Restablecimiento de contraseña autoservicio (SSPR)

BIO-key™

Índice

Estás buscando:

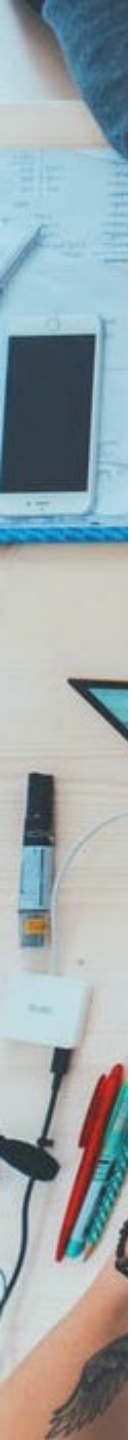
- Reduce no solo los costes del help desk, sino también los costes asociados a la pérdida de productividad para tus usuarios.
- Establece políticas de contraseñas más sólidas que trabajen con los usuarios para mejorar la administración de contraseñas y evitar malos hábitos.
- Elimina la necesidad de un ticket o una llamada telefónica al help desk para reducir el tiempo de espera de los usuarios.

Tiempo estimado de lectura: **10 minutos**

Resumen

Hoy en día, las contraseñas son una lucha para todos los que las usan y las respaldan. Los usuarios tienen demasiadas **contraseñas** para administrar, y las mejores prácticas de seguridad requieren que tengan contraseñas complejas y las cambien con frecuencia. Todo esto hace que se olviden las contraseñas, lo que genera una llamada al help desk y una interrupción para el equipo de IT.

Los **restablecimientos de contraseña** pueden suponer una importante pérdida de **recursos.**



Para resolver estos problemas y aliviar el estrés en tu help desk, debe buscar el restablecimiento de contraseña de autoservicio (SSPR).

Tener una solución SSPR puede mejorar la seguridad y la productividad de sus usuarios al mismo tiempo que reduce los costes para tu equipo de IT, liberándolos para que se centren en iniciativas más estratégicas.

Definición

Restablecimiento de contraseña autoservicio

Restablecimiento de contraseña autoserivcio (SSPR) es el proceso que permite a los usuarios restablecer su contraseña olvidada después de probar su identidad por otros medios.

Los usuarios pueden utilizar múltiples métodos de autenticación, incluidas respuestas de desafío, OTP o datos biométricos para identificar quiénes son para usar la solución SSPR para restablecer tu contraseña olvidada. Muchas soluciones también brindan a los usuarios opciones para recuperar una contraseña sin restablecerla y desbloquear su cuenta.

Esto disminuye las frustraciones tanto para los empleados como para el help desk al mismo tiempo que mejora las medidas de seguridad al disminuir el riesgo de que los usuarios compartan contraseñas, las escriban y reutilicen la misma para múltiples aplicaciones. SSPR permite a los directores de IT aplicar políticas de contraseñas más estrictas incluidos los requisitos de caracteres más altos y la caducidad de la contraseña sabiendo que sus usuarios tienen una forma de restablecer o recuperar rápidamente una contraseña si la olvidan.

Sin restablecimiento de contraseña autoservicio

Sin una solución de restablecimiento de contraseña autoservicio, las empresas pueden verse inundadas con llamadas al servicio de asistencia técnica y estirarse hasta el límite para tratar de manejar todas las solicitudes relacionadas con contraseñas. El volumen de llamadas y los tiempos de espera ejercen una gran presión tanto sobre los usuarios finales como sobre el equipo de soporte de IT. Mientras tanto, sus usuarios finales seguirán luchando con sus contraseñas complejas, lo que provocará una mala gestión de contraseñas a medida que los usuarios comiencen a compartir sus contraseñas, escribirlas o reutilizar la misma contraseña en tus cuentas.

Con restablecimiento de contraseña autoservicio

Con una solución de autoservicio de restablecimiento de contraseñas, los administradores de IT pueden aplicar políticas de contraseñas más estrictas, como la caducidad de la contraseña y la longitud mínima de la contraseña, al mismo tiempo que reducen la cantidad de llamadas al help desk relacionadas con la contraseña. Los usuarios pueden administrar sus propias contraseñas, para que puedan continuar con sus actividades diarias sin llamar al help desk.

Beneficios de usar SSPR

Las empresas utilizan una solución SSPR por muchas razones.

Los volúmenes de llamadas del help desk se reducen.
Los tickets de restablecimiento de contraseña caen rápidamente, lo que ahorra tiempo y dinero al departamento de IT al evitar tiempo innecesario de otros proyectos. También hay una disminución masiva en la interrupción general que puede causar una contraseña olvidada, lo que mejora la productividad en toda la empresa.

Los usuarios pueden administrar sus contraseñas sin involucrar al equipo de IT. SSPR permite a los usuarios restablecer y administrar sus propias contraseñas sin interrumpir su día.

Mayor seguridad al eliminar malos hábitos de contraseñas

los administradores de IT pueden aplicar políticas de contraseñas más estrictas, mientras que es más probable que los usuarios tengan una mejor "higiene de contraseñas", ya que pueden restablecer o recuperar rápidamente una contraseña olvidada por su cuenta.

Además, SSPR se puede combinar con la Autenticación Multifactor (MFA) para hacer que el proceso de restablecimiento/recuperación sea más seguro al requerir credenciales adicionales para que un usuario verifique que es quien dice ser.

La mayoría de los estudios muestran que el coste de un restablecimiento de **contraseña** puede oscilar entre **$ 25 y $ 75** por incidente y representa alrededor del **30%** o más de las llamadas al help desk

Forrester Research

SSPR puede reducir costes.

Un beneficio importante con la implementación de SSPR es que reduce los costes de las llamadas al help desk. Las llamadas al help desk cuestan mucho dinero con el coste promedio de $25 a $30 por llamada. Otra investigación muestra que las llamadas al help desk le cuestan a una empresa $ 70 de la tarifa por hora del help desk y los costes de personal.

Para los administradores de IT, la mayoría de las llamadas al help desk están relacionadas con contraseñas, desde bloqueos de cuentas, reactivación de cuentas y contraseñas olvidadas. La implementación de una solución de restablecimiento de contraseña de autoservicio puede reducir los costes y llamadas al help desk,

Forrester Research

permite a los usuarios finales realizar mejores prácticas de seguridad y ahorre dinero al departamento de iT. Una solución SSPR puede costar una mera fracción de lo que se gasta actualmente en las llamadas al help desk relacionadas con contraseñas que ofrecen un tremendo ROI para las empresas que lo implementan.

Cómo funciona: PortalGuard SSPR

BIO-key PortalGuard aprovecha las preguntas y respuestas de desafío y/o la Autenticación Multifactor (MFA) para autenticar al usuario antes de completar un restablecimiento de contraseña, recuperación u otras acciones de autoservicio. Las respuestas de los desafíos se cifran criptográficamente y se almacenan en un servidor central para ayudar a los usuarios itinerantes y evitar la necesidad de volver a inscribirse en múltiples máquinas. Las siguientes acciones también se pueden realizar desde dispositivos móviles como iPads y teléfonos inteligentes. PortalGuard se integra a la perfección con Microsoft Active Directory, Novell eDirectory, cualquier directorio compatible con LDAP y repositorios de usuarios de SQL personalizados.

PASO 1

Un usuario va a iniciar sesión y olvida su contraseña.

PASO 2

Hacen clic en el enlace "Olvidé mi contraseña" para iniciar un restablecimiento de contraseña.

PASO 3

PortalGuard les pide que se autentique usando la Autenticación Multifactor y responda 2 de 3 preguntas de seguridad previamente inscritas.

PASO 4

Luego, se lleva al usuario a la pantalla de restablecimiento de contraseña donde crea una nueva contraseña siguiendo las reglas de complejidad que IT ha configurado, incluida la longitud y la complejidad.

PASO 5

El usuario completa el restablecimiento de la contraseña y puede continuar iniciando sesión con su contraseña recién creada.

Historias de éxito de clientes

NORTHEAST IOWA COMMUNITY COLLEGE

El Northeast Iowa Community College (NICC) se enfrentó a brindar una experiencia digital optimizada y al mismo tiempo mejorar la ciberseguridad en todo el campus. Pudieron asegurar nuevos servicios como GSuite para estudiantes sin agregar fricción adicional al iniciar sesión.

¿Sabías qué?:

90% Northeast Iowa Community College experimentó una disminución del 90 % en las llamadas de restablecimiento de contraseña.

Northeast Iowa Community College

CIUDAD DE SACRAMENTO

Con una población de 500.000 habitantes, la Ciudad de Sacramento necesitaba una solución SSPR que mejorara la seguridad y aliviara la presión sobre su help desk. Gracias a SSPR, pudieron reducir significativamente las llamadas al help desk relacionadas con el bloqueo de cuentas y el restablecimiento de contraseñas.

¿Sabías qué?:

95% La ciudad de Sacramento experimentó una disminución del 95 % en las llamadas de restablecimiento de contraseña.

City of Sacramento

Qué buscar en una Solución SSPR

Qué buscar

Al buscar una **solución SSPR**, saber qué esperar y qué considerar es vital para obtener una solución que ayude tanto a tus usuarios como a tu equipo de IT.

FÁCIL INTEGRACIÓN

Una de las principales razones por las que desea implementar SSPR es para simplificar el acceso. Esto debería comenzar desde el principio con la instalación de la solución en tu entorno. Tu contraseña autoservicio es ideal.

La solución de restablecimiento debe ser una configuración plug and play, que se integre a la perfección con cualquiera que sea su repositorio de identidad: Active Directory, LDAP general o incluso tablas SQL personalizadas.

INTERFAZ DE USUARIO CONSISTENTE

Es importante mantener una interfaz de usuario coherente para reducir la capacitación de los usuarios y aumentar la adopción de SSPR. Además, es importante que la interfaz de usuario sea multifuncional y se verá igual sin importar si el usuario está operando en una Mac, PC, tableta o teléfono móvil. También se deben considerar características adicionales en tu evaluación, incluidos los indicadores visuales de las reglas de complejidad de la contraseña cuando un usuario crea su nueva contraseña.

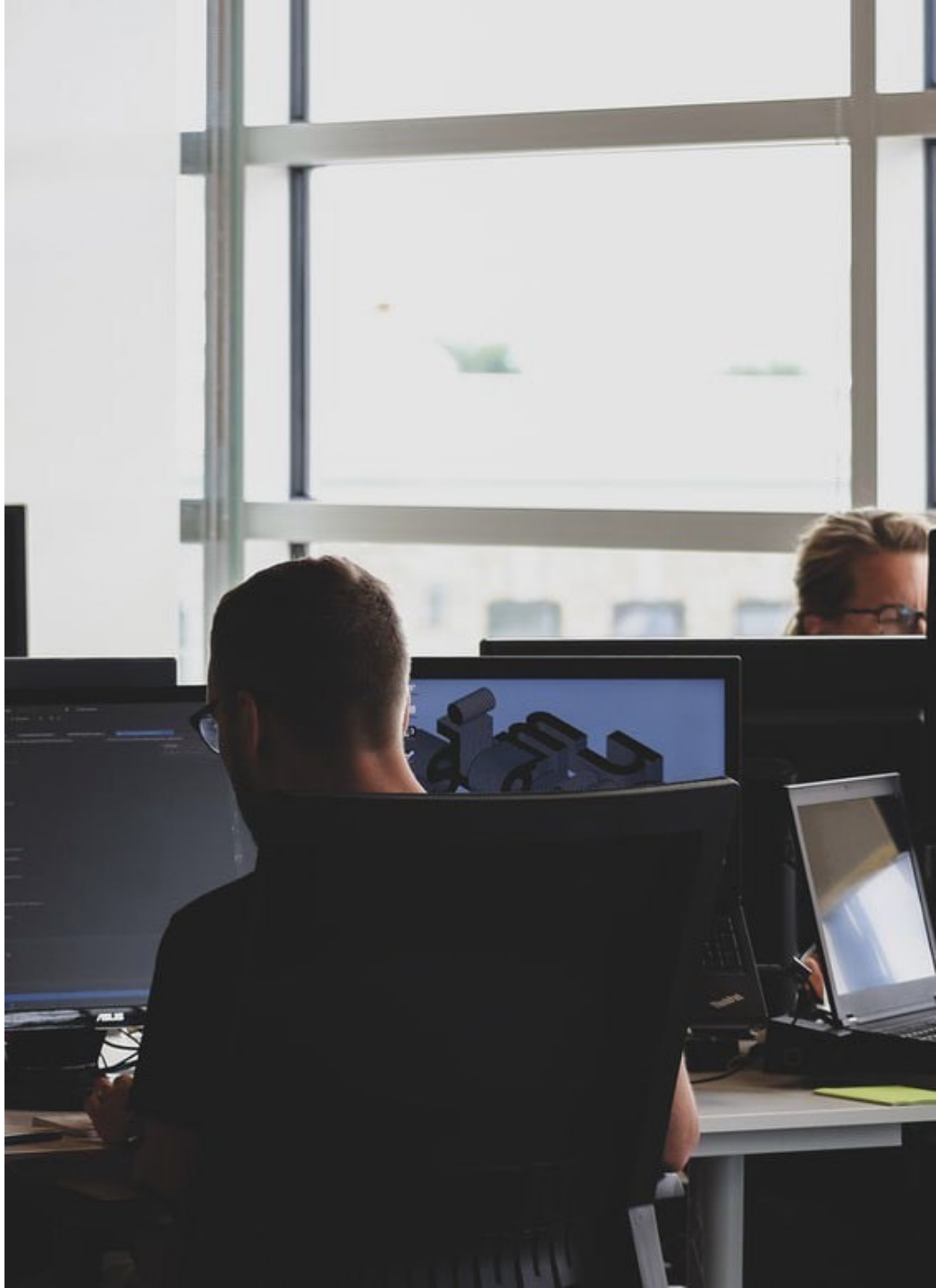
GRAN SOPORTE TÉCNICO

Es imprescindible elegir una empresa que respalde su producto con un excelente soporte técnico. Esto significa encontrar un proveedor que **NO** extienda tu solución a un servicio de terceros, que no tenga experiencia real con el producto o que solo esté leyendo scripts. Grandes equipos de soporte técnico se asociarán con tu equipo de IT y se centrarán en asegurarse de que sus usuarios mantengan su productividad.

Conclusión

Reducir las llamadas al help desk relacionadas con contraseñas no solo beneficia a los usuarios finales, sino también al equipo de soporte de IT. SSPR permitirá a tus usuarios administrar sus propias contraseñas y practicar una administración de contraseñas mejor y más segura. Los usuarios están satisfechos con tener una forma de administrar sus contraseñas, ya sea que estén en la oficina, en movimiento o fuera del horario laboral, sin tener que comunicarse con el help desk.

Para el equipo de IT, una solución SSPR reducirá los costes, evitará el agotamiento del equipo y los liberará para enfocarse en proyectos más estratégicos.



Cualquier aplicación. Una autenticación.

La solución PortalGuard de BIO-Key actúa como un portal basado en SAML que utiliza un conjunto único de credenciales para el inicio de sesión del portal, que luego otorga acceso a cuentas web registradas previamente, ya sea en la nube, privadas, locales o detrás de un firewall.

Más allá del inicio de sesión único, PortalGuard es una plataforma flexible de identidad como servicio (IDaaS) con múltiples capas de funcionalidad para ayudarlo a lograr sus objetivos de autenticación, incluida la autenticación multifactor, la autenticación contextual, el restablecimiento de contraseña de autoservicio y opciones de identidad biométrica líderes en la industria.

Regístrate a una prueba gratuita de PortalGuard

Prueba PortalGuard IDaaS y sus opciones flexibles para cumplir con sus objetivos de seguridad y brindar una experiencia de usuario optimizada.

¿QUÉ ESTÁ INCLUIDO?:

- Authenticación Multifactor (MFA)
- Single Sign-on
- Self-Service Password Reset
- BIO-key MobileAuth

Más información:

https://www.bio-key.com/

Si tienes alguna pregunta, no dudes en contactarnos:

https://www.bio-key.com/contact-us/

Acerca de BIO-key International

BIO-key International es un proveedor confiable de soluciones de gestión de acceso a la identidad y biometría vinculada a la identidad que permite un acceso conveniente y seguro a dispositivos, información, aplicaciones y transacciones de alto valor.

BIO-key ofrece la simplicidad y la flexibilidad necesarias para asegurar la experiencia digital moderna para usuarios locales y remotos, al tiempo que alivia la carga de los equipos de IT. Respaldado por décadas de experiencia, BIO-key tiene un historial comprobado de entrega exitosa de proyectos de Administración de Accesos e Identidad (IAM), sólidas relaciones con los partners y bajo coste total de propiedad.