# REDEFINIENDO La Seguridad De Contraseñas

Por Julia O'Toole
Fundadora & CEO de MyCena Limited

A medida que nuestro mundo se digitaliza cada vez más, nuestra necesidad de contraseñas aumenta. No hace mucho tiempo, podíamos apoyarnos en unas pocas contraseñas. Hoy en día, la mayoría de los usuarios de Internet tendrán más de 100 contraseñas.

Um mundo cada vez mais digital significa que o uso de senhas excederá os 300 bilhões até 2020[1].

A medida que nuestro mundo se digitaliza cada vez más, nuestra necesidad de contraseñas aumenta. No hace mucho tiempo, podíamos apoyarnos en unas pocas contraseñas. Hoy en día, la mayoría de los usuarios de Internet tendrán más de 100 contraseñas.

Y el problema está en aumento. Un informe reciente indica que el uso de contraseñas está aumentando rápidamente y es probable que supere los 300.000 millones para 2020[1].

Este informe describe el panorama de la seguridad de las contraseñas, desde la comprensión de los usuarios sobre el uso de las contraseñas hasta la introducción de una nueva forma de proteger sus contraseñas para que estas puedan protegerle.

1. Cybersecurity Ventures The World Will Need to Protect 300 Billion Passwords by 2020 https://www.inc.com/joseph-steinberg/300-billion-thats-how-many-passwords-may-be-in-use-by-2020.html

## Por qué existen las contraseñas en primer lugar

Las contraseñas son las llaves que abren las puertas de nuestro mundo digital. Así como nuestras llaves abren las puertas de nuestro espacio físico, las contraseñas abren las puertas de nuestro espacio digital. Fueron concebidas como una forma sencilla de demostrar nuestra identidad cuando utilizamos sitios web, cuentas de correo electrónico y aplicaciones. Las contraseñas son de hecho nuestra primera línea de defensa contra los intrusos.

Las contraseñas son las llaves que abren la puerta de entrada a nuestro mundo digital

## Por qué las contraseñas ya no protegen las puertas

Las contraseñas ya no hacen su trabajo. De hecho, un informe de investigaciones de violación de datos de Verizon muestra que el 81% de las violaciones de datos son el resultado de fallas en las contraseñas, ya sea a través de contraseñas débiles, reutilizadas o incluso robadas [1].

## Por qué seguimos usando contraseñas de alto riesgo

Nuestra mayor dependencia de las aplicaciones móviles y web ha provocado un aumento en el número de contraseñas. Desde simples cuentas de correo electrónico hasta banca en línea, nos enfrentamos a cientos de contraseñas que debemos utilizar.

Aunque sabemos que necesitamos usar contraseñas seguras, simplemente no podemos recordar cientos de combinaciones como 45£@fag54hF8sD* para desbloquear cada puerta. Como resultado, tendemos a utilizar combinaciones simples como 'name1234' o a reutilizar una sola contraseña con variaciones.

10% de las personas han usado al menos una de las 25 peores contraseñas

### Las diez peores contraseñas de 2018

La lista anual de SplashData de las peores contraseñas del año2 revela que los usuarios de ordenadores siguen utilizando las mismas contraseñas predecibles y fáciles de adivinar, a pesar del riesgo significativo de ser pirateados y de que les roben sus identidades. Casi el 10% de las personas han usado al menos una de las 25 peores contraseñas de la lista de este año, y casi el 3% han usado la peor contraseña, 123456.

1. 123456
2. password
3. 123456789
4. 12345678
5. 12345
6. 111111
7. 1234567
8. Sunshine
9. Qwerty
10. iloveyou

Además de esto, la mayoría de nosotros utilizamos regularmente los siguientes métodos inseguros para almacenar contraseñas [3] :

- 53% Memoria humana
- 32% Guardadas en el navegador
- 26% Hojas de cálculo
- 26% Escritas
- 1% Otros


Tener una contraseña débil es como no tener ninguna contraseña.

1. Verizon Data Breach Investigations Report https://www.verizondigitalmedia.com/blog/2017/07/2017-verizon-data-breach-investigations-report/
2. SplashData's Top 100 Worst Passwords of 2018 https://www.teamsid.com/splashdatas-top-100-worst-passwords-of-2018/
3. Cyber Security Breaches Survey 2018 from the Department for Digital, Culture, Media and Sport https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/702074/Cyber_Security_Breaches_Survey_2018_-_Main_Report.pdf

# Por qué las contraseñas son una gran amenaza para las empresas

## Cómo operan los hackers

Para entender por qué las contraseñas son una amenaza para la seguridad, es importante entender cómo operan los hackers.

- Phishing – los hackers pueden hacerse pasar por contactos genuinos, por ejemplo bancos, para convencer a los usuarios de que entreguen sus credenciales.
- Ingeniería social - los hackers extraen información de su perfil en línea y actividades para robar su identidad.
- Relleno de credenciales - los hackers suelen utilizar nombres de usuario y contraseñas de cuentas robadas de una violación de datos para intentar abrir otras cuentas utilizando herramientas de automatización web.
- Fuerza bruta - los hackers ejecutan scripts para probar combinaciones de credenciales para "adivinar" su contraseña.

Una alternativa llamada "spidering" es cuando los hackers estudian una compañía y aprenden su idioma. Por lo general, se dirige a las grandes empresas que disponen de mucha información sobre sí mismas en línea. A menudo se utiliza para acceder a contraseñas Wi-Fi, ya que muchos routers de oficina están protegidos por una contraseña que se refiere a la empresa, como 'Company1234'.

Más del 90% de los ataques son ejecutados por bots, que "rellenan" o "disparan" combinaciones probadas y nuevas. Estos robots utilizan credenciales filtradas e información de perfil de medios sociales para "adivinar" más rápido. La mayoría de las contraseñas pueden ser descifradas en 24 horas usando una herramienta de fuerza bruta que puede ser descargada gratuitamente.

Necesitas saber cómo piensa un hacker para evitar que te pirateen.

Las colecciones #2-5 representan 845 gigabytes o 2.200 millones de credenciales robadas, incluyendo nombres de usuario y contraseñas.

## Por qué la transformación digital aumenta las vulnerabilidades

Mientras que más del 60% de las empresas de Fortune 500 han pasado por una transformación digital, lo que ha permitido una mano de obra más colaborativa, por otra parte, sus redes conectadas también se han convertido en el sueño de todo hacker. Su superficie de ataque ahora es toda la fuerza laboral. Desde los jefes ejecutivos hasta los empleados subalternos, cualquier persona que esté conectada al sistema es vulnerable a los ataques cibernéticos y representa un riesgo potencial.

Mientras tanto, la necesidad de los usuarios de negocios de tener más y más cuentas significa que son más propensos a reutilizar contraseñas en múltiples cuentas, lo que aumenta su riesgo de ser hackeados. Por otro lado, las empresas que utilizan la comodidad del Single Sign On (SSO) son vulnerables a que los hackers rompan sus redes de información y bases de datos desde un único punto de acceso.

Por lo tanto, no es una sorpresa que los robos de credenciales estén en aumento. 2018 fue el peor año en el que se han registrado más violaciones de la seguridad cibernética. Esto fue seguido por dos de las mayores filtraciones de nombres de usuario y contraseñas de la historia, llamadas Collection#1[1] y Collections #2-5[2] en enero de 2019. Actualmente hay más de 3.000 millones de nombres de usuario y contraseñas a la venta en línea y esta cifra sigue aumentando cada día.


Sus contraseñas son vulnerables al relleno de credenciales, phishing, ingeniería social

1. Forbes https://www.forbes.com/sites/kateoflahertyuk/2019/01/17/collection-1-breach-how-to-find-out-if-your-password-has-been-stolen/#3c2d829a2a2e
2. Wired https://www.wired.com/story/collection-leak-usernames-passwords-billions/

## Por qué las nuevas leyes de protección de datos afectan a todas las empresas

Desde pequeñas empresas hasta grandes corporaciones, todas las empresas de cualquier sector necesitan contraseñas sólidas para proteger sus datos y los de sus clientes.

Con la entrada en vigor en todo el mundo de leyes de protección de datos como GDPR, las consecuencias financieras de no proteger los datos y la privacidad de los clientes pueden ser devastadoras, ya que las empresas están sujetas a multas de hasta 20.000.000 € o el 4% de su volumen de negocios global total.

Los ataques de araña consisten en el estudio de una empresa y la adquisición de su idioma, por ejemplo, empresa1234

## El riesgo de ser un "pez gordo"

La industria de la piratería informática está compuesta por una amplia gama de actores, desde criminales poco sofisticados hasta Estados-nación. Mientras que algunos hackers lanzan su red a gran escala, otros se concentran en objetivos de mayor valor en sectores más estratégicos.

Las infracciones en sectores como la defensa, la policía, el gobierno, la energía, el agua, los servicios públicos, las infraestructuras, la tecnología, las telecomunicaciones, las universidades, la banca, los servicios financieros, la asistencia sanitaria, los productos farmacéuticos, el transporte, la logística, el comercio minorista o la legislación pueden tener efectos devastadores.

En mayo de 2017, el ataque de rescate de WannaCry llevó a la cancelación de 19.000 operaciones y citas médicas en el Reino Unido, lo que costó 92 millones de libras esterlinas al Servicio Nacional de Salud (NHS) por la interrupción de los servicios e IT[1]. Y en septiembre de 2019, casi toda la población de Ecuador tuvo una filtración de sus datos personales[2].

La ya desaparecida empresa Nortel fue objeto de un ataque que duró años y que se remonta a hackers patrocinados por el Estado en China.

Cuando un "pez gordo" es atacado, inevitablemente también afecta a los proveedores, socios y clientes. En marzo de 2019, una violación de datos de Citrix podía afectar el acceso a la red privada virtual y las credenciales de 400.000 empresas en todo el mundo, incluido el 98% de las organizaciones de Fortune 500[3].

En la era de la guerra cibernética, ha habido evidencia abrumadora de que algunos ataques son patrocinados por el estado. Países como Corea del Norte, Irán y China son conocidos por llevar a cabo ciberataques y robos de propiedad intelectual.

Por ejemplo, la ya desaparecida empresa canadiense de telecomunicaciones Nortel fue objeto de un ataque que duró años, en el que los hackers robaron las contraseñas de los altos ejecutivos para acceder a correos electrónicos, investigaciones, planes de negocios y secretos comerciales. Posteriormente, los ataques fueron rastreados hasta hackers patrocinados por el Estado en China[4].

## Las empresas no siempre se dan cuenta de que se ha producido una violación.

Muchas empresas no reconocen una violación de la seguridad cibernética cuando se produce, y el 93% de las violaciones de datos no se descubren durante semanas[5].

Las brechas de datos pueden pasar semanas sin ser descubiertas

Durante ese tiempo se puede hacer una gran cantidad de daño. Los hackers pueden instalar malware en el ordenador de un empleado que puede extraer información confidencial de la red de la empresa antes de que la empresa se dé cuenta de que su seguridad ha sido violada.

1. Department of Health and Social Care https://www.hsj.co.uk/technology-and-innovation/cyber-attack-cost-nhs-92m-dhsc/7023560.article
2. The New York Times https://www.nytimes.com/2019/09/17/world/americas/ecuador-data-leak.html
3. Forbes https://www.forbes.com/sites/kateoflahertyuk/2019/03/10/citrix-data-breach-heres-what-to-do-next/#47a1e6b11476
4. The Register https://www.theregister.co.uk/2012/02/15/nortel_breach/
5. Verdict https://www.verdict.co.uk/password-security-surveillance-fears/

## ¿Su empresa se toma en serio la ciberseguridad?

Las empresas pueden tener buenas intenciones, pero esto no siempre se refleja en sus prácticas. El 74% de las empresas y el 53% de las organizaciones benéficas afirman que la ciberseguridad es una prioridad para la alta dirección de su organización. Sin embargo, a pesar de esto, todavía vemos:

- Solo el 27% de las empresas y el 21% de las organizaciones benéficas tienen una o varias políticas formales de ciberseguridad1.
- Solo el 9% de las empresas y el 4% de las organizaciones benéficas cuentan con una póliza de seguro de ciberseguridad.

## Equilibrio entre la prevención, el control y la reparación

Con más y más ataques cada día, la pregunta no es si su negocio será atacado, sino de cuándo. Existe una creciente presión sobre los CISOs para mitigar cada vez más riesgos con recursos limitados. Aproximadamente el 99% del gasto en ciberseguridad de las empresas se destina actualmente a la supervisión y reparación. Sin embargo, ni siquiera los mejores sistemas de supervisión y vigilancia protegen su empresa del robo de contraseñas.

Mientras que el 80% de los riesgos están relacionados con las contraseñas, la gestión de contraseñas solo representó el 0,53% del gasto total en ciberseguridad en 2017, una cifra que se prevé que aumente a sólo el 0,58% en 20232. Para ayudar a proteger a su personal, clientes y comunidades más amplias de las amenazas a la seguridad, las empresas necesitan priorizar la prevención y organizar mejor su primera línea de defensa.

## Cómo evitar que las contraseñas le hagan vulnerable

Un primer paso sería establecer un sistema de gestión de acceso a la identidad (IAM) que permita a los administradores asignar diferentes niveles de acceso para diferentes usuarios dentro de una organización. Esta puede no ser la primera consideración para las empresas más pequeñas, en particular las que no tienen un CISO.

Un segundo paso sería establecer un sistema de administración de contraseñas que sea conveniente y seguro para evitar que las personas usen contraseñas débiles o reutilizadas. Muchas empresas fracasan en esta área porque tienen un sistema de contraseñas defectuoso, lo que aumenta el riesgo de ataques.

En su informe, SplashData ofrece a las empresas los siguientes consejos para protegerse de los piratas informáticos:

- Utilizar frases de contraseña de doce caracteres o más con tipos mixtos de caracteres.
- Utilizar una contraseña diferente para cada uno de sus inicios de sesión, de modo que si un hacker obtiene acceso a una de sus contraseñas, no podrá utilizarla para acceder a otros sitios.
- Proteger sus activos y su identidad personal utilizando un administrador de contraseñas para organizar las contraseñas, generar contraseñas aleatorias seguras e iniciar sesión automáticamente en los sitios web.

1. Cyber Security Breaches Survey 2018 from the Department for Digital, Culture, Media and Sport https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/702074/Cyber_Security_Breaches_Survey_2018_-_Main_Report.pdf
2. Stratistics MRC https://www.strategymrc.com/report/password-management-market-2017 https://www.strategymrc.com/report/cyber-security-market https://www.strategymrc.com/report/cyber-security-market-2016; MyCena estimates

## Comprender los riesgos asociados con los administradores de contraseñas centralizados basados en la nube

Al ofrecer un método centralizado de almacenamiento de contraseñas, los administradores de contraseñas basados en la nube se han vuelto cada vez más populares en los últimos años. Esto se debe en gran medida a que:

- Le ayudan a generar contraseñas seguras: solo necesita recordar una contraseña maestra única. Escriba su contraseña maestra y obtenga acceso a todas las demás contraseñas que están almacenadas en la nube.
- Proporcionan una alternativa mucho más segura que el uso de post-its o contraseñas débiles como 123456.

Aunque los administradores de contraseñas basadas en la nube pueden ser convenientes, existen tres riesgos principales asociados con su arquitectura:

- En primer lugar, por construcción, todas sus contraseñas están centralizadas y se accede a ellas a través de una contraseña maestra, que se convierte en un único punto de vulnerabilidad. Imagine que si esa contraseña maestra se ve comprometida de alguna manera, usted expone todas sus contraseñas a la vez. Puede pensar en una contraseña maestra como la llave de un gerente de hotel. Un hacker solo necesita esta llave para acceder a todas las habitaciones. Para muchas empresas, este no es un riesgo que puedan asumir.
- En segundo lugar, todas sus contraseñas están en la nube, centralizadas, en la misma cesta que millones de contraseñas de otros usuarios. Esto hace que se convierta en un enorme imán para los hackers, que son atraídos como abejas a un tarro de miel y harán todo lo posible para entrar y robar el banco.
- Tercero, los servidores pueden ser violados, ya sea a través de contraseñas u otras vulnerabilidades. ¿Dejarías las llaves físicas de tu casa con alguien que no conoces? ¿Entonces por qué haces eso con tus llaves digitales? Dejarlas en la nube es precisamente eso.

Un gestor de contraseñas basado en la nube es práctico pero arriesgado


Su contraseña maestra es como la llave del reino

## Redefinir las reglas de seguridad de las contraseñas

Un problema bien definido es un problema que está resuelto a medias. Para encontrar una solución, necesitábamos romper el problema desde cero y repensar las reglas que permitían que las contraseñas cumplieran su función como su primera capa de seguridad. Encontramos tres reglas clave:

- Las contraseñas son como llaves. Del mismo modo que no es necesario que recuerde cómo cortar las llaves cada vez que quiera abrir una puerta, tampoco es necesario que recuerde sus contraseñas para abrir sus puertas digitales.
- Las contraseñas deben ser privadas por naturaleza y solo accesibles por su propietario y nadie más.
- Las contraseñas no deben ser vulnerables en un solo punto de acceso.

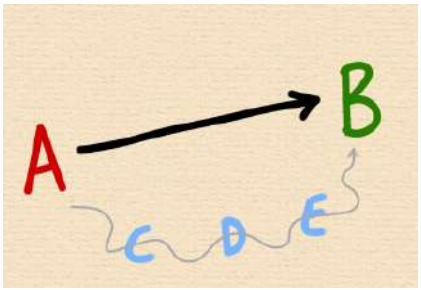
Redefinir las reglas de seguridad de las contraseñas

## Lecciones de la neurociencia: entendiendo la conveniencia

Para lograr la adopción y el uso de cualquier nueva tecnología, la conveniencia es clave. Esa regla se aplica a la seguridad. Si se tarda demasiado tiempo en abrir una puerta varias veces al día, la mayoría de las personas dejarán de cerrarla correctamente. Por lo tanto, la seguridad solo puede garantizarse si los sistemas y procedimientos que la proporcionan pueden aplicarse sin problemas.

En los últimos veinte años, la neurociencia nos ha enseñado mucho sobre cómo funciona nuestro cerebro. Un hallazgo clave es que nuestro cerebro tiende a volver al camino más fácil para viajar de A a B. He aquí algunos ejemplos:

- Cuando se trata de encontrar un objeto, es mucho más eficiente que el cerebro recuerde un lugar típico donde normalmente se pone ese objeto en lugar de recordar con precisión dónde está el objeto.
- Es más fácil para el cerebro seguir patrones conocidos o reconocibles que crear otros nuevos. Eso explica por qué el cerebro no es tan bueno creando nuevas contraseñas aleatorias.
- Nuestro cerebro es visual y tiende a emparejar lo que está buscando con objetos y patrones vistos anteriormente.



El cerebro tiende a volver al camino más fácil

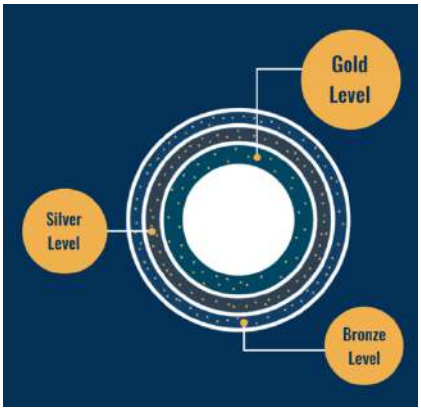
# Hacer que las contraseñas vuelvan a funcionar

Una vez definido el problema, nos queda resolverlo.

## Método de acceso a datos almacenados estructurados (datos MASS) internacional pendiente de patente

Los datos MASS son una solución innovadora que permite localizar y descentralizar las contraseñas, distribuyendo y reduciendo así el riesgo de perderlo todo de una vez. Permite la creación de múltiples niveles de seguridad para almacenar contraseñas dependiendo de su sensibilidad, con autenticación local multinivel y control total por parte del usuario de contraseñas y configuraciones de seguridad.

- No hay almacenamiento de nubes.
- Sin contraseña maestra.
- No hay un solo punto de vulnerabilidad.



Datos MASS: bóveda local de contraseñas de varias capas dentro de su dispositivo

## La conveniencia ideal para una seguridad ideal

La ciberseguridad es responsabilidad de todos. Para que sea ampliamente adoptada, la solución tiene que ser rápida, conveniente y fácil de usar.

- Permita que el propietario de las contraseñas demuestre su identidad de forma fácil y segura en cada nivel para acceder a sus contraseñas en cualquier momento y en cualquier lugar con una combinación de huella dactilar, identificador facial, PIN, patrón de bloqueo y frase de contraseña de voz.
- Generar contraseñas seguras de forma predeterminada.
- Permite buscar, copiar y pegar contraseñas sin tener que escribir, volver a escribir o ver una contraseña determinada.

La comodidad es la clave: cree, guarde, busque, encuentre, copie y pegue contraseñas en cuestión de segundos.

## Creación de una solución de nivel empresarial

Para adaptarse al entorno empresarial, la solución debe ser fácilmente desplegada y utilizada. Viene en dos partes:

- Una consola a través de la cual un gerente puede incorporar rápidamente a todos los empleados, fortalecer y supervisar las políticas de contraseñas, como la configuración de la longitud de la contraseña, la frecuencia de cambio de contraseña y las alertas de contraseña débil.
- Una aplicación móvil que los empleados utilizan para acceder a sus contraseñas de forma rápida y segura, que incluye funciones como multidispositivo, multiplataforma, integración de escritorio, modo de viaje, sincronización, migración, recordatorios de copias de seguridad automatizadas y uso compartido seguro de contraseñas.

Una consola permite a los administradores reforzar las políticas de contraseñas y supervisar el cumplimiento de las mismas.

## Respetar la privacidad por defecto

Después de muchos años de deterioro de la privacidad, los legisladores han fortalecido las leyes de privacidad para salvaguardar nuestras sociedades y las libertades individuales. Apoyamos profundamente esa tendencia. De hecho, nuestra solución está construida con privacidad por defecto.

Las contraseñas se cifran dentro del dispositivo mediante el cifrado AES-SHA 256. Esto significa que incluso si pierde su dispositivo, un ladrón no podrá acceder a sus contraseñas. La única persona que puede recargar su copia de seguridad de contraseñas encriptadas es usted.

Sus datos biométricos, como las huellas dactilares y la identificación facial, son aún más sensibles. Puede cambiar una contraseña, pero no puede cambiar su cara o su dedo. Por lo tanto, toda la autenticación personal se mantiene dentro de su dispositivo local, sin un repositorio central de datos biométricos en la nube para que nadie los robe.

Privacidad por defecto: No volver a ver o escribir nunca más una contraseña

## Limitar los daños causados por el phishing

También es posible que no tenga que volver a ver una contraseña. Esto significa que, desde la creación de sus contraseñas hasta el uso de sus contraseñas a través de "copiar y pegar", nunca tiene que haber un momento en el que tenga que mostrar o escribir sus contraseñas, lo que limita las posibilidades de cometer errores de escritura o de que alguien husmee detrás de usted y le robe sus contraseñas.

Incluso si un hacker logra engañarlo para que pegue una contraseña en su sitio falso, robándola así, esa contraseña no puede ser reutilizada para ingresar a otras cuentas, ya que cada una de sus contraseñas son únicas y todas son fuertes. Por lo tanto, toda su red no está expuesta a ningún tipo de robo.

## Actuar como su primera línea de defensa

Una vez que la solución se despliega dentro de una organización, se convierte de hecho en su primera línea de defensa. Para entrar en cualquier aplicación o red protegida por contraseña dentro de una empresa, un empleado deberá primero probar su identidad en su propio dispositivo. Solo entonces podrán acceder a la contraseña segura y única que buscan. Esa contraseña fuerte y única probará entonces que el empleado tiene el derecho (porque tiene la clave única) de acceder a esa aplicación o red.


Actuar como su primera línea de defensa


Descubra las soluciones de seguridad de contraseñas descentralizadas de MyCena

## Descubre MyCena

MyCena Business Fortress es una revolucionaria solución de seguridad de contraseñas de nivel empresarial que es descentralizada, fácil de implementar, conveniente y segura. Aprenda a instalar y configurar MyCena fácilmente para su empresa.

MyCena Personal Fortress es una revolucionaria aplicación de seguridad de contraseñas personales que los usuarios individuales pueden descargar en sus dispositivos móviles. Aprenda a proteger sus contraseñas con MyCena Personal Fortress.

## MyCena como servicio

MyCena as a Service (MaaS) es un paquete de servicios completo que ofrece lo mejor de la solución con soporte avanzado, reduciendo el esfuerzo para implementar y administrar la solución dentro de la empresa y sus empleados.

## Puntos clave para recordar

La ciberseguridad es la principal amenaza para las organizaciones. El número de violaciones de datos aumenta día a día, cada una de las cuales trae consigo multas, acciones legales y remedios, al tiempo que daña irreversiblemente la reputación de la empresa y la confianza de los clientes.

Para proteger a sus empresas, los consejos de administración y los altos ejecutivos deben comprender de dónde provienen las amenazas y tomar medidas decisivas. Como el 81% de las infracciones comienzan con las contraseñas, la protección con contraseña ya no es solo una opción, es un imperativo.

Los CISOs de las empresas pueden mitigar los riesgos dirigiendo y ayudando a sus empleados a utilizar contraseñas únicas y sólidas como primera línea de defensa y descentralizando el almacenamiento de contraseñas con MyCena Business Fortress. Los CIOs también pueden mitigar los riesgos de violación de datos aprovechando MyCena como un servicio.

Para cualquier consulta, póngase en contacto con
support@MyCena.co

Visite nuestro sitio web para más información
Prueba gratuita disponible
https://MyCena.co

Descarga desde la Appstore o Google Play.