿Comparte su empresa las contraseñas de las cuentas que utilizan varias personas?

#	Respuestas	Respuestas (%)	Suma
A1	Sí	46,10%	461
A2	No	53,90%	539

ELIGE UNA RESPUESTA

P14. ¿Sus contraseñas relacionadas con el trabajo que se comparten entre compañeros incluyen el nombre de la empresa?

#	Respuestas	Respuestas (%)	Suma
A1	Sí	33,80%	338
A2	No	47,20%	472
A3	Esto no es aplicable a mí	19,00%	190

ELIGE UNA RESPUESTA

P15. ¿Utiliza actualmente la misma contraseña para las cuentas personales y las relacionadas con el trabajo?

#	Respuestas	Respuestas (%)	Suma
A1	Sí	43,70%	437
A2	No	56,30%	563

ELIGE UNA RESPUESTA

P16. ¿Alguna de sus contraseñas relacionadas con el trabajo contiene el nombre o el cumpleaños de su pareja?

#	Respuestas	Respuestas (%)	Suma
A1	Sí	34,20%	342
A2	No	65,80%	658

ELIGE UNA RESPUESTA

P17. ¿Alguna de sus contraseñas relacionadas con el trabajo contiene el nombre o el cumpleaños de su hijo?

#	Respuestas	Respuestas (%)	Suma
A1	Sí	31,40%	314
A2	No	52,00%	520
A3	No tengo hijos	16,60%	166

ELIGE UNA RESPUESTA

P18. ¿Sus hijos han entrado alguna vez en sus cuentas o programas relacionados con el trabajo o han accedido a ellos?

#	Respuestas	Respuestas (%)	Suma
A1	Sí	20,60%	206
A2	No	59,40%	594
A3	No tengo hijos	20,00%	200

ELIGE UNA RESPUESTA

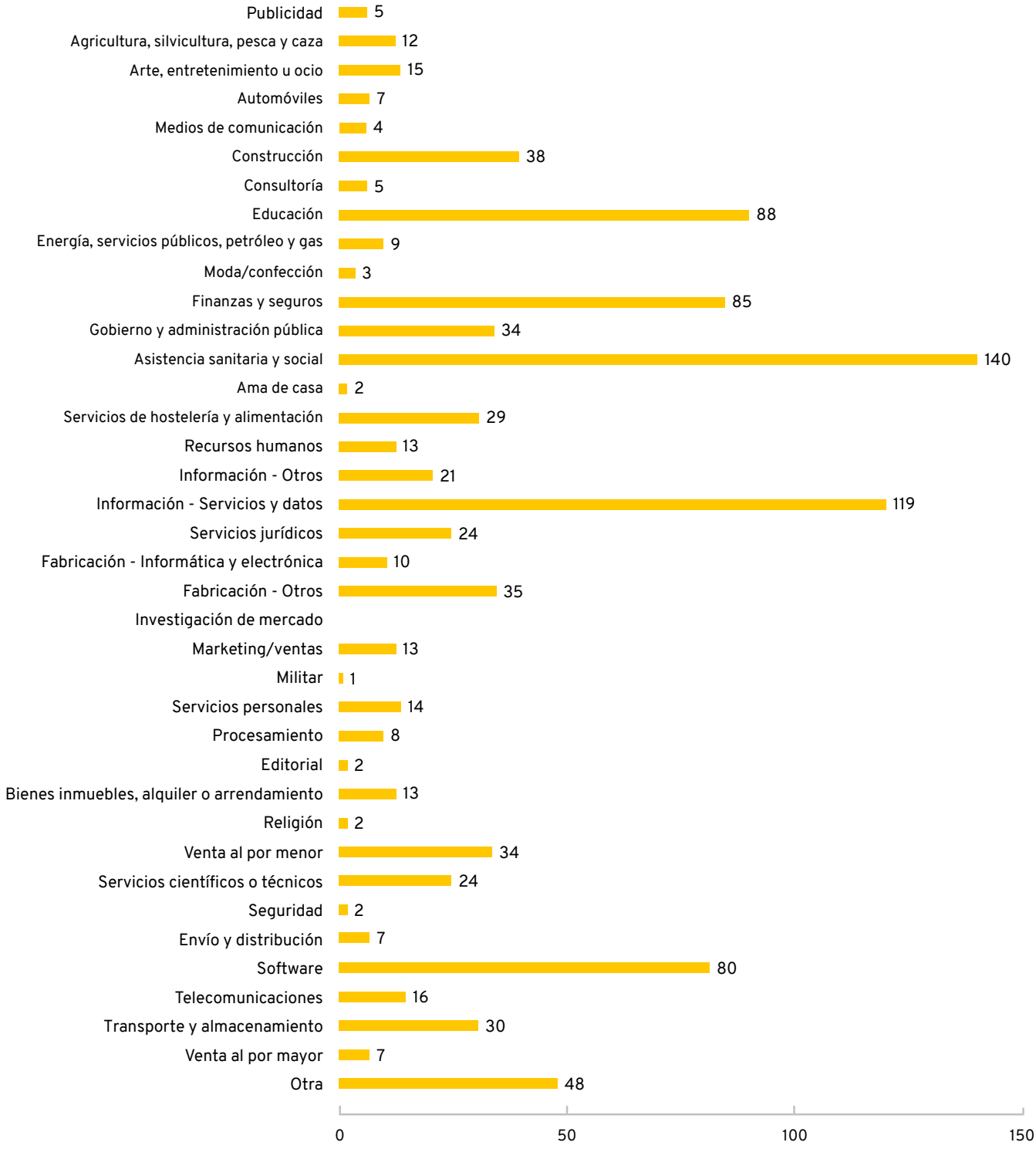
P19. ¿Mantiene cuentas personales protegidas por contraseña en su dispositivo de trabajo?

#	Respuestas	Respuestas (%)	Suma
A1	Sí	53,35%	534
A2	No	46,65%	467

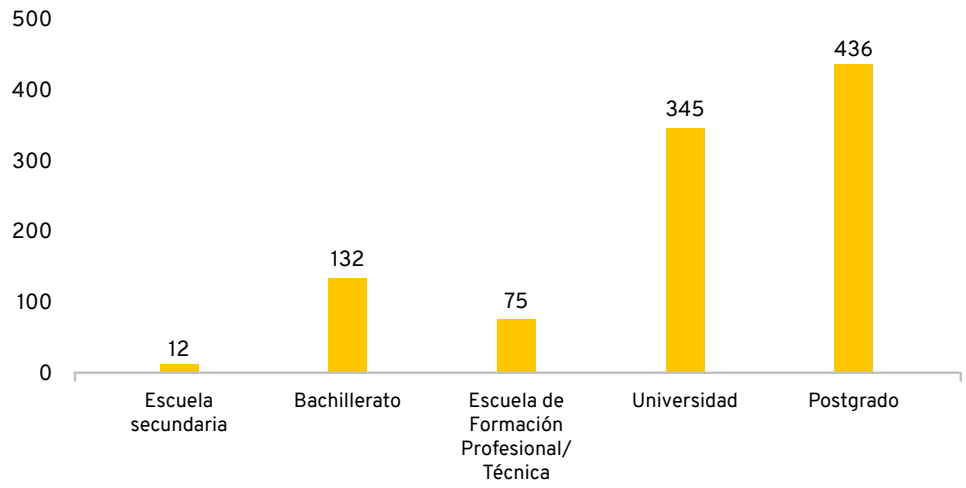
Demografía de la audiencia

Tamaño de la muestra 1000

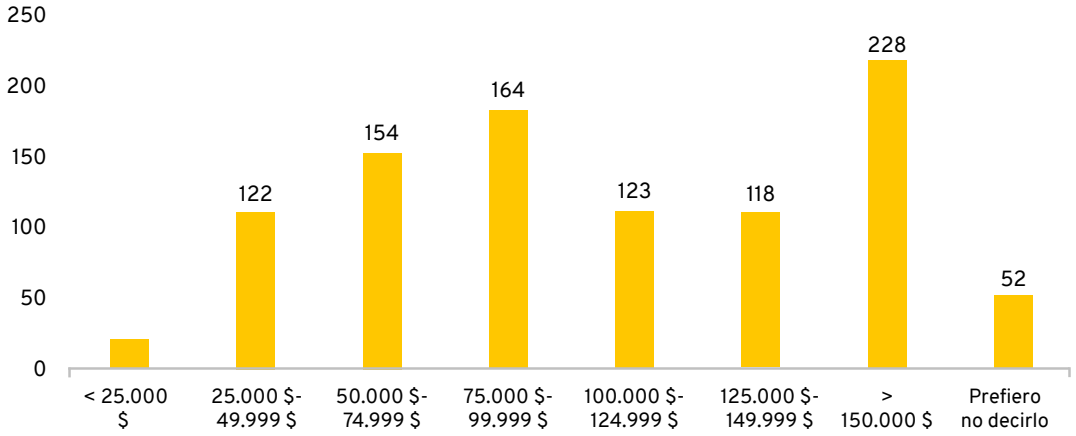
Profesión



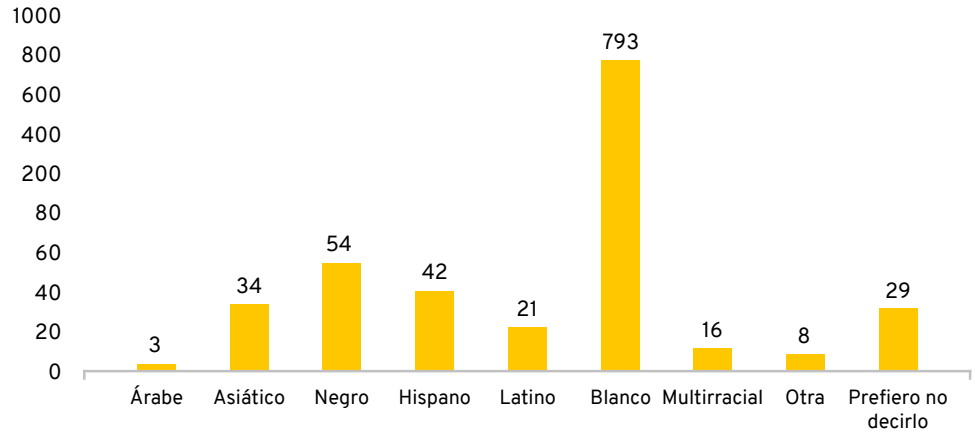
Educación



Ingresos

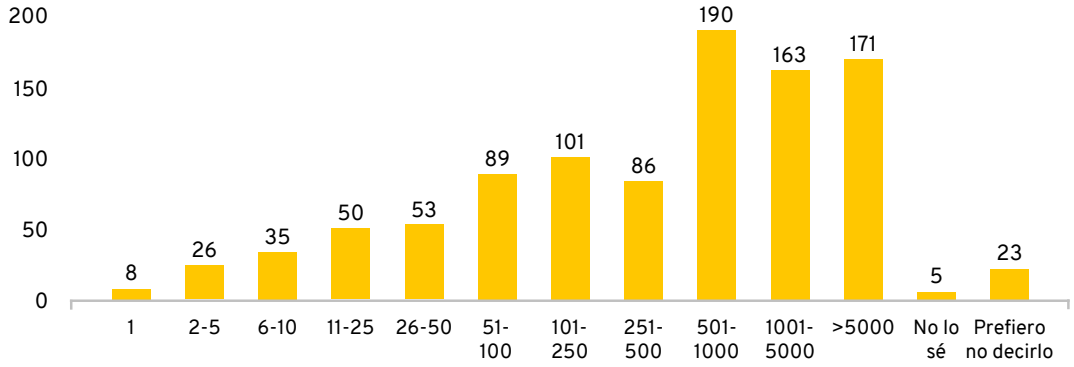


Origen étnico

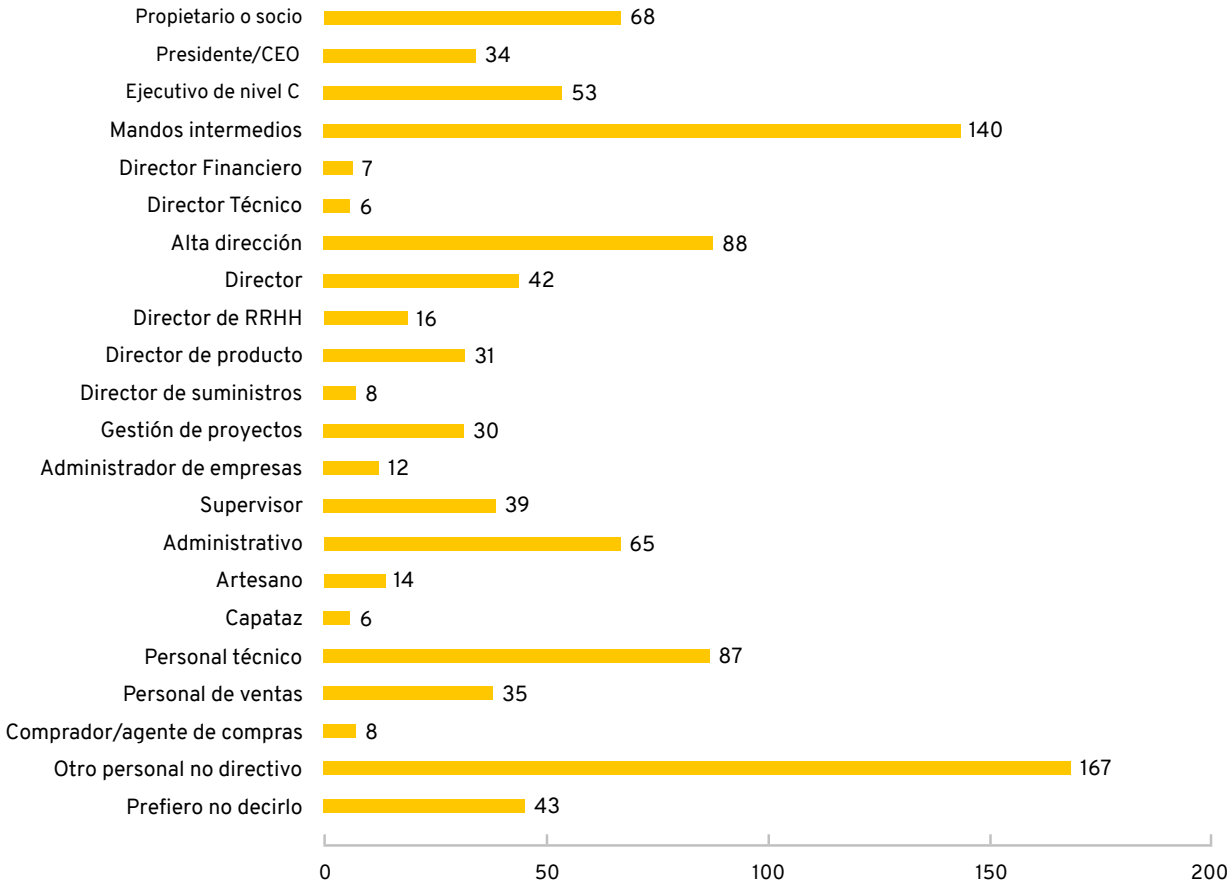


Situación laboral

Número de empleados



Papel en la organización



Lenguas habladas

Clasificaciones y premios

Keeper ha sido nombrado mejor gestor de contraseñas del año y Selección del editor por PC Magazine, Selección del editor por PCWorld durante dos años consecutivos y ha obtenido cuatro premios G2 al Mejor software y cuatro premios InfoSec al Mejor producto de gestión de contraseñas para PYMES y al Mejor producto de ciberseguridad para PYMES. Keeper cuenta con las certificaciones SOC-2 e ISO 27001, y está incluida en la lista para ser utilizada por el gobierno federal a través del Sistema para la Administración de Subvenciones (System for Award Management - SAM).

Gartner peerinsights™

Gartner Peer Insights
4,9 de 5 estrellas

spiceworks

Spiceworks
5 de 5 estrellas

PC PCMAG.COM

Editors' Choice
4,5 de 5 estrellas

G2

2020 Enterprise Leader
4,7 de 5 estrellas

INFOSEC AWARDS WINNERS CYBER DEFENSE MAGAZINE 2019

- **Selección del editor Gestión de contraseñas de ciberseguridad**
- **Director Ejecutivo más vanguardista del Año**

INFOSEC AWARDS WINNER CYBER DEFENSE MAGAZINE 2020

- **Mejor producto para la gestión de contraseñas**
- **Mejor producto para la ciberseguridad de las pymes**
- **Selección del editor como director ejecutivo del año**
- **Director de tecnología más innovador del año**

PC PCMAG.COM EDITORS' CHOICE

PC PCMAG.COM BEST of THE YEAR 2020

Mejor gestor de contraseñas del año y Selección del editor 2019 y 2020

PCWorld EDITORS' CHOICE

Selección del editor 2018 y 2019

G2 Leader WINTER 2021
G2 Leader Enterprise WINTER 2021
G2 Leader Mid-Market WINTER 2021
G2 Leader Small Business WINTER 2021
G2 Leader Europe WINTER 2021
G2 Top 100 Software Products 2020
G2 Top 100 2020
G2 Top 50 2020
G2 Top 50 2020

Para descargar una copia del informe sobre imprudencias en el uso de contraseñas en el trabajo, la infografía y más, visite nuestro **centro de recursos** especializado Para obtener más información sobre Keeper Security o sobre cómo proteger a su organización de las filtraciones de datos relacionadas con las contraseñas, vaya a **keepersecurity.com**.

Metodología

Keeper Security contrató a Pollfish para realizar esta encuesta a 1000 empleados a tiempo completo en Estados Unidos. Sólo se incluyó a las personas que utilizaban contraseñas para acceder a cuentas online relacionadas con el trabajo. La encuesta finalizó en febrero de 2021.

Sobre Keeper Security, Inc.

Sobre Keeper Security, Inc. Keeper Security, Inc. (Keeper) es la plataforma de ciberseguridad patentada y altamente valorada para prevenir las filtraciones de datos y las ciberamenazas relacionadas con las contraseñas. El software de seguridad y encriptación de conocimiento cero de Keeper cuenta con la confianza de millones de personas y miles de empresas de todo el mundo para mitigar el riesgo de robo cibernético, impulsar la productividad de los empleados y cumplir con la normativa. En 2020, Keeper fue nombrado Mejor gestor de contraseñas del año y Selección del editor de PCMag por tercera vez. Keeper también ha sido elegido por los editores de PCWorld y es el ganador de cuatro premios G2 al Mejor Software y del premio InfoSec al mejor producto de gestión de contraseñas para la ciberseguridad de las pymes. Keeper cuenta con las certificaciones SOC-2 e ISO 27001, y también está incluida en la lista para ser utilizada por el gobierno federal a través del Sistema para la Administración de Subvenciones (System for Award Management - SAM).