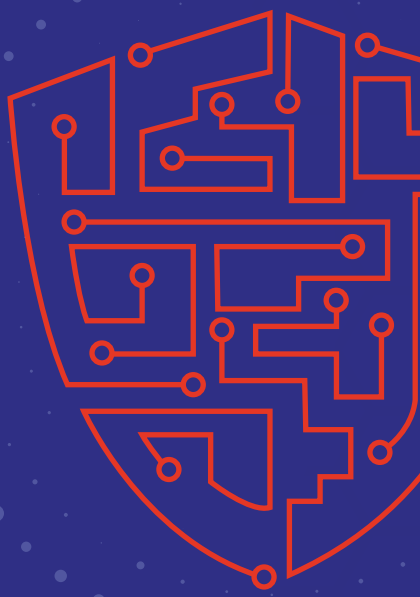
ManageEngine
Password Manager Pro

Documento de políticas de seguridad



www.passwordmanagerpro.com

Introducción

ManageEngine diseña soluciones de gestión de TI para ayudar a decenas de millones de administradores de TI en todo el mundo a abordar de forma proactiva sus desafíos de TI. Nuestros clientes recurren a nosotros para mejorar su postura de seguridad, y damos la máxima prioridad a mantener los datos de nuestros clientes seguros y privados, lo que se refleja en nuestros productos, cultura interna y procesos. Este documento explora nuestros procesos de seguridad a nivel de organización y de producto. Haga clic aquí para ver nuestra política de seguridad detallada.

Saltar a la seguridad del producto >>

Cumplimiento estricto de la higiene de la seguridad

Nuestros equipos de seguridad, del centro de control de red (NOC) y de privacidad, se dedican a desarrollar e implementar un riguroso marco de seguridad que incluye la educación y formación periódicas de los empleados, la creación y el mantenimiento de nuestros sistemas de defensa, la optimización de los procesos de revisión de la seguridad en todos los equipos y departamentos internos, y el monitoreo constante de nuestras redes corporativas para detectar y mitigar las actividades sospechosas.

Proceso de respuesta y gestión de incidentes

En ManageEngine, tenemos un equipo dedicado a la gestión de incidentes para monitorear, supervisar y responder a los incidentes en tiempo real. Nuestro equipo tiene como objetivo detectar y responder a los incidentes con las medidas correctivas adecuadas siempre que sea posible.

En caso de incidente, proporcionamos a nuestros clientes un extenso informe, que responde al qué, quién, cómo y cuándo del incidente de seguridad, acompañado de información esencial sobre nuestro proceso de respuesta. Además, proporcionamos detalles sobre las medidas que aplicaremos para evitar que se repita el incidente.

Para informar de cualquier incidente de seguridad y privacidad, puede escribirnos a incidents@zohocorp.com, y lo abordaremos inmediatamente.

Notificación de violación

Como responsables del tratamiento de datos, notificaremos a todos los organismos de protección de datos afectados por una violación de datos en un plazo de 72 horas desde que tengamos conocimiento de dicha violación, tal y como lo exige el Reglamento General de Protección de Datos (GDPR). También notificamos debidamente a nuestros clientes cuando lo requieran, en función de los requisitos específicos. Como procesador de datos, notificaremos los incidentes a los responsables del tratamiento de datos afectados lo antes posible. En el caso de los incidentes relacionados con un usuario o una organización específica, lo notificaremos al interesado a través de su correo electrónico profesional. En cuanto a los incidentes generales, notificaremos a nuestros usuarios a través de correos electrónicos, blogs, foros y redes sociales informándoles del incidente y, si es necesario, de las siguientes medidas correctivas a ejecutar.

Gestión de la vulnerabilidad: Corrección de la seguridad, versiones y proceso de aplicación de parches

Para garantizar una seguridad estricta, el Centro de Respuesta de Seguridad de ManageEngine (MESRC) utiliza una combinación de herramientas internas y de terceros para identificar las vulnerabilidades de seguridad o los bugs (listados en CVE o reportados en las redes sociales) en nuestros productos, redes corporativas, endpoints, bases de datos y otros activos. Las vulnerabilidades identificadas y notificadas que requieren una reparación oportuna se registran y se priorizan según su gravedad. Además, llevamos a cabo exhaustivas evaluaciones de riesgo, pruebas de comprobación de vulnerabilidad y mitigamos todos los sistemas vulnerables proporcionando las correcciones y las versiones de parches adecuadas en nuestras versiones de seguridad. Más información.

Divulgación responsable

Practicamos una seguridad de TI proactiva y colaborativa

Además de reforzar nuestra rutina de seguridad, agradecemos a nuestros clientes, socios y entusiastas de la seguridad que nos hagan llegar sus inquietudes al respecto, lo que nos ayuda a estar al tanto de las amenazas a la seguridad. Trabajamos constantemente con especialistas e investigadores del sector para mantenernos al corriente de los últimos avances en materia de seguridad, aprovechando esta experiencia colectiva para crear productos de seguridad de TI a prueba de errores.

Nuestro programa de notificación de vulnerabilidades, Bug Bounty, se compromete a trabajar con la comunidad de seguridad para identificar, verificar y aplicar los controles y parches adecuados a las vulnerabilidades notificadas. Si ha descubierto un posible problema de seguridad en nuestra línea de productos, notifíquelo a https://bugbounty.zoho.com/, o escríbanos directamente a security@zohocorp.com.

Una vez que se notifica una vulnerabilidad, el MESRC, junto con los expertos en productos, investiga la validez, los riesgos y la gravedad asociados a las vulnerabilidades notificadas y aplica las medidas correctivas a nuestros usuarios en forma de correcciones de errores (bugs), paquetes de actualización y parches de seguridad.

Password Manager Pro: Resumen general

Password Manager Pro se ocupa de las contraseñas administrativas que ofrecen un acceso seguro a las credenciales y dispositivos de la empresa. Cualquier acción comprometedora en la seguridad de estas contraseñas expondrá a las organizaciones a graves riesgos. Por lo tanto, hemos diseñado Password Manager Pro para ofrecer la máxima seguridad, incluso durante la instalación de la aplicación, la autenticación del usuario, la transmisión de datos, el almacenamiento y el uso regular.

Seguro por diseño

Nuestro modelo de ciclo de vida de desarrollo de software (SDLC) obliga a nuestro equipo de ingenieros de Password Manager Pro a cumplir estrictamente nuestras normas de codificación segura, que incluyen el siguiente marco de evaluación de la seguridad y los pasos para identificar y sortear cualquier posible fallo de seguridad:

Marco de seguridad

Ciclo de vida de desarrollo de software

Análisis y diseño	Desarrollo	Control de calidad/ lanzamiento
Recopilar y analizar los requisitos para identificar cualquier fallo o brecha de seguridad. Preparar un plan de evaluación de la vulnerabilidad para abordar los problemas de seguridad planteados por los usuarios y los analistas de seguridad en las versiones anteriores. Desarrollar un prototipo de producto o función que incluya los cambios, y someterlos a la autoridad de gestión de cambios para su aprobación.	Pruebas unitarias continuas de las nuevas funciones y módulos desarrollados para garantizar que se ajusten a los requisitos del usuario y a la lógica empresarial principal. Someter las dependencias de código de terceros y las bibliotecas a pruebas de vulnerabilidad antes de utilizarlas para garantizar que sean seguras.	Realizar pruebas de integración, automatización y penetración para garantizar que las nuevas funciones o módulos sean seguros frente a posibles vulnerabilidades/fallas. Pruebas de humo continuas para garantizar que la funcionalidad principal del producto permanezca intacta sin abrir nuevas brechas de seguridad. Generar informes de evaluación de la seguridad para identificar nuevas áreas de mejora. Ejecutar análisis continuos de vulnerabilidad después del lanzamiento para la identificación oportuna y la aplicación de parches a las vulnerabilidades.

- Nuestro repositorio e infraestructura de compilación de versiones están protegidos con el protocolo SSH/HTTPS y se encuentran en una red segmentada segura con controles de acceso y autenticación estrictos.

- Nuestros marcos de seguridad y de código son compatibles con OWASP y se implementan en la capa de aplicación.

- Todas las actualizaciones y nuevas funciones de Password Manager Pro están sujetas a políticas internas de gestión de cambios y a evaluaciones periódicas de vulnerabilidad, y los cambios se implementan en producción sólo si los aprueban las autoridades de gestión de cambios y seguridad correspondientes.

- Todos los cambios de código, las dependencias de terceros, los paquetes de lanzamiento y los paquetes de actualización se someten a múltiples niveles de revisión de seguridad interna, esfuerzos de automatización y pruebas de penetración, y análisis de vulnerabilidad para garantizar que estén bien protegidos de los errores lógicos y los problemas de seguridad.

- Los binarios se firman con un certificado de firma de código y la clave privada se almacena de forma segura en la red segmentada con acceso limitado.

- Cada actualización y nueva función de Password Manager Pro está sujeta y se rige por una política interna de gestión de cambios, que autoriza el cambio solicitado antes de implementarlo en producción.

- El equipo de ingenieros de Password Manager Pro trabaja estrechamente con los equipos de seguridad internos para obtener sus comentarios y retroalimentación e identificar áreas de mejora en términos de fortalecimiento de nuestra postura de seguridad.

Además de las medidas de seguridad mencionadas, nos esforzamos continuamente por hacer que la aplicación sea más segura. La siguiente sección proporciona detalles completos sobre las especificaciones de seguridad de ManageEngine Password Manager Pro.

Password Manager Pro: Especificaciones de seguridad

Password Manager Pro protege los datos a varios niveles y se clasifica en las siguientes categorías:

Especificaciones de seguridad	
1. Mecanismo de bóveda y cifrado	• Cifrado AES-256 • Doble cifrado: primero en la aplicación y luego en el nivel de la base de datos • La clave de cifrado y los datos cifrados no pueden residir juntos • Modo compatible con FIPS 140-2 • SafeNet Luna PCIe HSM • Criptografía personalizada • Arquitectura multi instancia (versión MSP)

2. Identificación y autenticación	**Autenticación a nivel de aplicación** • Integración con almacenes de identidades como Microsoft AD, Azure AD, cualquier servicio de directorio compatible con LDAP, Azure AD y RADIUS • Mecanismo de autenticación local mediante el algoritmo SHA2 (SHA512) • Restablecimiento forzoso de la contraseña para la autenticación local • Autenticación con smart card • Inicio de sesión único SAML 2.0 **Autenticación de dos factores** • PhoneFactor • RSA SecurID • Una contraseña única enviada por email • Google Authenticator • RADIUS Authenticator • Microsoft Authenticator • Okta Verify • Duo Security • YubiKey
3. Seguridad e integridad de los datos	**Transmisión de datos** • Cifrada y a través de HTTPS • Modo SSL para las conexiones de los clientes **Restablecimiento remoto de la contraseña** • Restablecimiento remoto automático y programado de la contraseña para más de 70 tipos de recursos • Restablecimiento remoto de la contraseña mediante agentes • Restablecimiento de la contraseña de la cuenta de servicio de Windows • IRestablecimiento de la cuenta de IIS AppPool • Receptor de restablecimiento de contraseña

	• Plugin de restablecimiento de contraseña para tipos de recursos personalizados • Restablecimiento de contraseñas a través de conjuntos de comandos SSH **Almacenamiento y gestión de datos** • Cifrado doble AES-256 • Gestión de claves SSH • Gestión de certificados SSL/TLS **Gestión de contraseñas entre aplicaciones** • Conexiones HTTPS para las comunicaciones entre aplicaciones • Verificación mediante certificado SSL **Seguridad de las contraseñas de DevOps** • Gestión de contraseñas para plataformas CI/CD: Jenkins, Ansible, Chef y Puppet **Validación de entradas de GUI de la web** • Protección contra las inyecciones SQL, el cross-site scripting, el desbordamiento del buffer y otros ataques **Restricciones de IP**
4. Medidas de control de acceso	**Control de acceso a los datos** • Mecanismo de control de acceso granular • Flujo de trabajo de solicitud-liberación de acceso a la contraseña • Integración del sistema de generación de tickets

5. Acceso remoto seguro	**Conexiones remotas con un solo clic** • Sesiones de Windows Remote Desktop Protocol (RDP), SSH, SQL y VNC desde cualquier navegador compatible con HTML5 • No se necesita de ningún plug-in adicional ni software de agente • Las conexiones remotas se canalizan a través del servidor Password Manager Pro • Las contraseñas necesarias para establecer sesiones remotas no tienen que estar disponibles en el navegador del usuario • No hay conectividad directa entre el dispositivo del usuario y el host remoto • Transferencia segura de archivos a los equipos de destino **Conexión automática a sitios web y aplicaciones** • Extensiones del navegador: Firefox, Internet Explorer y Chrome • Mejores prácticas de CSP • Prevención de la ejecución de JavaScript en línea (inline) • Solicitudes AJAX
6. Gestión de sesiones privilegiadas	• Grabación y reproducción de sesiones privilegiadas • Monitoreo en tiempo real
7. Auditoría, control de responsabilidad y alertas en tiempo real	**Funciones de detección y medidas de no repudio** • Alertas en tiempo real de eventos de contraseña, usuario y acceso • Pistas de auditoría en profundidad • Compatibilidad SIEM • Traps SNMP y mensajes syslog

8. Informes exhaustivos	• Informes de cumplimiento out-of-the-box para HIPAA, PCI, NERC-CIP y el GDPR • Informes de uso de contraseñas y violación de políticas • Informes de usuarios y accesos • Informes personalizados y de consulta
9. Mecanismos de disponibilidad	**Alta disponibilidad** • Instancias redundantes del servidor y la base de datos de Password Manager Pro • Conexión TCP directa con latencia para la replicación de bases de datos • Agentes de Password Manager Pro para segmentos de red no accesibles directamente **Acceso sin conexión** • Exportación de contraseñas como un archivo HTML cifrado • Frase de contraseña adicional para el cifrado AES-256 **Acceso móvil** • Aplicaciones nativas para iOS, Android y BlackBerry • Frase de contraseña como clave de cifrado • Acceso sin conexión • Pistas de auditoría para la sincronización de datos con el dispositivo móvil **Almacenamiento seguro en la nube**
10. Recuperación ante desastres	**Opción de copias de seguridad** • Copia de seguridad de la base de datos periódica y en tiempo real • Almacenamiento cifrado de los archivos de copia de seguridad **Acceso de emergencia** • Cuentas de super-administrador para atender emergencias o interrupciones repentinas

Funciones de seguridad

1. Mecanismo de bóveda y cifrado: Seguridad por diseño

1.1 Instalación de la clave maestra

- Password Manager Pro utiliza el cifrado AES-256 (el cifrado más robusto conocido y aprobado por el gobierno estadounidense). La clave utilizada para el cifrado se genera automáticamente y es única para cada instalación. Esto sirve como clave de cifrado de primer nivel.

- La clave de cifrado de primer nivel no se puede guardar con la instalación de Password Manager Pro. Esto se hace para garantizar que la clave de cifrado y los datos cifrados, tanto en las bases de datos en tiempo real como en las respaldadas, no residan juntos.

- La configuración recomendada es almacenar la clave en un servidor o dispositivo físicamente separado y garantizar que esté disponible para el servidor durante el inicio de la aplicación. Posteriormente, la clave se mantiene sólo en la memoria del servidor y nunca se escribe en ningún sitio.

- Password Manager Pro también es compatible con la rotación periódica de la clave de cifrado, en la que se genera una nueva clave que se aplica a los datos existentes y luego se descarta la clave antigua. Más información

1.2 Clave de la base de datos

- La base de datos de Password Manager Pro está protegida a través de una clave independiente, que se genera automáticamente y es única para cada instalación.

- La clave de la base de datos se puede almacenar de forma segura dentro de Password Manager Pro.

- Password Manager Pro también permite a los usuarios almacenar la clave de la base de datos en cualquier ubicación segura, dejando la clave accesible sólo para el servidor.

- El RDBMS está siempre configurado para aceptar sólo conexiones seguras (fuerza el modo SSL para las conexiones de los clientes) y los clientes sólo pueden conectarse

desde el mismo host local. En los casos en los que el servidor web y el RDBMS tienen que residir en servidores separados, la configuración aplica las conexiones sólo desde las direcciones IP configuradas.

1.3 Modo de conformidad con FIPS

- Password Manager Pro se puede ajustar para que funcione en el modo de conformidad con FIPS 140-2 (utilizando un servidor SQL como base de datos backend), en el que todo el cifrado se realiza a través de sistemas y bibliotecas con certificación FIPS 140-2.

1.4 SafeNet Luna PCIe HSM

- Password Manager Pro también es compatible con SafeNet Luna PCIe HSM para ofrecer a los administradores la opción de activar el cifrado de datos por hardware.

- SafeNet HSM gestiona todos los métodos de cifrado y descifrado, y almacena la clave y los datos cifrados directamente en su módulo de hardware, que se instala en un equipo o en un servidor de red.

1.5 Criptografía personalizada

- Además de la técnica de criptografía predeterminada, Password Manager Pro ofrece la opción de utilizar criptografía personalizada, es decir, métodos de cifrado y descifrado personalizables mediante la implementación de la interfaz Java PMPEncryptDecrypt con métodos setter y getter, lo que permite a los administradores utilizar su propia clave y lógica de cifrado.

1.6 Arquitectura multi inquilino (edición MSP)

- Password Manager Pro ofrece una edición MSP para la segmentación segura de datos entre departamentos o, en el caso de los clientes MSP, entre sus clientes. La segmentación se realiza a nivel de filas de la base de datos en el RDBMS.

- A cada departamento o cliente que requiera segmentación de datos se le proporciona un rango de valores para la identidad única de cada fila. Todas las operaciones de la base de datos realizadas para ese departamento o clientes se restringen automáticamente a ese rango de valores. Para más detalles, haga clic aquí.

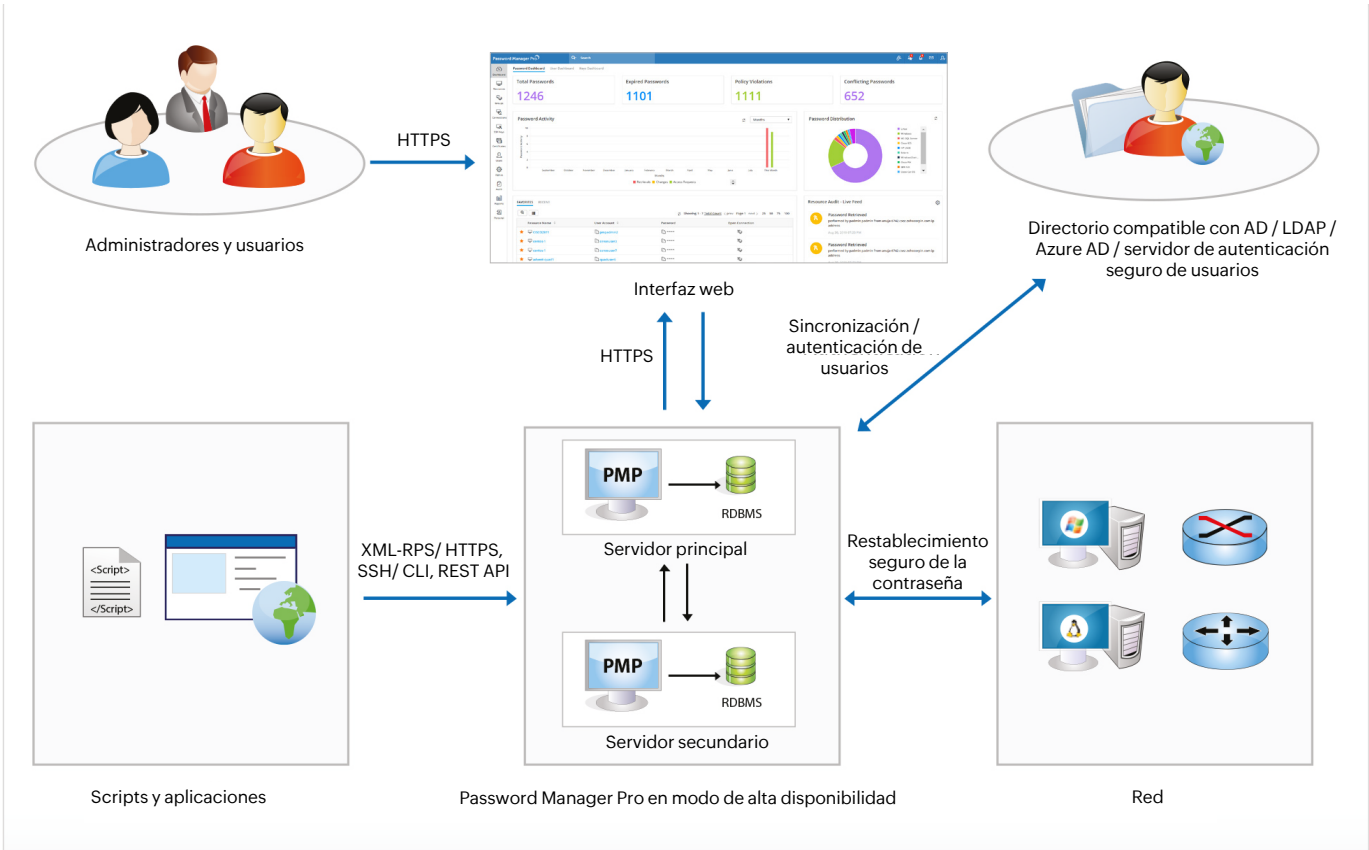


Fig 1. Arquitectura del producto

2. Identificación y autenticación

2.1. Autenticación robusta a nivel de aplicación: diversas opciones

Password Manager Pro ofrece diversas opciones para identificar de forma exclusiva a los usuarios que accederán a la aplicación. Todas las opciones se complementan con diversas disposiciones de autenticación de dos factores, que proporcionan una capa adicional de seguridad.

- **Integración con almacenes de identidades:**
- Password Manager Pro se integra fácilmente con almacenes de identidades externos como Microsoft Active Directory, cualquier servicio de directorio compatible con LDAP (Novell eDirectory y Oracle OID) y RADIUS. Los usuarios pueden ser importados desde los almacenes de identidad y se puede aprovechar el mecanismo de autenticación respectivo. Los usuarios serán identificados de forma única a través de sus respectivas cuentas en el almacén de identidades. Más información.

- **Cuentas únicas y autenticación local segura:** Password Manager Pro incluye un mecanismo de autenticación local en el que se crean cuentas únicas para los usuarios. Los usuarios podrán acceder a la aplicación con sus credenciales. Password Manager Pro emplea el algoritmo SHA2 para generar las contraseñas, lo que garantiza que cada contraseña de acceso sea única y esté protegida de forma irreversible.

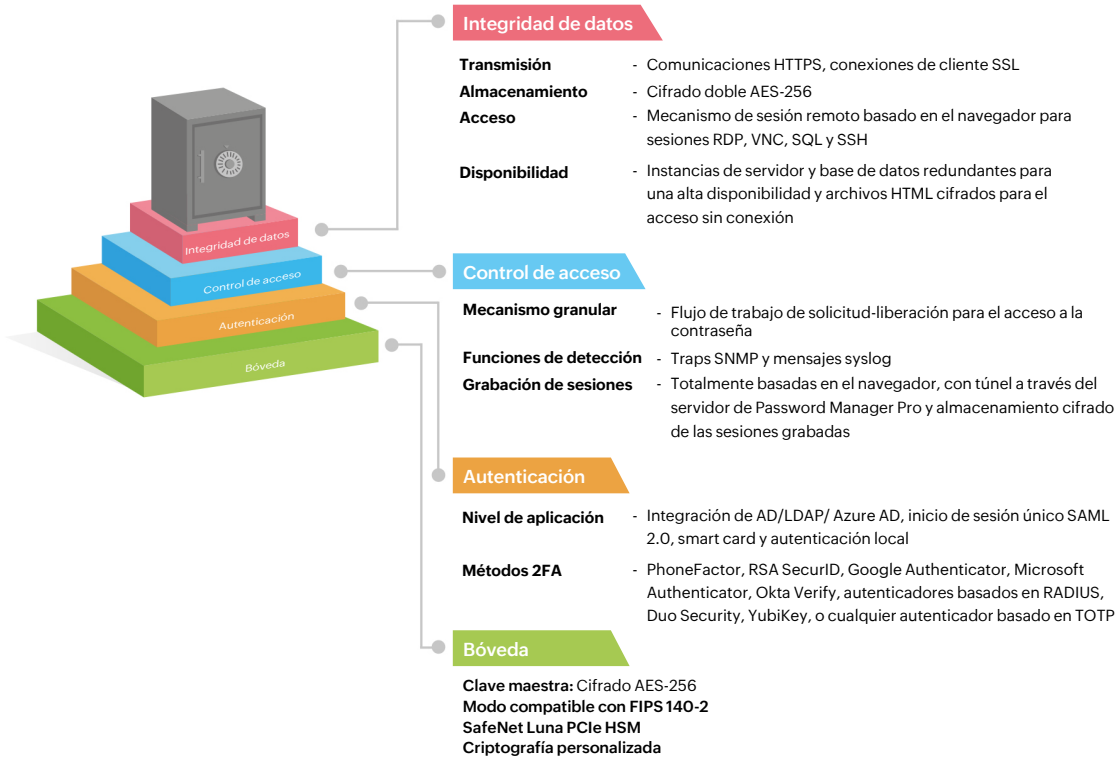
- **Tarjeta de acceso común:** Password Manager Pro es compatible con la autenticación con tarjeta inteligente. El usuario debe poseer la tarjeta inteligente y conocer también el número de identificación personal (PIN). Para más detalles, haga clic aquí.

- **Restablecimiento obligatorio de la contraseña para la autenticación local:** Como precaución de seguridad, Password Manager Pro requiere que el usuario restablezca la contraseña de autenticación local como primer paso obligatorio en los siguientes escenarios:

    - El usuario se conecta por primera vez con su contraseña por defecto
    - Cuando la contraseña de acceso es la misma que el nombre de usuario
    - Cuando el usuario olvida la contraseña y recibe por correo electrónico una nueva contraseña generada por el sistema

- En todos estos casos, el usuario podrá seguir adelante sólo después de restablecer la contraseña.

- **Servicio compatible con SAML:** Password Manager Pro ofrece compatibilidad con SAML 2.0, lo que facilita la integración con soluciones de gestión de identidades federadas para el inicio de sesión único. Password Manager Pro actúa como proveedor de servicios (SP) y se integra con el proveedor de identidad (IdP) utilizando SAML 2.0. La integración consiste básicamente en proporcionar detalles sobre el SP al IdP y viceversa. Después de integrar Password Manager Pro con un IdP, los usuarios conectados pueden iniciar sesión desde la GUI del proveedor de identidad respectivo sin tener que volver a proporcionar las credenciales. Para más detalles, haga clic aquí.



2.2. Mecanismo de garantía: Autenticación de dos factores (2FA)

Para introducir un nivel adicional de seguridad, Password Manager Pro proporciona una autenticación de dos factores. Los usuarios deberán autenticarse en dos etapas sucesivas para acceder a la interfaz web. El segundo nivel de autenticación puede realizarse mediante una de las siguientes opciones:

- **PhoneFactor:** Este proveedor líder mundial de 2FA basado en el teléfono permite una seguridad sencilla y efectiva al realizar una llamada de confirmación a su teléfono durante el proceso de inicio de sesión.

- **RSA SecurID:** Integre RSA SecurID con Password Manager Pro para generar un token de validación único que cambia cada 60 segundos.

- **Contraseña única por correo electrónico:** Autentique mediante el envío de contraseñas únicas por correo electrónico a los usuarios. Las contraseñas validan al usuario durante una sesión de inicio de sesión y luego expiran.

- **Google Authenticator:** Los tokens numéricos basados en el tiempo se pueden recibir instalando la aplicación Google Authenticator en su smartphone o tablet.

- **RADIUS Authenticator:** Aproveche los mecanismos de autenticación de cualquier sistema compatible con RADIUS, como Vasco Digipass, para crear contraseñas de un solo uso.

- **Microsoft Authenticator:** Proporcione el token de seis dígitos en la aplicación Microsoft Authenticator.

- **Okta Verify:** Utilice el token de seis dígitos en la aplicación Okta Verify.

- **Duo Security:** Aproveche la autenticación de Duo Security.

- **YubiKey:** Genere contraseñas de un solo uso con YubiKey.

- Aparte de estos, Password Manager Pro es compatible con cualquier autenticador basado en TOTP.

Para más detalles, haga clic aquí.

3. Seguridad e integridad de los datos

3.1 Transmisión de datos

Todas las transmisiones de datos entre la interfaz de usuario de Password Manager Pro y el servidor están cifradas y tienen lugar a través de HTTPS.

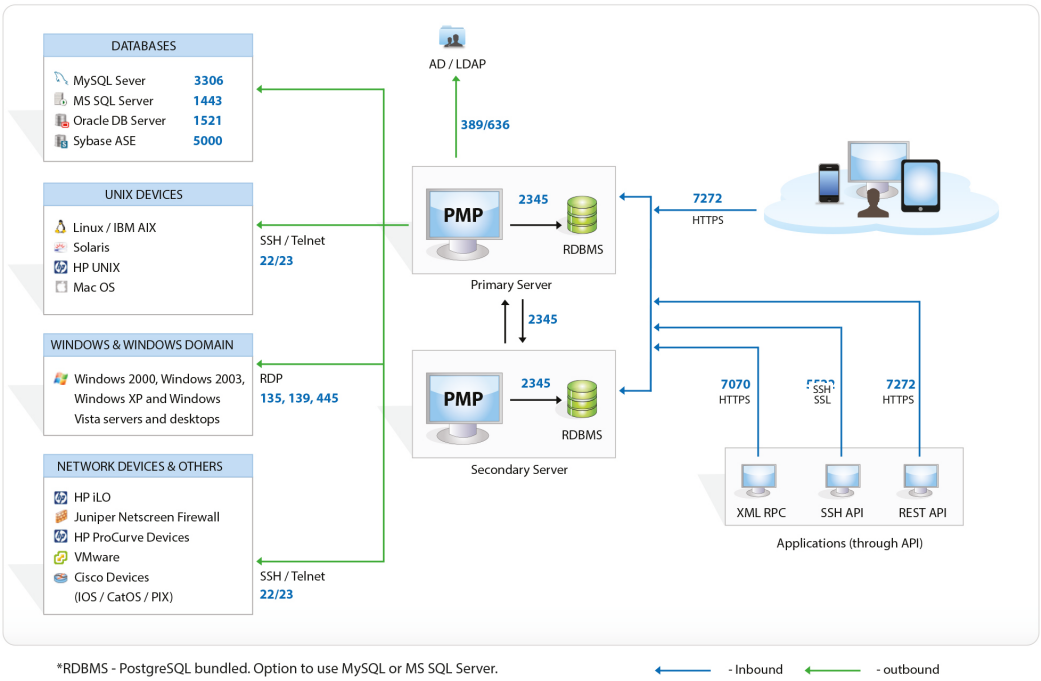


Fig. 3. Diagrama de flujo de datos

- Toda la transmisión de datos entre el servidor Password Manager Pro y la base de datos se realiza a través de SSL.

- Para las acciones de restablecimiento remoto de contraseñas, existe la opción de transmitir las contraseñas de los usuarios mediante SSH.

- **Comunicación entre Password Manager Pro y los agentes:** Password Manager Pro permite implementar agentes que pueden conectarse al servidor. La comunicación es siempre unidireccional, es decir, el agente siempre inicia esta conexión. Por lo tanto, sólo el servidor debe estar disponible para los agentes, eliminando la necesidad de crear agujeros en el firewall o crear rutas VPN para que el servidor llegue a todos los agentes. El agente realiza periódicamente un ping al servidor a través de HTTPS para comprobar si hay alguna operación (restablecimiento de contraseña o verificación de contraseña) pendiente por ejecutar. El agente llevará a cabo las tareas y, tras completarlas, notificará al servidor los resultados. Más información.

- La comunicación entre los servidores primario y secundario está cifrada a través de HTTPS.

3.2 Restablecimiento remoto de la contraseña

- **Restablecimiento remoto automático y programado de contraseñas:** Password Manager Pro es compatible con el restablecimiento remoto de contraseñas sin agente para más de 70 tipos de recursos out-of-the-box, cuyos detalles se pueden encontrar aquí.

- **Restablecimiento remoto de la contraseña mediante agentes:** El agente Password Manager Pro restablece automáticamente la contraseña de los recursos remotos que no están conectados al servidor Password Manager Pro. Una vez implementado el agente en los equipos de destino, se comunicará con la aplicación y realizará los cambios de contraseña.

- **Restablecimiento de la contraseña de la cuenta de servicio de Windows:** Password Manager Pro identifica las cuentas de servicio asociadas a una determinada cuenta de dominio. Al restablecer la contraseña de una cuenta de dominio gestionada en Password Manager Pro, encontrará los servicios que utilizan esa cuenta de dominio en particular como una cuenta de servicio y automáticamente restablecerá su contraseña.

- **Restablecimiento de la cuenta IIS AppPool:** Al restablecer las contraseñas de las cuentas de dominio, Password Manager Pro identificará los IIS AppPools asociados a esa cuenta de dominio en particular y actualizará automáticamente sus contraseñas.

- **Receptor de restablecimiento de contraseña:** El receptor de restablecimiento de contraseñas es un script o ejecutable que puede ser invocado cada vez que se cambie o restablezca la contraseña de una cuenta en el repositorio de Password Manager Pro. El receptor puede ser invocado incluso para los cambios de contraseña local y para los recursos para los que el restablecimiento remoto de la contraseña no es compatible out-of-the-box.

- **Plug-ins de restablecimiento de contraseña para tipos de recursos personalizados:** El plug-in de restablecimiento de contraseña permite a los administradores añadir su propia clase de implementación y aplicar el restablecimiento automático de la contraseña para los recursos que no son compatibles con Password Manager Pro out-of-the-box, como los tipos de recursos heredados, las aplicaciones internas y más. Los plug-in también pueden diseñarse para imponer controles de acceso a las cuentas heredadas y permitir el restablecimiento automático de las contraseñas al instante de su uso. De esta manera, las contraseñas de estas cuentas servirán como contraseñas de un solo uso que se restablecen después de cada uso a través del plug-in asociado.

- **Restablecimiento de contraseñas a través de conjuntos de comandos SSH:** Para los recursos personalizados basados en SSH, Password Manager Pro permite a los administradores añadir directamente los comandos SSH de restablecimiento de contraseña utilizados en los recursos a la interfaz web de Password Manager Pro, sin necesidad de un terminal CLI. Password Manager Pro ofrece un conjunto de comandos básicos por defecto junto con una opción para añadir comandos personalizados, organizarlos en el orden de ejecución y combinarlos en un nuevo conjunto de comandos.

3.3 Almacenamiento y gestión de datos

- Password Manager Pro está diseñado como una aplicación web con un servidor web para la lógica del negocio y RDBMS para el almacenamiento de datos.

- Tras aplicar los vectores de inicialización adecuados y otras buenas prácticas estándar en torno al cifrado, se genera en el servidor web la clave de cifrado de primer nivel con el algoritmo AES-256.

- Los datos cifrados se envían al RDBMS para su almacenamiento mediante consultas SQL. A continuación, Password Manager Pro cifra los datos con las funciones AES integradas de RDBMS para obtener una doble capa de cifrado.

- Los datos grabados de las sesiones privilegiadas también se cifran antes de su almacenamiento y sólo se pueden reproducir a través del reproductor propietario, ya que los datos se almacenan en el formato propietario.

- Password Manager Pro también almacena y gestiona de forma segura claves SSH, certificados SSL/TLS, archivos, documentos, imágenes y otras identidades digitales.

3.4 Gestión de contraseñas entre aplicaciones

- En el caso de las contraseñas entre aplicaciones, Password Manager Pro expone una API web, y las aplicaciones se conectan e interactúan a través de HTTPS. La identidad de la aplicación se verifica forzándola a emitir un certificado SSL válido, que coincida con los datos que ya se hayan registrado en Password Manager Pro acerca de la aplicación. Más información.

3.5 Seguridad de las contraseñas de DevOps

- **Gestión de contraseñas para plataformas CI/CD:** Password Manager Pro ayuda a eliminar las credenciales incorporadas en la canalización de DevOps al proporcionar funciones de integración con varias herramientas de CI/CD, como Jenkins, Ansible, Chef y Puppet. La integración garantiza que las credenciales requeridas se recuperen de forma segura desde la bóveda de Password Manager Pro cada vez que se ejecute una tarea, en lugar de almacenarse en texto plano dentro de los archivos de script.

3.6 Validación de entradas de GUI de la web

- Password Manager Pro valida minuciosamente todas las entradas en la GUI. Se filtra el uso de caracteres especiales y el código HTML y la aplicación está protegida contra los ataques más comunes, como las inyecciones de SQL, el cross-site scripting, los desbordamientos de búfer y otros ataques.

3.7 Restricciones de IP

- Password Manager Pro permite a los administradores limitar las conexiones entrantes al servidor de Password Manager Pro aplicando restricciones basadas en IP para minimizar el tráfico no deseado.

Proporciona una capa adicional de seguridad al permitir que el administrador elija exactamente a qué sistemas se les debe permitir o bloquear el acceso y el envío de solicitudes al servidor Password Manager Pro.

4. Medidas de control de acceso

4.1 Control de acceso a los datos

- Todo el acceso a los datos en Password Manager Pro está sujeto al mecanismo de control de acceso detallado. Las prácticas de titularidad e intercambio de contraseñas están bien definidas, y los usuarios solamente tienen acceso a las contraseñas autorizadas.

- En el caso de los activos altamente sensibles, se puede aplicar una capa adicional de seguridad que obliga a los usuarios autorizados a pasar por un mecanismo de solicitud-liberación. Siempre que se necesite acceder a la contraseña de un recurso de TI sensible, se debe realizar una solicitud, que se dirige al administrador (personas designadas para autorizar el acceso) para su aprobación y se libera por un periodo de tiempo limitado. Más información.

- Todos los accesos a las contraseñas (quién ha accedido a qué contraseña y cuándo) y todas las operaciones realizadas por los usuarios en cualquier recurso se registran en pistas de auditoría, lo que garantiza la responsabilidad de todos los usuarios y acciones.

- Además, como parte de la aplicación de políticas, las organizaciones pueden aleatorizar automáticamente las contraseñas de los recursos de TI sensibles de forma periódica. Password Manager Pro asigna contraseñas robustas y únicas a los activos. También analiza las contraseñas de los sistemas para comprobar la complejidad requerida e informa de las infracciones. Estas disposiciones ayudan a evitar el acceso no autorizado a las contraseñas, lo que impide el acceso no autorizado a los sistemas y aplicaciones. Más información.

- **Integración con sistemas de ticketing:** Password Manager Pro también se integra con una amplia gama de sistemas de generación de tickets para validar automáticamente las solicitudes de servicio relacionadas con el acceso privilegiado. La integración garantiza que sólo los usuarios con un ID de ticket válido puedan acceder a las contraseñas privilegiadas autorizadas. Esta integración también se extiende al flujo de trabajo de Password Manager Pro, que ayuda a conceder aprobaciones a las solicitudes de acceso con contraseña tras la validación automática de las correspondientes solicitudes de servicio en el sistema de generación de tickets.

5. Acceso remoto seguro

5.1 Conexiones remotas con un solo clic

- Password Manager Pro permite a los usuarios lanzar sesiones RDP, SSH, SQL y VNC de Windows altamente seguras, fiables y completamente emuladas desde cualquier navegador compatible con HTML5 sin necesidad de software adicional plug-in o de agente.

- Las conexiones remotas a los endpoints se canalizan a través del servidor Password Manager Pro, por lo que no se requiere una conectividad directa entre el dispositivo del usuario y el host remoto.

- Además de una fiabilidad superior, la conectividad canalizada (en túnel) proporciona una seguridad extrema, ya que las contraseñas necesarias para establecer sesiones remotas no tienen que estar disponibles en el navegador del usuario. Más información.

- Password Manager Pro permite a los usuarios transferir de forma segura archivos a los equipos de destino durante las sesiones remotas. En el caso de Windows, los archivos se pueden transferir hacia y desde el equipo de destino durante una sesión RDP facilitada por RDP. Para las sesiones SSH en sistemas Linux, las transferencias de archivos son unidireccionales, es decir, sólo hacia el equipo de destino, utilizando el protocolo de copia segura (SCP).

5.2 Conexión automática a sitios web y aplicaciones con extensiones del navegador web

- Password Manager Pro ofrece extensiones de navegador para Firefox, Internet Explorer y Chrome. Las extensiones han sido diseñadas para garantizar el máximo nivel de seguridad y privacidad de los datos.

- Se aplican las mejores prácticas de la Política de Seguridad de Contenidos (CSP) para combatir eficazmente los ataques de inyección de contenidos.

- La ejecución de JavaScript en directo y las solicitudes AJAX a otros sitios se han desactivado para evitar ataques XSS.

- Se ha garantizado el máximo nivel de seguridad en todas las etapas de la recuperación y el tránsito de datos, incluso cuando:
    i. Se validan las frases de contraseña
    ii. Se recuperan los datos encriptados del servidor
    iii. Se mantienen las contraseñas y otros datos sensibles como variables de JavaScript (a las que no puede acceder ninguna aplicación externa ni otras extensiones)
    iv. Se almacenan otros datos en segundo plano como registros locales
    v. Se pasan credenciales a los sitios web
    vi. TEl usuario se desconecta o permanece inactivo durante un tiempo determinado, tras el cual los datos locales se borran por completo.

6. Gestión de sesiones privilegiadas

- Todas las acciones realizadas por los usuarios durante la sesión privilegiada se graban en vídeo y se almacenan de forma segura para futuros análisis forenses. Más información.

- Además de la grabación de sesiones, Password Manager Pro permite a los administradores monitorear las sesiones privilegiadas en tiempo real. Si se encuentra alguna actividad sospechosa, el administrador puede cortar la conexión inmediatamente.

7. Auditoría, control de responsabilidad y alertas en tiempo real

7.1 Funciones de detección

- Password Manager Pro proporciona alertas y notificaciones en tiempo real sobre varios eventos de contraseñas, incluyendo el acceso, la modificación, la eliminación, los cambios en los permisos de uso compartido y otros eventos específicos. Más información.

- El módulo de auditoría, que registra todas las acciones del usuario y del sistema, también permite a los administradores configurar qué eventos deben enviarse a los sistemas de gestión de eventos e información de seguridad (SIEM). Las alertas de eventos pueden enviarse como mensajes syslog estándar o como traps SNMP. Más información.

7.2 Medidas de no repudio

- Cada acción y tarea programada ejecutada por los usuarios en la interfaz de usuario es auditada.

- La información de auditoría, que contiene detalles como quién hizo qué operación, cuándo y desde dónde, se almacena en la misma base de datos. Los logs de auditoría son a prueba de manipulaciones, lo que garantiza el no repudio.

- El RDBMS está siempre configurado para aceptar solamente conexiones seguras (fuerza el modo SSL para las conexiones de los clientes), y los clientes sólo pueden conectarse desde el mismo host local. En los casos en que el servidor web y el RDBMS tienen que residir en servidores separados, la configuración permite las conexiones solamente desde direcciones IP específicas.

8. Informes exhaustivos

La información sobre todas las actividades de contraseñas y accesos privilegiados en su empresa se presenta en forma de informes exhaustivos en Password Manager Pro. El estado y los resúmenes de las diferentes actividades, como el inventario de contraseñas, el cumplimiento de las políticas, la caducidad de las contraseñas, la actividad de los usuarios, etc., se proporcionan en forma de tablas y gráficos, que ayudan a los administradores de TI a tomar decisiones bien informadas sobre la gestión de contraseñas.

- **Informes de conformidad out-of-the-box:** Password Manager Pro facilita el cumplimiento de las auditorías de seguridad y los requisitos de conformidad establecidos en diversas normativas con la ayuda de los informes de conformidad sobre PCI DSS, ISO/IEC 27001, NERC-CIP y el GDPR.

- **Informes preconfigurados:** Password Manager Pro proporciona una serie de informes preconfigurados sobre todas las actividades de contraseñas y de los usuarios, políticas de contraseñas y seguridad diversas, certificados y claves SSH.

- **Informes personalizados:** Password Manager Pro ofrece la opción de crear informes personalizados a partir de informes preconfigurados y de auditoría al especificar ciertos criterios. Los informes personalizados están diseñados para obtener información específica de la base de datos Password Manager Pro según las necesidades del cliente.

- **Informes de consulta:** Los administradores también pueden crear informes de consulta para recuperar datos específicos de la base de datos Password Manager Pro, ya sea escribiendo su propia consulta SQL o personalizando una consulta SQL de los informes existentes. Password Manager Pro permite que las sentencias SQL consulten directamente la base de datos, obtengan información de las tablas proporcionadas y formateen los datos en un informe.

- Para más información sobre los informes, haga clic aquí.

9. Mecanismos de disponibilidad

9.1 Alta disponibilidad

- Password Manager Pro ofrece alta disponibilidad para garantizar el acceso ininterrumpido a las contraseñas, lo que es posible gracias a las instancias redundantes del servidor y de la base de datos.

- Una instancia será la principal, a la que se conectarán todos los usuarios, mientras que la otra será la instancia secundaria o de reserva. Los administradores y usuarios pueden conectarse a la instancia primaria o secundaria para acceder a la consola GUI a través de un navegador de desktop, un smartphone o una tablet.

- Los servidores primario y secundario pueden estar instalados geográficamente separados, incluso a través de continentes, pero siempre que tengan una conexión TCP directa con una latencia lo suficientemente buena podrán realizar la replicación de la base de datos.

- Los servidores pueden gestionar los endpoints con los que tiene conexiones TCP directas. Para los sistemas gestionados que se encuentran en una DMZ o en segmentos de red no accesibles directamente para el servidor, se pueden instalar agentes que puedan alcanzar el servidor a través de HTTPS estándar.

- En cualquier momento, los datos de las instancias primaria y secundaria estarán sincronizados. La replicación de datos se realiza a través de un canal seguro y cifrado. Más información.

9.2 Acceso sin conexión

- Password Manager Pro facilita la exportación segura de las contraseñas para su acceso sin conexión en forma de archivo HTML cifrado e incluso sincroniza el archivo con su dispositivo móvil.

- Antes de la exportación, se pide al usuario una frase de contraseña para proteger los datos con el cifrado AES-256. Sólo se puede acceder a la copia sin conexión proporcionando la frase de contraseña. Además, esta frase de contraseña no se almacena en ningún lugar del servidor.

- Cada vez que el usuario realiza una copia sin conexión de los recursos/contraseñas compartidos con él, la actividad queda registrada en la pista de auditoría.

9.3 Acceso móvil

- Password Manager Pro ofrece aplicaciones nativas para las plataformas iOS, Android y BlackBerry. Las aplicaciones móviles permiten a los administradores de TI de las empresas y a los usuarios recuperar las contraseñas de forma segura desde cualquier lugar, sin comprometer la seguridad de los datos. La aplicación móvil es tan segura como la instalación del desktop y utiliza el mismo cifrado AES-256. Toda la comunicación entre Password Manager Pro y la aplicación móvil está protegida por el protocolo HTTPS sobre SSL.

- Las aplicaciones están protegidas por una frase de contraseña adicional introducida por el usuario, que se utiliza como clave de cifrado. Así, incluso si el dispositivo móvil es robado, las contraseñas no pueden ser descifradas en texto plano.

- Si se configura la 2FA para un usuario, éste debe cumplirla también mientras utiliza la aplicación móvil.

- Las aplicaciones no permiten a los usuarios permanecer conectados, sino que les obligan a autenticarse cada vez que acceden a la aplicación.

- Cada vez que se realiza una copia de datos sin conexión en el servidor web, la aplicación nativa sincroniza el archivo con el dispositivo del usuario y esta actividad queda registrada en la pista de auditoría. Después de que el usuario elimine el archivo HTML, también se borra del dispositivo del usuario como parte de la sincronización.

9.4 Almacenamiento seguro en la nube

- Además de la opción de exportar las contraseñas a una hoja de cálculo en texto plano o a un archivo HTML cifrado, Password Manager Pro ofrece disposiciones de almacenamiento en la nube para permitir el acceso a las contraseñas en cualquier momento y lugar de forma segura. Para ello, se puede habilitar la auto-sincronización del archivo HTML cifrado a los dispositivos móviles de los usuarios autorizados a través de las cuentas de Dropbox, Amazon S3 y Box.

10. Recuperación ante desastres

10.1 Disposición de copias de seguridad

- Password Manager Pro ofrece disposiciones tanto para la copia de seguridad en tiempo real de la base de datos como para la copia de seguridad periódica a través de tareas programadas.

- Todos los datos sensibles del archivo de copia de seguridad se almacenan de forma cifrada en un archivo ZIP bajo el directorio <Password Manager Pro_Home/backUp> o bajo el directorio de destino configurado por el administrador.

- La copia de seguridad no tendrá la clave maestra de cifrado porque Password Manager Pro no permite que tanto la clave de cifrado como los datos cifrados, en la base de datos en tiempo real y en la de copia de seguridad, residan juntos. A menos que se presente la clave de cifrado, los datos sensibles no pueden descifrarse a partir de la copia de seguridad.

- Mientras se realiza una operación de copia de seguridad de la base de datos, no se puede realizar ningún cambio de configuración en Password Manager Pro. Más información.

10.2 Fallo y recuperación del sistema

- En caso de desastre o pérdida de datos, los usuarios pueden realizar rápidamente una nueva instalación de la misma versión de Password Manager Pro y restaurar los datos respaldados en la base de datos.

- La recuperación ante desastres para Password Manager Pro con MS SQL Server como base de datos back-end sólo puede realizarse con la llave maestra utilizada inicialmente para el cifrado en la instalación. Más información.

10.3 Acceso de emergencia

- Para efectos de atender una emergencia repentina, uno o varios administradores pueden ser designados como super-administradores que tendrán acceso incondicional a toda la información del sistema, incluyendo todas las contraseñas añadidas al sistema por otros administradores.

- Los administradores no pueden designarse a sí mismos como super-administradores. Esto tiene que ser aprobado y llevado a cabo por uno o más administradores.

- Cuando el sistema tiene uno o más super-administradores configurados, todos los administradores serán notificados al respecto.

- Después de que un administrador se convierta en un super-administrador, puede iniciar sesión en Password Manager Pro y habilitar la opción para evitar la creación de cuentas adicionales de super-administrador.

11. Proceso de compilación y aplicación de parches

- El equipo de Password Manager Pro colabora estrechamente con el MESRC para realizar los análisis de vulnerabilidad y las pruebas de penetración obligatorias antes de cada lanzamiento importante, para garantizar que las últimas versiones sean completamente infalibles. Además, el equipo también ejecuta evaluaciones continuas de vulnerabilidad en estas compilaciones para garantizar que estén libres de cualquier nueva vulnerabilidad.

- Los usuarios son notificados inmediatamente para que se actualicen a la última versión cuando haya un nuevo parche de seguridad o una actualización.

- En caso de que se produzca un problema de seguridad o un escalamiento, se pide a los usuarios que presenten un informe detallado sobre la vulnerabilidad o el fallo de seguridad. Mientras tanto, el equipo de producto evalúa la validez y los riesgos asociados al error y prioriza el lanzamiento en función de la gravedad.

- Las compilaciones de las correcciones se publican entre 24 y 72 horas después de la notificación de un problema, dependiendo de la gravedad del mismo, y el equipo aprobará las compilaciones de las versiones para su lanzamiento sólo después de que se hayan probado para detectar otras vulnerabilidades o errores.

www.passwordmanagerpro.com

4141 Hacienda Drive Pleasanton,
CA 94588, USA
US +1 888 204 3539
UK : +44 (20) 35647890
Australia : +61 2 80662898
www.passwordmanagerpro.com

ManageEngine
Password Manager Pro

Por consultas: hello@passwordmanagerpro.com
Demostración: demo.passwordmanagerpro.com