ESCUELA SUPERIOR POLITÉCNICA DEL LITORAL

Facultad de Ingeniería en Electricidad y Computación

TESIS DE GRADO (COMPLEXIVO)

"Optimización de la Gestión de Accesos Privilegiados en una Empresa mediante la Implementación de la plataforma Password safe"

Previo a la obtención del Título de:

MAGISTER EN SISTEMAS DE INFORMACIÓN GERENCIAL

Presentado por:

JOSE ALBERTO ROCA AGUILERA

Guayaquil –Ecuador

2024

AGRADECIMIENTO

En primer lugar, me gustaría agradecer a mis padres Sandra Aguilera y José Roca, quienes me inculcaron los mejor de ellos para seguir siempre adelante, también agradecer a mis hermanas y resto de familia quienes me han empujado a seguir y finalizar en este camino duro y largo, a la ESPOL por darme la mejor experiencia en el ámbito profesional y a mis compañeros de clases con quienes tuve valiosos momentos de trabajo intelectual.

También quiero agradecer a los amigos que estuvieron siempre pendientes de esta finalización y preguntaban frecuentemente.

DEDICATORIA

A Dios con todo mi corazón a mi familia, mis hijos Peter, Janis y Jaren y sobre todo a mi esposa María Fernanda quien ha estado desde el principio apoyándome moralmente y en decisiones difíciles de tomar que al final dieron sus frutos. También a mis padres y en especial a mi Papá quien fue alumno de esta prestigiosa escuela. Una dedicatoria especial a mis abuelitas Carmen y Yolanda.

TRIBUNAL DE SUSTENTACIÓN

Firmado electrónicamente por:
LENIN EDUARDO FREIRE COBO

MGS. Lenin Freire Cobo

REVISOR

Firmado electrónicamente por:
JUAN CARLOS GARCIA PLUA

MGS. Juan Carlos Garcia

REVISOR

DECLARACIÓN EXPRESA

“Los derechos de titularidad y explotación, me corresponde conforme al reglamento de propiedad intelectual de la institución; y doy mi consentimiento para que la ESPOL realice la comunicación pública de la obra por cualquier medio con el fin de promover la consulta, difusión y uso público de la producción intelectual"

JOSÉ ALBERTO ROCA AGUILERA

RESUMEN

El presente documento tiene como objetivo detallar la implementación de una plataforma centralizada para la gestión de accesos privilegiados en una empresa del sector de telecomunicaciones. Esta iniciativa surge de la necesidad crítica de modernizar y fortalecer el control sobre los accesos y permisos a los diversos ambientes de producción que conforman el ecosistema tecnológico de la organización.

Para abordar esta necesidad, se ha decidido implementar la plataforma *Password safe* para optimizar la gestión de accesos privilegiados. Actualmente, la empresa enfrenta desafíos significativos con su proceso manual de gestión de accesos, que es ineficiente y presenta riesgos de seguridad. La nueva implementación pretende automatizar estos procesos y fortalecer la seguridad en la administración de accesos privilegiados.

La iniciativa incluye la instalación y configuración de infraestructuras virtuales y la integración con Active Directory para facilitar la gestión de usuarios. Se crearán políticas de acceso y contraseñas robustas, y se mapearán los usuarios en grupos para controlar mejor sus permisos. Además, se realizarán ajustes y pruebas para asegurar que las plataformas y cuentas se gestionen adecuadamente dentro de la plataforma *Password safe*.

La gestión de accesos privilegiados se transformará significativamente, con la creación de políticas claras y la configuración de sistemas de alta disponibilidad y recuperación ante desastres. También se integrarán numerosas aplicaciones para asegurar que todos los accesos privilegiados sean gestionados de forma centralizada y segura. El proyecto incluye pruebas exhaustivas para garantizar que el sistema funcione correctamente y cumpla con los requisitos

de seguridad de la empresa. Este proyecto tiene como objetivo transformar la gestión de accesos privilegiados, automatizando procesos, mejorando la seguridad y asegurando el cumplimiento de las normativas del sector.

INDICE GENERAL

AGRADECIMIENTOS ii

DEDICATORIA iii

TRIBUNAL DE SUSTENTACIÓN iv

RESUMEN vi

ABREVIATURAS Y SIMBOLOGIA x

ÍNDICE DE TABLAS xi

ÍNDICE DE FIGURAS xii

INTRODUCCIÓN xiii

CAPITULO 1 15

GENERALIDADES 15

1.1 ANTECEDENTES 15

1.2 SITUACION ACTUAL 16

1.3 DESCRIPCIÓN DEL PROBLEMA 19

1.4 SOLUCIÓN PROPUESTA 23

CAPÍTULO 2 27

METODOLOGÍA PARA EL DESARROLLO DE LA SOLUCIÓN 27

2.1. ANÁLISIS Y DEFINICIÓN DE LA SOLUCIÓN 27

2.2. IMPLEMENTACIÓN DE LA SOLUCIÓN 30

2.3. PRUEBAS 44

CAPÍTULO 3 53

EVALUACIÓN DE RESULTADOS 53

3.1. ACCESOS Y SEGURIDAD 53

3.2. MONITOREO Y AUDITORIA 54

3.3. POLITICAS DE ACCESO 54

3.4. AUTOMATIZACION Y ROTACION DE CONTRASEÑAS 55

CONCLUSIONES Y RECOMENDACIONES 56

BIBLIOGRAFIA 60

ABREVIATURAS Y SIMBOLOGIA

AD	Active Directory
API	Application Programming Interface (Interfaz de Programación de Aplicaciones)
CRM	Customer Relationship Management (Gestión de Relaciones con el Cliente)
GB	Gigabyte
GHz	Gigahertz
GUI	Graphical User Interface (Interfaz Gráfica de Usuario)
HA	High Availability (Alta Disponibilidad)
HTTPS	HyperText Transfer Protocol Secure (Protocolo de Transferencia de Hipertexto Seguro)
LDAP	Lightweight Directory Access Protocol (Protocolo Ligero de Acceso a Directorios)
MFA	Multi-Factor Authentication (Autenticación Multifactor)
PAM	Privileged Access Management (Gestión de Accesos Privilegiados)
PC	Personal Computer (Computadora Personal)
PuTTY	PuTTY (Programa de Emulación de Terminal y Cliente de SSH)
RDP	Remote Desktop Protocol (Protocolo de Escritorio Remoto)
REST	Representational State Transfer (Transferencia de Estado Representacional)
S.O	Sistema Operativo
SQL	Structured Query Language (Lenguaje de Consulta Estructurado)
SSH	Secure Shell (Intérprete de Órdenes Seguro)
TIC	Tecnologías de la Información y la Comunicación
TI	Tecnología de la Información
VPN	Virtual Private Network (Red Privada Virtual)
WinSCP	Windows Secure Copy (Software para Transferencia Segura de Archivos)

ÍNDICE DE FIGURAS

Figura 1. Arquitectura preliminar Password Safe 34

Figura 2. Solicitud de acceso 38

Figura 3. Esquema de recuperación Activo/Pasivo 40

Figura 4. Creación de cuentas 41

Figura 5. Creación de Active Directory Group 42

Figura 6. Configuración de reportaría 43

Figura 7. Ejemplo de reportes 44

Figura 8. Usuario Inicia sesión 45

Figura 9. Selecciona el tipo de aplicación que quiere acceder 46

Figura 10. usuario indica cuando quiere acceder y el tiempo de sesión 46

Figura 11. Luego de la aprobación, el usuario puede ingresar a la aplicación sin necesidad de ingresar contraseña 47

Figura 12. Revisión de las sesiones activas 48

Figura 13. Se verifica la sesión del permiso anterior activa 48

Figura 14. Monitoreo en vivo de la sesión del usuario 49

Figura 15. Se modifica el acceso solo a nivel de aplicación (ADUG) dentro del servidor 50

Figura 16. Ingreso al servidor por medio de PasswordSafe 50

Figura 17. El usuario solo puede visualizar la aplicación con privilegios mínimos 51

Figura 18. se valida las políticas de contraseña del activo 52

Figura 19. Validación de que la contraseña esté rotando 52

ÍNDICE DE TABLAS

Tabla 1. Requerimientos del Hardware 35

Tabla 2. Grupos active Directory 37

INTRODUCCIÓN

Imagina que en una empresa hay ciertas personas que tienen las llaves maestras de todas las puertas, incluyendo las que protegen los documentos más importantes y las áreas más sensibles. En una empresa de telecomunicaciones, una de sus áreas más sensibles es la de tecnologías, que contiene activos críticos para las operaciones diarias e información sensible sobre sus clientes.

Para proteger estos activos, es necesario contar con un custodio que administre las llaves de ingreso. Este proceso se llama gestión de accesos privilegiados (PAM) [1]. Para acceder a estas áreas, los empleados deben consultar con el custodio si pueden entrar y pedir prestadas las llaves. Este custodio controla quién puede acceder, cuándo y para qué propósito, asegurando que solo las personas adecuadas tengan acceso a las áreas críticas de la empresa.

Este documento se enfoca en una empresa de telecomunicaciones con años de trayectoria en Ecuador, especializada en la provisión de servicios de telefonía móvil e internet residencial. A lo largo de su historia, la compañía ha desarrollado diversas soluciones que permiten a sus usuarios gestionar y activar servicios de manera eficiente y conveniente, consolidándose como un actor clave en el sector de las telecomunicaciones del país.

un componente vital en la estrategia de seguridad de cualquier organización tecnológica.

El presente proyecto nace de la necesidad de modernizar y fortalecer los procesos de gestión de accesos privilegiados en la empresa. Esta iniciativa no solo busca mejorar la seguridad de los sistemas y la información, sino también optimizar los procesos internos, aumentar la eficiencia operativa y facilitar el cumplimiento de las normativas cada vez más exigentes del sector de las telecomunicaciones.

La implementación de una solución robusta para la gestión de accesos privilegiados se presenta como una oportunidad estratégica para la empresa. Además de reforzar sus políticas internas de seguridad informáticas lo cual cuidan celosamente, esta iniciativa permitirá a la compañía modernizar su gestión de accesos, cuidar sus plataformas críticas para el negocio y cuidar información sensible de sus clientes.

CAPÍTULO 1

GENERALIDADES

1.1 Antecedentes

A lo largo de sus años de operación, la empresa ha experimentado un notable crecimiento en su base de clientes y en las plataformas tecnológicas que constituyen los pilares fundamentales para ofrecer sus servicios críticos.

Este crecimiento en la cartera de clientes ha ido de la mano con una expansión en la demanda de servicios, lo que ha impulsado el desarrollo e implementación de nuevas plataformas para adaptarse a estas necesidades emergentes. Como resultado, a lo largo de los años, la empresa ha acumulado un inventario significativo de plataformas críticas, cada una de ellas sujeta a continuos proyectos de mejora y expansión para potenciar estos servicios.

Esta evolución constante ha generado un aumento en las solicitudes de acceso a estas plataformas, tanto por parte del personal interno de proyectos como de los proveedores externos. Estos accesos son necesarios para realizar nuevas configuraciones y ajustes. Sin embargo, esta situación ha llevado en ocasiones a que las plataformas experimenten inconvenientes debido a cambios que, aunque controlados, no siempre han sido completamente soportados o correctamente evaluados en cuanto a su impacto.

Como consecuencia, se han producido casos de afectación del servicio donde, si bien se ha podido identificar al responsable, no se ha contado con un mecanismo de control preventivo eficaz sobre los cambios requeridos.

Históricamente, la empresa ha gestionado los accesos privilegiados mediante un proceso manual que involucra múltiples pasos:

- Los accesos se solicitan y se someten a dos niveles de aprobación dentro del departamento de Producción del área TIC.
- Una vez aprobados, un ingeniero de apoyo concede manualmente los accesos a las plataformas requeridas.
- Este sistema se ha utilizado para gestionar accesos a diversos sistemas operativos, plataformas de despliegue de aplicaciones, entornos de desarrollo SQL y otras herramientas críticas para el negocio.
- A lo largo del tiempo, este enfoque ha demostrado ser ineficiente y propenso a errores, lo que ha llevado a la búsqueda de una solución más avanzada y segura.

1.2 Situación actual

En la actualidad, si un técnico necesita las llaves de acceso para ingresar a uno de los activos tecnológicos, debe solicitarlas y entrar en algunas ocasiones acompañado del custodio hasta la puerta y en otras deberá ir solo y el custodio deberá confiar ciegamente sobre lo que hará. Entendiendo esto y llevados al entorno de los activos tecnológicos, explicaremos como se conceden estos accesos de forma manual siguiendo por medio de estos puntos:

2. **Proceso de solicitud y aprobación de accesos:**

   Usuarios utilizan un portal web para la solicitud de accesos privilegiados a distintas plataformas tecnológicas. Estas solicitudes requieren la autorización de gerencias y jefaturas, las cuales son concedidas o denegadas en el mismo portal.

   Si el permiso se concede, se asigna a un custodio para que gestione el acceso a la persona solicitante.

3. **Gestión de credenciales:**

   Las credenciales de usuarios con privilegios se almacenan en una herramienta que guarda las contraseñas de los activos custodiados por el departamento dueño del mismo, donde el custodio procederá a ingresar con una credencial a esta herramienta y localizar el usuario y Password de la plataforma solicitada, para luego ingresarla en la plataforma solicitada.

4. **Métodos de asignación de accesos:**

   a. **Acceso local:**

      El ingeniero custodio ingresa las credenciales en una PC designada con acceso de red a las plataformas productivas, para lo cual el solicitante debe estar físicamente presente en esta PC para utilizar los accesos.

   b. **Acceso remoto interno:**

      Si el solicitante tiene los permisos necesarios de red en su estación de trabajo para conectarse a las plataformas solicitadas, el custodio puede aplicar las

credenciales vía escritorio remoto desde su PC a dicha estación o acudir presencialmente a esta PC para ingresar las credenciales.

En este punto no hay supervisión por parte del custodio en cuanto a lo que realiza el solicitante ya que estaría distante.

c. **Acceso remoto con supervisión:**

Si el solicitante no se encuentra físicamente en la empresa y no tiene permisos de red para ingresar a la red de la empresa, se puede dar los accesos vía video conferencia, donde el custodio en su estación de trabajo, ingresará a las plataformas solicitadas y aplicará las credenciales necesarias para luego dar el control remoto de su PC al solicitante. Por lo que el custodio deberá solo observar lo realizado por el custodio. Por lo general este método se da con los proveedores externos de la compañía.

5. **Control de acceso:**

El acceso a plataformas de producción desde PCs locales, está controlado por permisos de red y por segmentos de red y la confiabilidad del custodio sobre el solicitante, es decir el custodio sabe quién es y qué acción desea realizar el solicitante.

Esta estructura actual, si bien intenta mantener un cierto nivel de control, presenta varios desafíos en términos de eficiencia, seguridad y escalabilidad. La dependencia de procesos manuales y la falta de un sistema integral de gestión de accesos privilegiados son aspectos que merecen atención para mejorar la postura de seguridad de la organización.

1.3 Descripción del problema

La empresa enfrenta múltiples riesgos y vulnerabilidades de seguridad en sus activos tecnológicos de producción con el permiso de accesos e ingreso de credenciales de usuarios privilegiados, es decir, si el custodio confía las llaves de accesos, todo quedará en fe y confianza de que el solicitante sabe lo que hace y que no cometerá algún ilícito.

A continuación, se detallan los principales problemas identificados en proceso actual para dar accesos con usuarios privilegiados a las distintas plataformas. Cada uno de estos puntos representa un área de preocupación que requiere atención inmediata para fortalecer nuestra postura de seguridad, mejorar la eficiencia operativa y garantizar el cumplimiento de las regulaciones del sector:

- **Gestión manual para dar accesos**

  El proceso manual de gestión de accesos privilegiados es ineficiente y no controlado. La necesidad de intervención constante del custodio para cada solicitud de acceso consume tiempo valioso y reduce la productividad general del equipo de TI.

- **Pérdida de Contraseñas**

  El almacenamiento centralizado de credenciales en una herramienta de gestión de contraseñas, aunque es un paso en la dirección correcta, aún depende de la intervención manual para su uso. Esto aumenta el riesgo de exposición de contraseñas durante el proceso de acceso y podría llevar a la pérdida o compromiso de credenciales críticas.

Adicional, esta herramienta usa un archivo plano cifrado para guardar las claves, el mismo que reside en un repositorio compartido entre los custodios de cada activo del que son responsables, pero ¿y que pasa si este archivo se pierde, se corrompe o alguien realiza cambios masivos en las credenciales, perdiendo las correctas?

- **Tiempo ilimitado de sesión**

Tanto los accesos en sitio o remotos, no cuentan con un tiempo limitado de actividad dentro de las plataformas, lo que aumenta los riesgos y la dificultad para entender que actividades se realizaron dentro de ese periodo de tiempo.

- **Supervisión no controlada**

La falta de supervisión del custodio sobre las actividades del solicitante representa un riesgo significativo. No existe un mecanismo automatizado para monitorear o limitar las acciones realizadas por los usuarios con accesos privilegiados.

- **Falta de Auditoría**

Solo se cuenta con el registro de la solicitud del acceso, pero una vez dado este acceso no se tiene visualización de lo que se hace dentro del activo. Sin una plataforma que registre y monitoree todas las actividades realizadas con accesos privilegiados, es difícil detectar y responder a actividades sospechosas o malintencionadas. La auditoría continua es esencial para la seguridad y el cumplimiento normativo.

- **Principio de mínimo privilegio no aplicado**

  Las credenciales actuales que maneja el departamento de producción, no cuentan con perfiles adecuados para las distintas plataformas, ya que estos usuarios tienen privilegios de super administrador, lo que aumenta la vulnerabilidad en la seguridad informática en el caso de que esta credencial sea usada con otros fines o sea obtenida por agentes externos.

- **Respuesta inmediata a incidentes limitada**

  En el caso de un ataque interior o exterior, existe dificultad para revocar rápidamente accesos en caso de una brecha de seguridad. Actualmente para revocar los permisos de las credenciales, se tendría que realizar un revocatorio manual desde el servidor, base de datos o aplicación.

- **Incumplimiento a las políticas de la empresa**

  Las políticas de la empresa sobre seguridad Informática, demanda el control y el minimizar riesgos sobre la gestión de credenciales en sus activos tantos críticos como de apoyo, para lo que la actual gestión deja una brecha abierta para incumplir estas políticas [1]. Esta brecha puede llevar a un robo o daños en la información que maneja la empresa, lo que puede ocasionar demandas por partes reguladoras estatales públicas.

- **Persistencia no controlada de credenciales**

  Existe un riesgo significativo relacionado con la persistencia no autorizada de credenciales en las estaciones de trabajo de los solicitantes. Muchas aplicaciones y plataformas ofrecen la opción de “recordar contraseña” para comodidad del usuario. Por

ejemplo, herramientas de desarrollo de bases de datos instaladas localmente pueden almacenar las credenciales en el perfil del usuario, eliminando la necesidad de volver a ingresarlas en futuras sesiones. De manera similar, las aplicaciones web, como los sistemas CRM, pueden aprovechar las funciones de almacenamiento de contraseñas de los navegadores. Esta práctica, aunque conveniente, representa un grave riesgo de seguridad por varias razones:

a. Acceso no autorizado

Si la estación de trabajo se ve comprometida o es accedida por un usuario no autorizado, las credenciales almacenadas podrían ser utilizadas para acceder a sistemas críticos sin necesidad de pasar por el proceso de solicitud y aprobación.

b. Permiso extendido no autorizado

La disponibilidad constante de credenciales privilegiadas contradice el principio de otorgar acceso solo cuando es necesario y por el tiempo requerido.

c. Vulnerabilidades ante ataques externos e internos

A pesar de que las PCs de los usuarios cuentan con restricciones y controles de instalación, así como bloqueos de dispositivos externos, existe un riesgo latente de comprometer la seguridad:

- **Infección por malware:** Si un atacante logra introducir malware en la red, por ejemplo, a través de ingeniería social o aprovechando una vulnerabilidad no

parchada, las credenciales almacenadas localmente en las aplicaciones y navegadores podrían ser fácilmente comprometidas.

- **Robo de credenciales VPN:** En caso de que las credenciales de VPN de un usuario sean robadas, un atacante podría ganar acceso a la red interna. Si este usuario tiene credenciales privilegiadas almacenadas en las aplicaciones, el atacante podría conectarse solo con un clic, accediendo a sistemas críticos sin levantar sospechas inmediatas.

- **Dificultad de contención:** En caso de un incidente de seguridad, la presencia de credenciales almacenadas en múltiples puntos dificultaría significativamente la contención y la revocación efectiva de accesos comprometidos.

Estos escenarios subrayan la necesidad crítica de una solución que no solo gestione la asignación de accesos privilegiados, sino que también prevenga activamente el almacenamiento no autorizado de credenciales y proporcione mecanismos robustos de autenticación y monitoreo.

1.4 Solución propuesta

La solución propuesta para minimizar y controlar los riesgos en los accesos sobre los activos tecnológicos de la empresa es la implementación de una solución a la Gestión de Accesos Privilegiados (PAM).

PAM (Privileged Access Management) es una tecnología y un conjunto de buenas prácticas que ayudan a las organizaciones a controlar y monitorear el acceso de usuarios con permisos

especiales a los sistemas críticos [1]. Estos usuarios, llamados "usuarios privilegiados", tienen más permisos que el usuario promedio y pueden acceder a datos y configuraciones importantes. La plataforma que nos ayudará a implementar estas buenas prácticas se llama *Password safe de la empresa BeyondTrust*, esta plataforma no solo nos ayudará con la auto gestión de accesos, si no con la custodia segura de las contraseñas, las sesiones controladas en los accesos, los ingresos a las plataformas dentro de *Password safe* y el reporte y auditoria de posibles anomalías [2].

Abordemos un poco más cuales son las soluciones que trae esta plataforma:

Automatización de la gestión de accesos:

Password safe gestiona la solicitud de un ingreso con usuario privilegiado, asignando niveles de aprobación, flujo de trabajo y elimina la necesidad de intervención manual constante y reduciendo el riesgo de errores humanos y solo dejando la supervisión, control avanzado de la sesión y auditoria forense.

Descubrimiento Automatizado:

La plataforma tiene un motor de detección que escanea el entorno, identifica y clasifica activos y cuentas para gestionarlos según las reglas del negocio.

Gestión centralizada de credenciales:

Password safe utilizará un repositorio seguro para almacenar y gestionar todas las credenciales privilegiadas, eliminando la necesidad de que los usuarios o custodios conozcan directamente las contraseñas. Estas claves pueden ser recuperada mediante la GUI o API, obviamente si tienes los permisos para hacerlo.

Implementación de mínimos privilegios:

Password Safe otorgará credenciales con privilegios mínimos necesarios para realizar las tareas que necesita hacer el solicitante, reduciendo así la superficie de ataque y el riesgo de uso indebido de accesos privilegiados [3].

Ingreso a las plataformas sin usuario y password

Una de las características especiales que tiene la plataforma *Password safe*, es la de ingresar por RDP o SSH un ambiente con un solo clic, sin necesidad de ingresar usuario o Password. [3]

Tiempo limitado de privilegios:

Just-in-Time es un modelo de seguridad que limita drásticamente el tiempo durante el cual una cuenta posee privilegios elevados o limitados, lo que reduce la ventana en que un atacante pueda aprovechar los privilegios que tenga la cuenta y realizar daños no deseados.

Monitoreo de sesiones activas:

Los usuarios con permisos de administrador o con roles para el monitoreo de sesiones activas, pueden ver y administrar las sesiones activas en tiempo real, donde se podrá bloquear, finalizar o cancelar si el administrador así lo decide.

Auditoría y reportes:

La plataforma proveerá información para visualizar las grabaciones de las sesiones del solicitante, el cual podrá mostrar los distintos eventos que realizó en la sesión, como: Clic en elementos, abrir ventanas. Las sesiones pueden ser descargables o solo tomar print de un fotograma sobre un evento y descargarlo como un elemento jpg [3].

Escalabilidad y eficiencia: La plataforma permitirá una gestión eficiente de un volumen creciente de solicitudes de acceso, mejorando la productividad del equipo de TI.

Adopción de la nueva gestión:

Introducir una nueva cultura para la solicitud de accesos en los activos productivos de la empresa, adoptando los nuevos flujos de solicitud, autorizaciones, tiempos de sesión y restricciones.

Esta solución no solo abordará los problemas de seguridad identificados, sino que también mejorará significativamente la eficiencia operativa, fortalecerá nuestra postura de seguridad y facilitará el cumplimiento normativo. La implementación de esta plataforma nos permitirá gestionar de manera efectiva los riesgos asociados con los accesos privilegiados, protegiendo así nuestros activos tecnológicos críticos y la información sensible de nuestra empresa de telecomunicaciones.

CAPÍTULO 2

METODOLOGÍA PARA EL DESARROLLO DE LA SOLUCIÓN

2.1. Análisis y definición de la solución

La implementación de *Password safe* de la empresa BeyondTrust aportará beneficios significativos en términos de eficiencia operativa, cumplimiento normativo y cultura de seguridad. Aunque existen desafíos en la implementación, los beneficios a largo plazo justifican ampliamente la inversión y el esfuerzo requeridos.

A continuación, se analiza como la solución traerá mejoras y seguridad en los accesos con usuarios privilegiados a las distintas plataformas de la empresa:

1. Impacto en la Seguridad:

La implementación de mínimos privilegios y tiempo justo, reducirá significativamente la superficie de ataque, limitando el potencial daño de un compromiso de credenciales evitando exponer las contraseñas.

El Baúl seguro centralizado eliminará el riesgo asociado con el almacenamiento local de credenciales, abordando directamente la vulnerabilidad identificada en las estaciones de trabajo de los usuarios.

2. **Mejora en la eficiencia operativa:**

La automatización de la gestión de accesos reducirá el tiempo dedicado a tareas manuales como ingresar las credenciales manualmente en un estimado del 70%, liberando recursos del equipo de TI para otras actividades críticas. Adicional, no será necesario controlar manualmente el tiempo de acceso del solicitante, los mismo podrán expirar luego de un tiempo predeterminado.

3. **Cumplimiento Normativo:**

Las capacidades de auditoría y reportes facilitarán las evidencias para crear nuevas políticas que cumplan con las demandas de la empresa sobre seguridad informática, asegurando la información sensible de la empresa que satisfaga el cumplimiento de regulaciones del sector de telecomunicaciones [4].
Se estima una reducción del 80% en el tiempo necesario para preparar informes de cumplimiento.

4. **Prevención de Amenazas Internas:**

El monitoreo en tiempo real y la grabación de sesiones actuarán como disuasivo para el mal uso interno de privilegios. La capacidad de detectar comportamientos anómalos podría prevenir hasta un 90% de los intentos de abuso de privilegios

5. Desafíos de la implementación:

Se requerirá una fase de capacitación intensiva para todos los usuarios y administradores, estimada en 4-6 semanas.

Posible resistencia inicial de los usuarios acostumbrados a métodos tradicionales de acceso, lo que podría resultar en una disminución temporal de la productividad (5-10%) durante el primer mes.

6. Escalabilidad:

La solución *Password safe* es altamente escalable, capaz de manejar un crecimiento proyectado de usuarios y sistemas del 200% en los próximos 5 años sin necesidad de cambios significativos en la arquitectura.

7. Impacto en la Cultura de Seguridad:

La implementación de esta solución fomentará una cultura de seguridad más robusta en toda la organización.

Se espera un aumento del 40% en la concienciación sobre seguridad entre los empleados después de 6 meses de implementación.

8. Recuperación ante Desastres:

La centralización de la gestión de accesos privilegiados mejorará significativamente la capacidad de respuesta ante incidentes.

Se estima una reducción del 60% en el tiempo necesario para revocar accesos comprometidos en caso de una brecha de seguridad.

2.2. Implementación de la solución

La implementación se llevará a cabo en 3 fases: *Análisis del Proyecto, Planificación de la Implementación, Implementación de la Solución.* Cada fase incluye tareas específicas e hitos que aseguran una transición suave y efectiva hacia el nuevo sistema.

- **FASE 1: Análisis previo a la implementación**

Esta fase establece las bases para el éxito de la implementación. Comenzará con una reunión inicial con el cliente para discutir la solución y los objetivos del proyecto. Durante esta reunión, se realizará la entrega formal de las licencias necesarias para la plataforma *Password safe*. Luego, se llevará a cabo el Kick Off, donde se definirán los objetivos, alcances, entregables, responsabilidades y se conformará el equipo de trabajo entre la empresa y TECSINFO SA. Se documentarán los requisitos técnicos y operativos del cliente y se preparará la arquitectura preliminar de la solución. Esta fase culmina con la presentación de la documentación de requisitos y la arquitectura, formalizada mediante la firma del acta de asistencia del Kick Off.

Puntos relevantes de la fase 1:

- **Objetivo del proyecto**

Implementar una solución de Gestión de Accesos Privilegiados utilizando la plataforma *Password safe* para mejorar la seguridad, eficiencia y control en la administración de accesos privilegiados dentro de la empresa.

- **Alcance**

- Implementar 2 equipos en alta disponibilidad Activo/Pasivo.
- Integrar 3600 plataformas
- Configurar 4 roles, 4 flujos de aprobación, 4 reportes personalizados
- Configurar segundo factor de autenticación
- Realizar una transferencia de conocimiento sobre la plataforma instalada
- Realizar 2 mantenimientos preventivos semestrales

- **Arquitectura Preliminar**

La arquitectura básica de esta solución se compone de varios componentes clave que trabajan en conjunto para gestionar, supervisar y asegurar los accesos a los recursos críticos. A continuación, se describe cada uno de los componentes de la arquitectura [3]:

Usuarios y Solicitudes de Acceso:

Los usuarios pueden realizar solicitudes de acceso a través de una interfaz web o una interfaz de API. Estas solicitudes son esenciales para iniciar el flujo de trabajo de gestión de accesos privilegiados.

Las aplicaciones también pueden realizar solicitudes de acceso a través de una API REST, permitiendo una integración fluida con otros sistemas y aplicaciones.

Control Avanzado de Flujos de Trabajo:

Las solicitudes de acceso son gestionadas por el módulo de Control Avanzado de Flujos de Trabajo, que aplica reglas de aprobación específicas para asegurar que solo los accesos autorizados sean concedidos.

Este módulo asegura que todas las solicitudes pasen por un proceso de aprobación definido, que puede incluir múltiples niveles de autorización según la criticidad del acceso solicitado.

Recuperación de Contraseñas y Proxy de Sesión:

Una vez aprobada una solicitud, el sistema permite la recuperación de contraseñas de forma segura. Las contraseñas son gestionadas y almacenadas de manera segura, minimizando el riesgo de exposición.

El módulo de Proxy de Sesión permite a los usuarios acceder a los recursos sin revelar las credenciales subyacentes. Este enfoque proporciona una capa adicional de seguridad al gestionar las sesiones de acceso [6].

Grabación y Supervisión de Sesiones:

Todas las sesiones de acceso privilegiado son grabadas para su posterior revisión. Esto incluye la capacidad de grabar, reproducir y auditar sesiones, lo que es esencial para la supervisión y el cumplimiento.

Los registros de auditoría y las sesiones grabadas se almacenan de manera segura, permitiendo la revisión y el análisis detallado de las actividades realizadas durante las sesiones de acceso.

Integración con Recursos Críticos:

La solución está diseñada para integrarse con una amplia gama de recursos críticos, incluyendo servidores, estaciones de trabajo, dispositivos, aplicaciones, bases de datos, medios sociales y entornos de nube.

Esta integración asegura que todos los accesos a estos recursos estén controlados y supervisados adecuadamente [3].

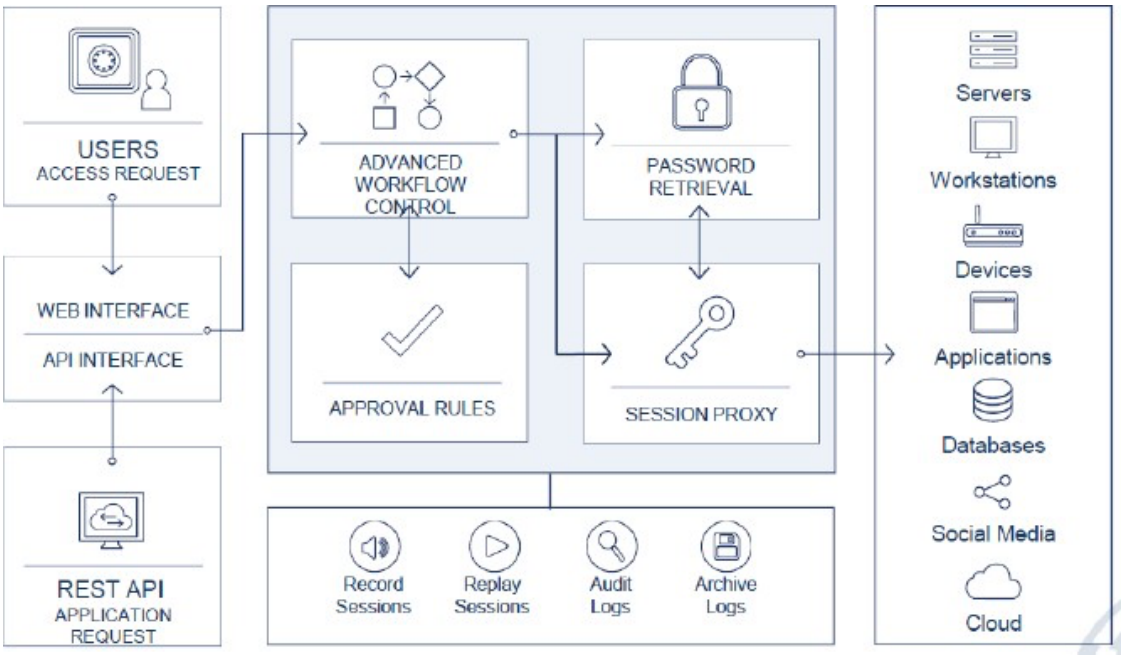

Figura 1. Arquitectura preliminar Password Safe
Fuente: El autor

- **FASE 2: Planificación de la Implementación**

En esta fase, se elaborará un documento detallado de alcance de la implementación y un cronograma del proyecto, asegurando que todas las partes estén alineadas en cuanto a expectativas y plazos. Se socializará y aceptará el cronograma con el cliente. Se prepararán y revisarán los requisitos de hardware, conectividad y permisos, así como los de usuarios y credenciales. También se definirán y revisarán los grupos de Active Directory y el listado y versiones de aplicaciones necesarias para la implementación. La fase concluye con la entrega y revisión de todos estos requisitos, formalizada mediante la firma del acta de entrega de requisitos.

Puntos relevantes de la fase 2:

- **Requisitos del Hardware**

se usarán 4 servidores para la solución, dos Virtual appliance con S.O Windows server de 48 GB de memoria R.A.M, ,949 GB de disco duro y procesados 2.70 GHz (8 procesadores). 2 servidores para los worker nodes con S.O Windows server de 24 GB, 400 GB de disco duro y 2.70 GHz de procesador.

Los dos appliance tendrán el software U-Series de beyondTrust y tendrán la configuración Activo/pasivo. El appliance nodo 1 sera el servidor activo y Appliance nodo 2 sera el failover como contingencia ante recuperación de desastres

Servidor	Sistema Operativo	Memoria	Disco	Procesador
Virtual Appliance Nodo 1	Windows server	48 GB	949 GB	2.70 GHz (8 Procesadores)
Virtual Appliance Nodo 2	Windows server	48 GB	949 GB	2.70 GHz (8 Procesadores)
Terminal Services Nodo 1	Windows server	24 GB	400 GB	2.70 GHz
Terminal Services Nodo 2	Windows server	24 GB	400 GB	2.70 GHz

Tabla 1. Requerimientos del Hardware

Fuente: El autor

- **Grupos active Directory**

Se define los grupos de usuarios que tendrán ciertos roles necesarios dentro de la plataforma *Password safe*, los Grupos se los dividirá por áreas que por el momento son dos grupos que intervendrán el departamento de Infraestructura y el de producción. Cada departamento tendrá roles de Aprobador y de solicitante.

Los roles de auditor y administrador, se configurará en un solo grupo y serán definidos de la siguiente manera:

PAM_Auditor: Permite a los usuarios de este directorio correr reportes y análisis

PAM_ISA: Permite a los usuarios de este directorio configurar cuentas y sistemas administrados

PAM_Approver_SO_REDES: Permite a los usuarios de este directorio aprobar solicitudes para la liberación de contraseñas administradas o archivos de conexión de sesión remota.

PAM_Approver_PROD: Permite a los usuarios de este directorio aprobar solicitudes para la liberación de contraseñas administradas o archivos de conexión de sesión remota.

PAM_Requestor_SO_REDES: Permite a los usuarios de este directorio enviar una solicitud para recuperar contraseñas administradas o archivos de conexión de sesión remota.

PAM_Requestor_PROD: Permite a los usuarios de este directorio enviar una solicitud para recuperar contraseñas administradas o archivos de conexión de sesión remota.

Grupo	Área	Rol
PAM_Auditor		Auditor
PAM_ISA		Administrador de Seguridad de la Información
PAM_Approver_SO_REDES	Infraestructura	Aprobador
PAM_Approver_PROD	Producción	Aprobador
PAM_Requestor_SO_REDES	Infraestructura	Solicitante
PAM_Requestor_PROD	Producción	Solicitante

Tabla 2. Grupos active Directory
Fuente: El autor

- **Definir las Políticas de accesos y contraseñas**

Se va a definir los siguientes grupos de políticas para la implementación de *Password safe*:

Políticas de Acceso: Se establecerán períodos de tiempo y frecuencia para que los usuarios soliciten contraseñas o inicien sesiones de acceso remoto, garantizando que estos accesos se realicen solo dentro de los horarios autorizados. También se implementarán restricciones para limitar el acceso a ciertos usuarios o grupos, basadas en sus roles específicos dentro de la organización.

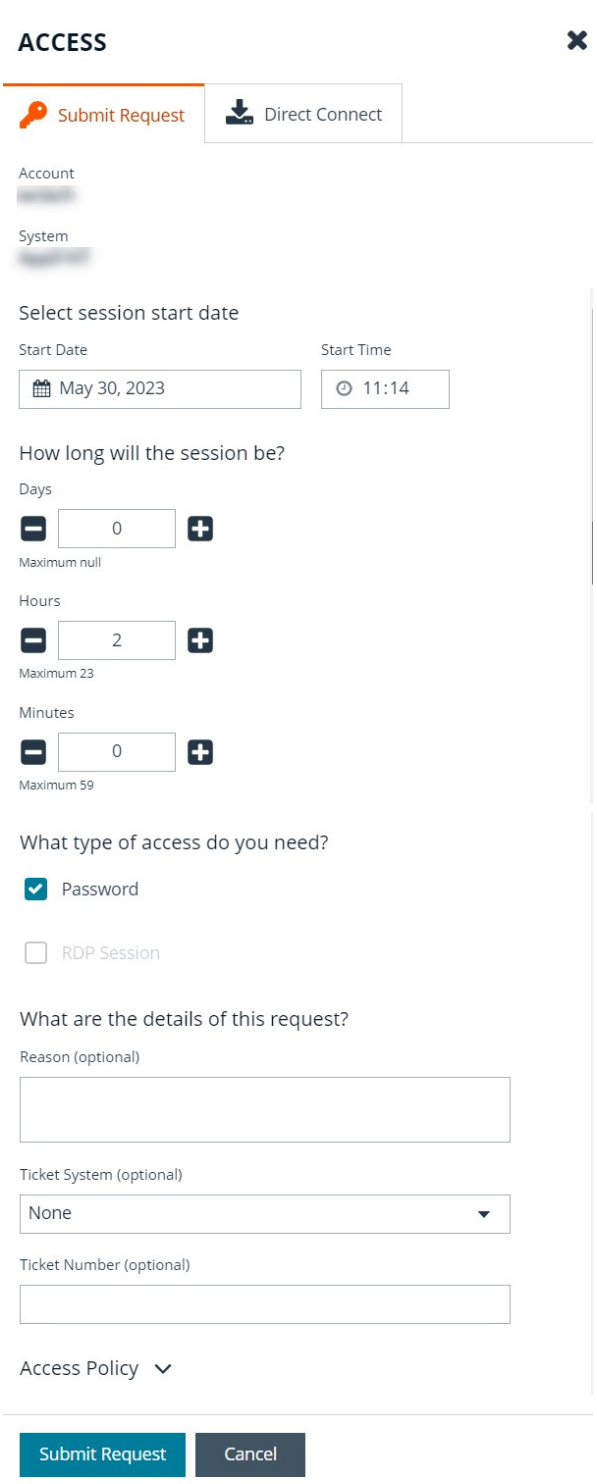

Figura 2. Solicitud de acceso

Fuente: El autor

Políticas de Contraseñas: Se configurará una política de contraseñas predeterminada, ajustando la longitud y la complejidad para cumplir con los estándares de seguridad. Además, se crearán nuevas políticas de contraseñas que especifiquen requisitos adicionales, como la expiración periódica de contraseñas y la imposibilidad de reutilizar contraseñas antiguas, asegurando una gestión robusta de credenciales.

- **Listado y versiones de Aplicaciones**

Como se mencionó, la plataforma *Password safe* permitirá el acceso luego de ser concedido, a distintas aplicaciones necesarias para la revisión, ejecución, actualización y eliminación de requerimientos de los solicitantes. Para esto se acuerda configurar en la plataforma appliance e instalar en los Nodos workers las siguientes aplicaciones:

- PuTTY versión 0.76
- WinSCP versión 5.21
- Microsoft SQL Server Management Studio versión 18.12
- Oracle SQL Developer versión 21.4
- Google Chrome versión 114.0.5735.199
- Microsoft Edge versión 114.0.1823.67
- FileZilla Client versión 3.62.2
- Cisco AnyConnect Secure Mobility Client versión 4.10.05095

- **Fase 3: Implementación de la solución**

- **Configuración inicial de los Virtual Appliance**

La implementación de la solución comienza con la instalación y configuración inicial de los componentes clave, seguida de la configuración de los dos virtual appliances. Este proceso incluye la actualización de ambos virtual appliances para asegurar que cuenten con las últimas mejoras y correcciones de seguridad. Además, se configurará un esquema de alta disponibilidad (HA) activo/pasivo en los dos virtual appliances, garantizando la continuidad operativa y la resiliencia del sistema. También se procederá con la configuración de hasta dos Worker Nodes, que permitirán distribuir las cargas de trabajo de manera eficiente y mantener el rendimiento óptimo del sistema.

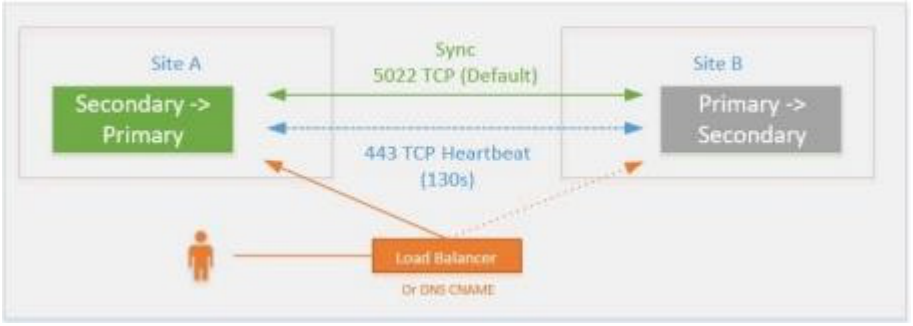

Figura 3. Esquema de recuperación Activo/Pasivo
Fuente: El autoir

Posteriormente, se realizará la activación de las licencias de Windows necesarias para el correcto funcionamiento de la solución. La última fase de esta implementación incluye la instalación de hasta 69 aplicaciones de conexión diferentes, abarcando una

amplia gama de herramientas y programas utilizados por los usuarios para acceder a los sistemas protegidos. Este enfoque integral garantiza que todos los componentes y aplicaciones necesarios estén correctamente configurados y operativos, brindando una plataforma segura y eficiente para la gestión de accesos y credenciales.

- **Configuración de PasswordSafe**

Una vez que se ha instalado el software PaswordSafe y se han realizado las configuraciones necesarias, se procede a la creación de cuentas, usuarios y assets, asegurando que todos los elementos necesarios estén integrados en el sistema.

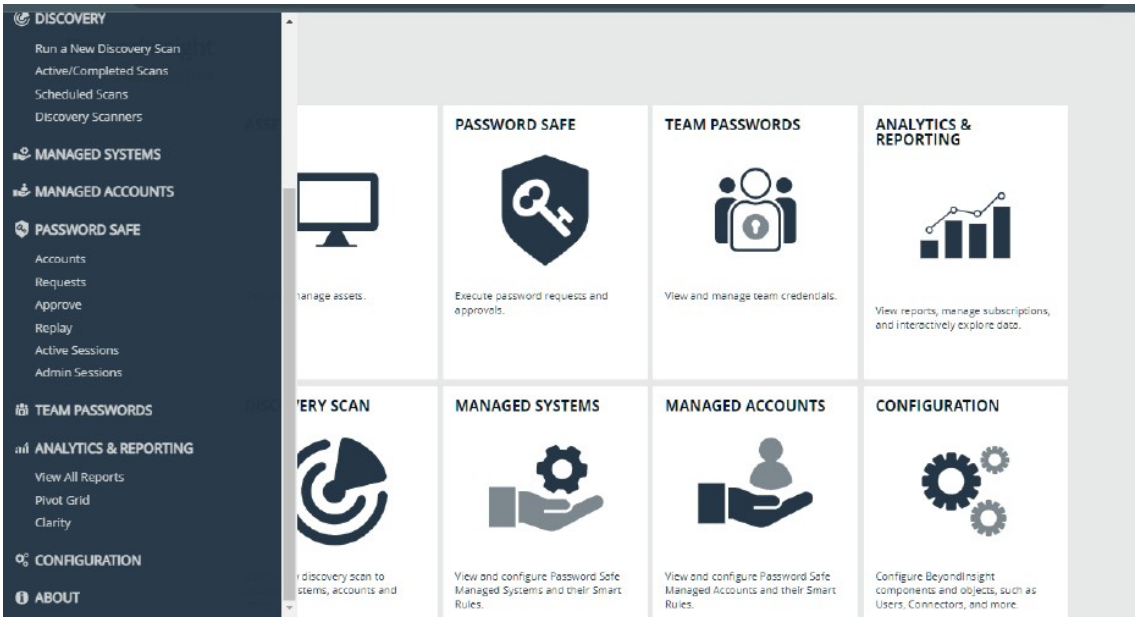

Figura 4. Creación de cuentas
Fuente: El autor

Luego, se procederá con la integración con Active Directory, lo cual permitirá una gestión centralizada y eficiente de las credenciales y accesos. También se crearán

hasta 20 cuentas funcionales para garantizar que todos los usuarios necesarios tengan acceso adecuado.

Se realizarán 11 escaneos para el descubrimiento de plataformas, afinando los resultados del escaneo y creando manualmente hasta 10 plataformas de cada tipo identificadas. Adicionalmente, se crearán hasta 4 políticas de password para asegurar que las contraseñas cumplan con los estándares de seguridad de la organización. Se mapearán los usuarios en hasta 4 grupos de Active Directory, configurando los roles de acceso a la consola de *Password safe*.

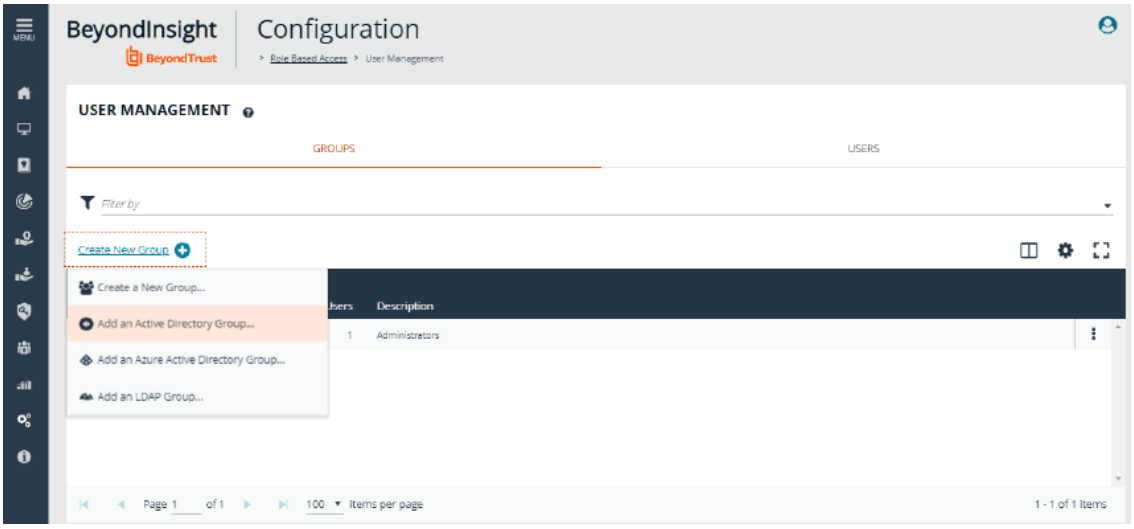

Figura 5. Creación de Active Directory Group
Fuente: El autor

La creación de hasta 11 Smart Rules permitirá añadir plataformas a *Password safe*, mientras que el afinamiento y las pruebas de estas Smart Rules asegurarán su correcta implementación. También se crearán Smart Rules para añadir cuentas a *Password safe* y se realizará su afinamiento y pruebas. Las cuentas serán incorporadas en la bóveda de credenciales para garantizar su seguridad.

Se configurarán hasta 4 reportes personalizados para proporcionar información detallada sobre el uso y acceso de las credenciales. La configuración y pruebas de sesiones y accesos incluirán diversas plataformas y aplicaciones. Para servidores Windows, se utilizará Escritorio Remoto/RDP, mientras que para servidores Unix/AIX/HPUX/Linux se emplearán Putty, TELNET y SSH. Para bases de datos, se utilizarán herramientas de línea de comandos como Putty, TELNET, SSH y Remote Desktop, además de aplicaciones específicas como PLSQL Developer, Cloud Control (Browser), Microsoft SQL Server y Management Studio.

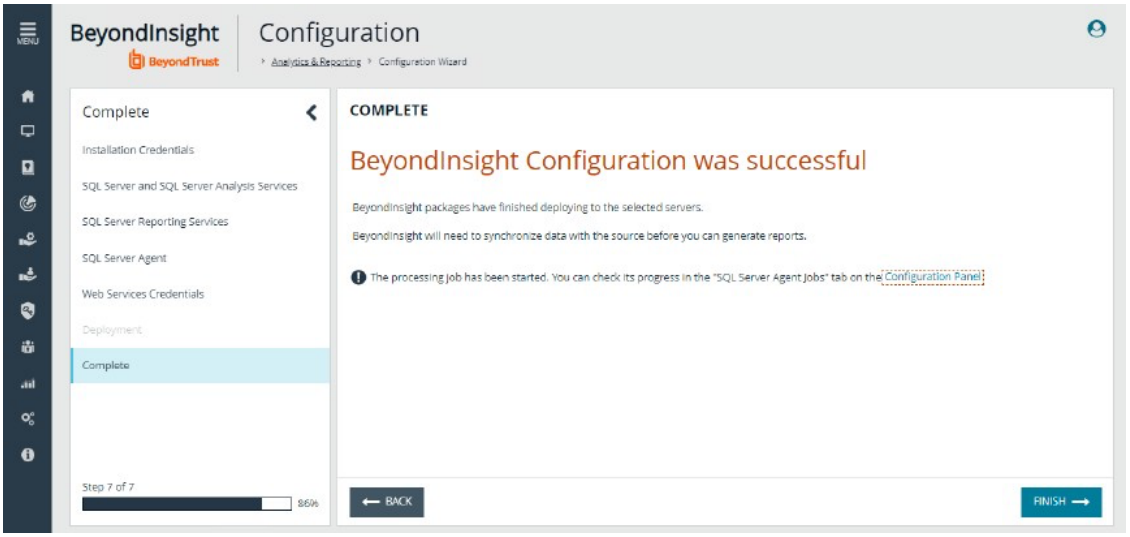

Figura 6. Configuración de reportaría

Fuente: El autor

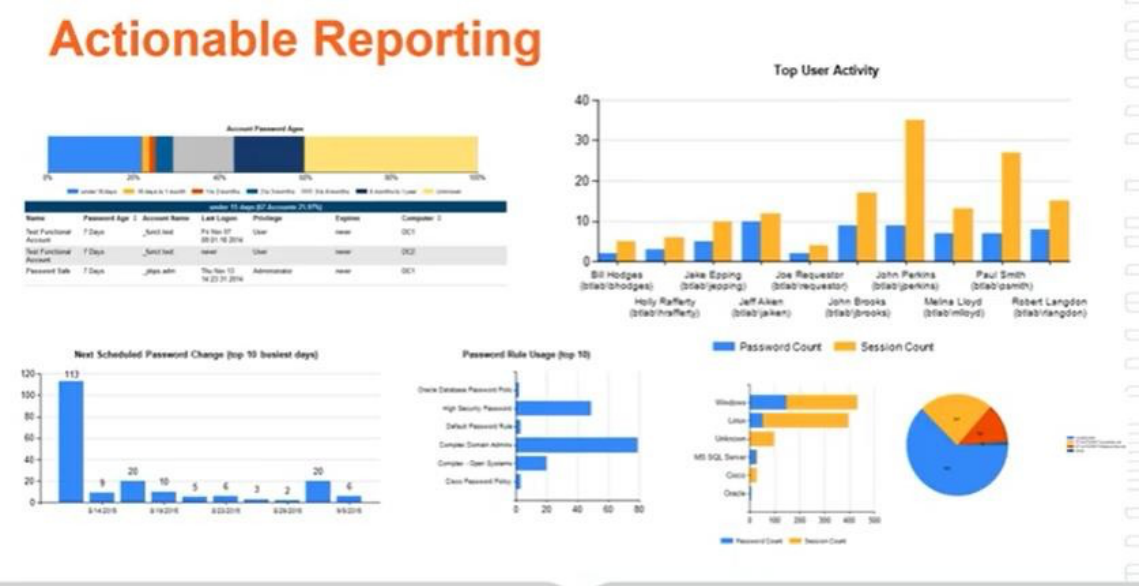

Figura 7. Ejemplo de reportes
Fuente: El autor

La configuración y pruebas también abarcarán sesiones en routers, switches y firewalls utilizando aplicaciones como TELNET, SSH y HTTPS. Se configurarán sesiones en consolas de navegadores web utilizando aplicaciones HTTPS. Se incluirán equipos destinados a la comunicación en redes móviles celulares y redes fijas, así como equipos de directorios (AD/LDAP) utilizando aplicaciones como Escritorio Remoto y Putty. Finalmente, se configurarán hasta 4 políticas de acceso y se implementará la autenticación multifactor (MFA) para la consola web de *Password Safe*, asegurando un nivel adicional de seguridad.

2.3. Pruebas

Se efectuarán pruebas integrales de la herramienta *Password safe* para confirmar que todas sus funcionalidades operan según lo esperado. Estas pruebas incluirán la evaluación de todas las características del sistema, desde la gestión de contraseñas hasta la supervisión y auditoría de

accesos, garantizando que la herramienta cumpla con los estándares de seguridad y rendimiento establecidos por la organización.

- **Pruebas de Acceso de Usuario Privilegiado**

Objetivo: Verificar que los usuarios privilegiados pueden acceder a las aplicaciones y sistemas configurados según las políticas definidas.

Descripción: Un usuario iniciará sesión con una cuenta estándar y luego utilizará *Password safe* para obtener acceso privilegiado a sistemas específicos como servidores Unix/Linux y Windows.

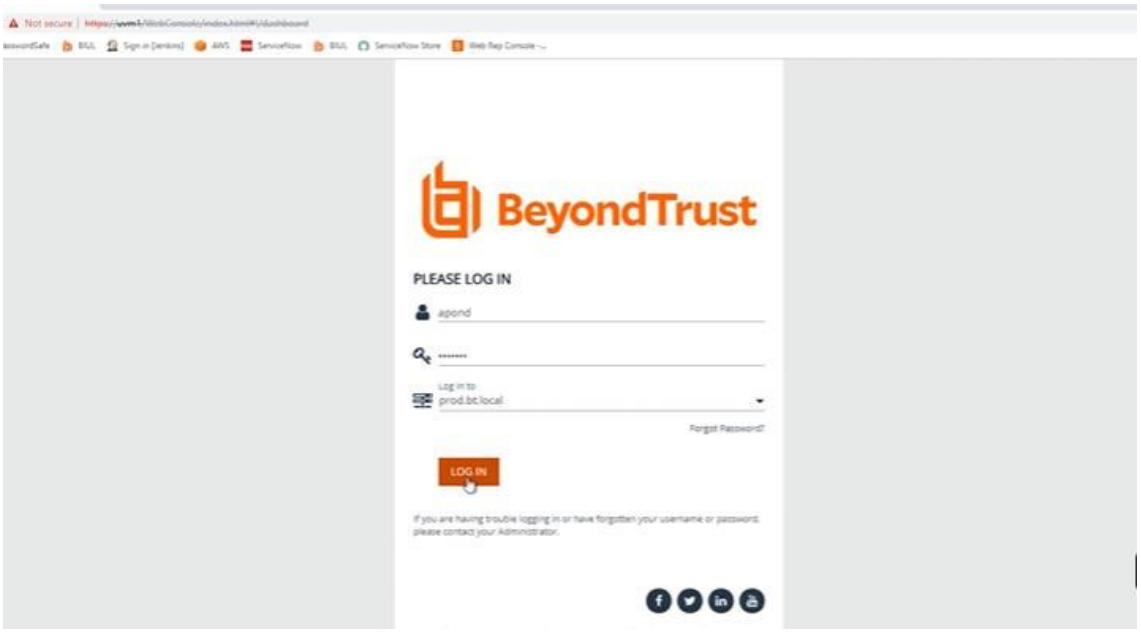

Figura 8. Usuario Inicia sesión

Fuente: El autor

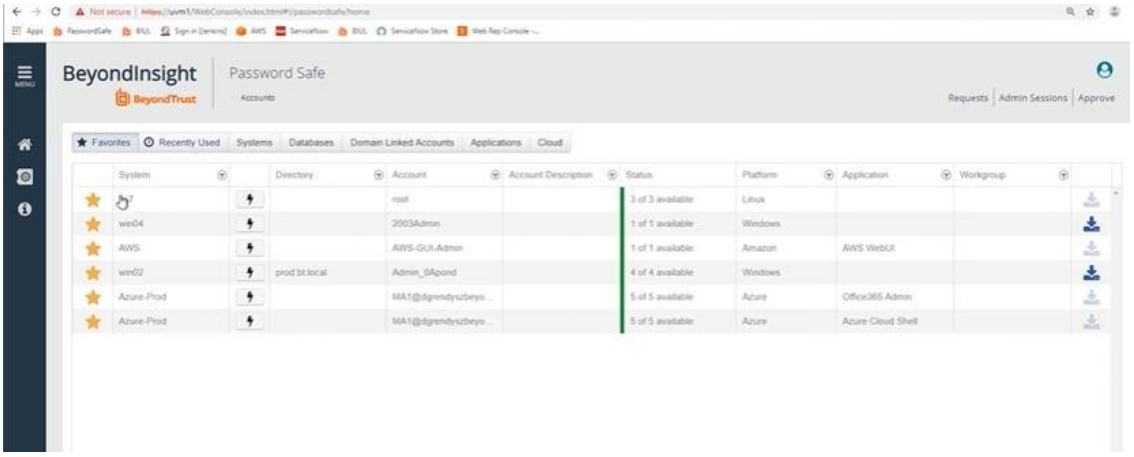

Figura 9. Selecciona el tipo de aplicación que quiere acceder

Fuente: El autor

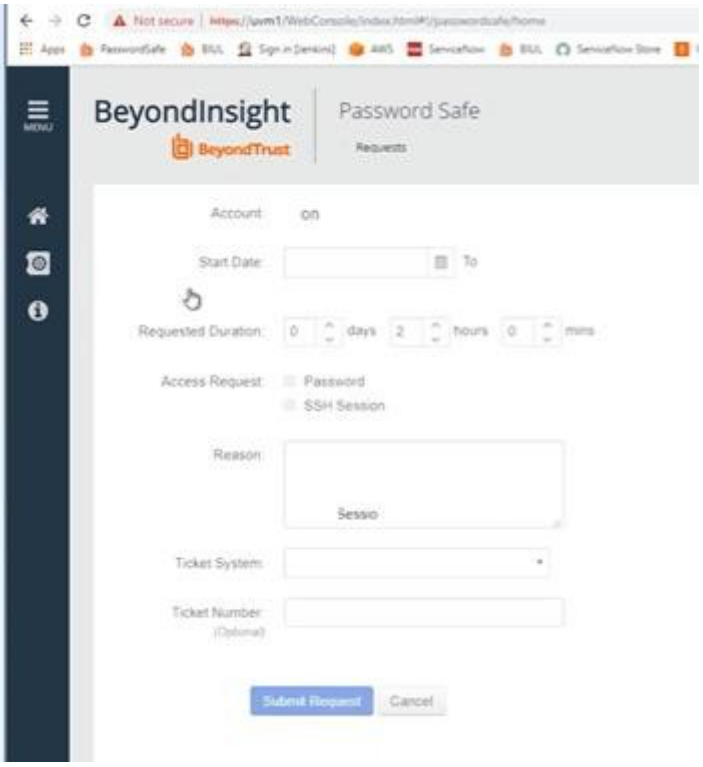

Figura 10. usuario indica cuando quiere acceder y el tiempo de sesión

Fuente: El autor

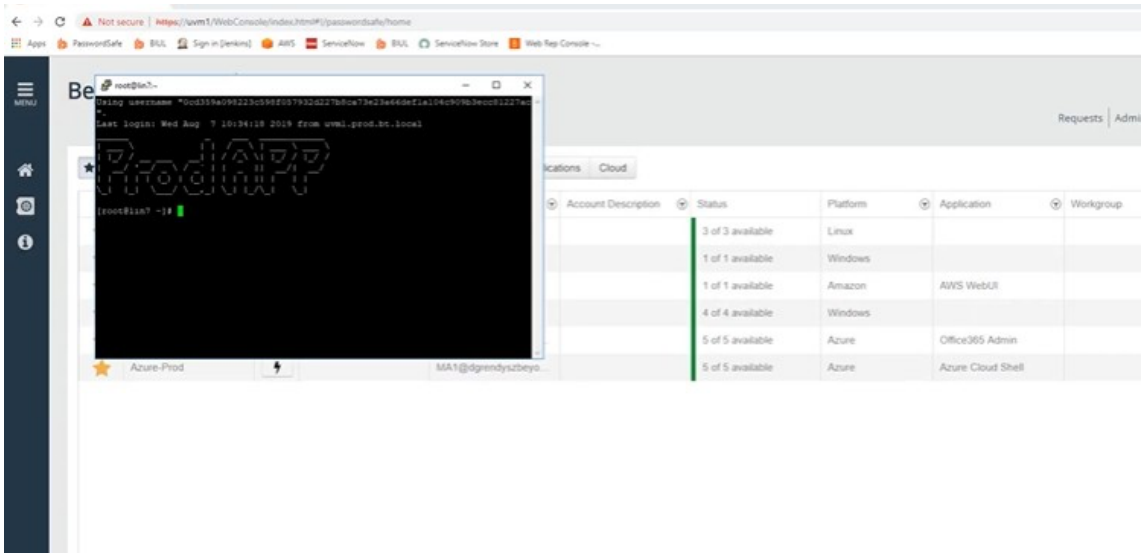

Figura 11. Luego de la aprobación, el usuario puede ingresar a la aplicación sin necesidad de ingresar contraseña

Fuente: El autor

Resultado: Los usuarios pueden acceder a los sistemas y aplicaciones sin conocer las contraseñas, y todas las actividades son monitoreadas y registradas.

- **Pruebas de Monitorización y Auditoría de Sesiones**

  Objetivo: Asegurar que todas las actividades de los usuarios privilegiados son registradas y pueden ser auditadas.

  Descripción: Mostrar cómo se registran las sesiones de SSH y RDP, incluyendo pulsaciones de teclas y comandos ejecutados. También se muestra cómo los administradores pueden ver y reproducir estas sesiones en tiempo real.

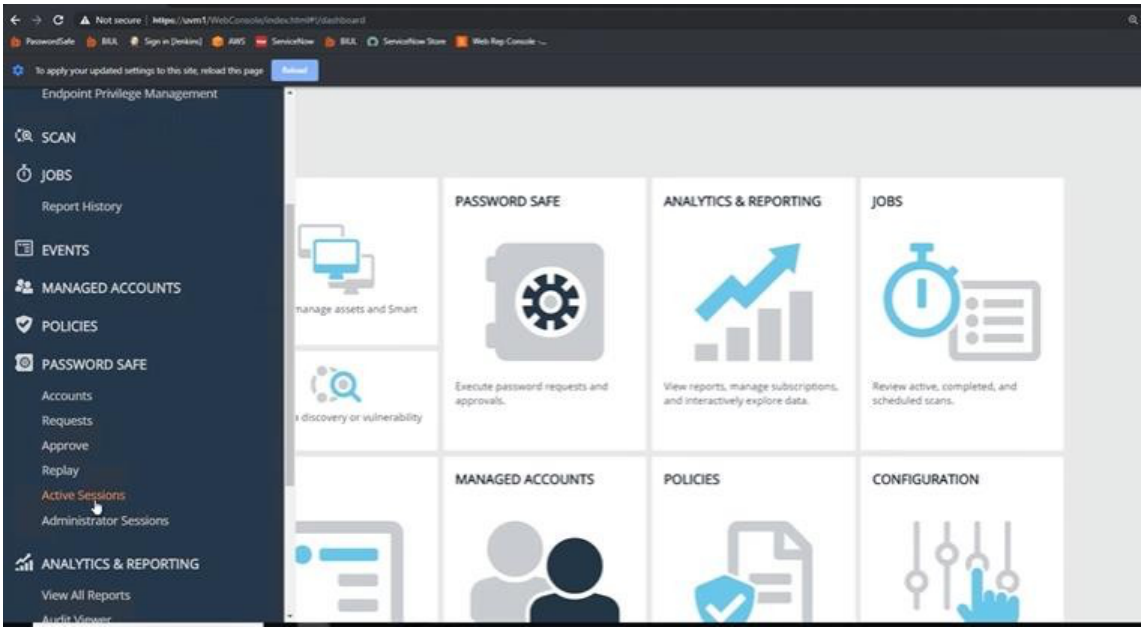

Figura 12. Revisión de las sesiones activas

Fuente: El autor

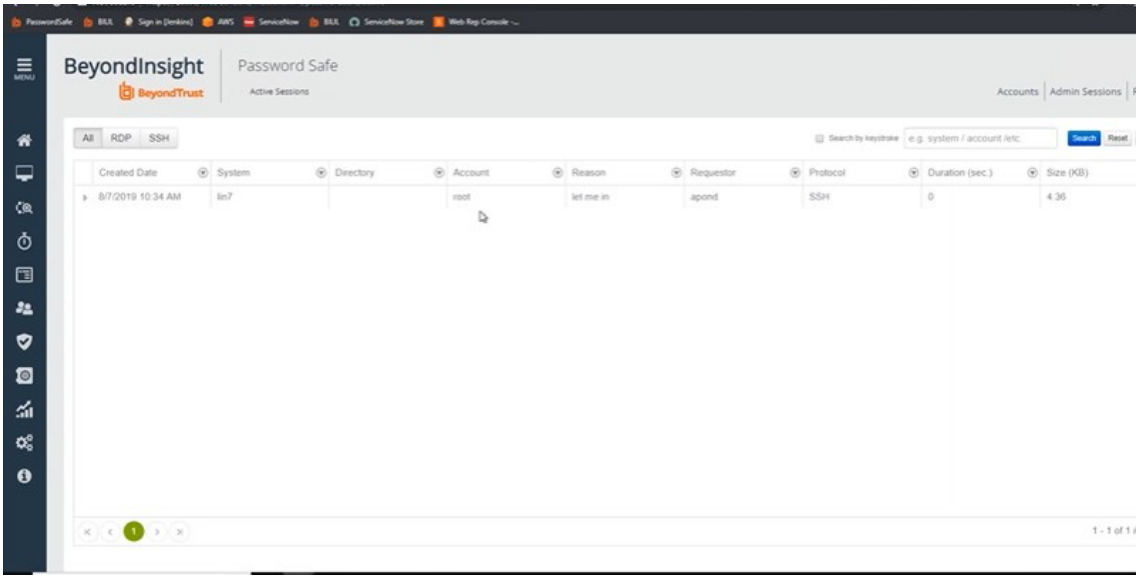

Figura 13. Se verifica la sesión del permiso anterior activa

Fuente: El autor

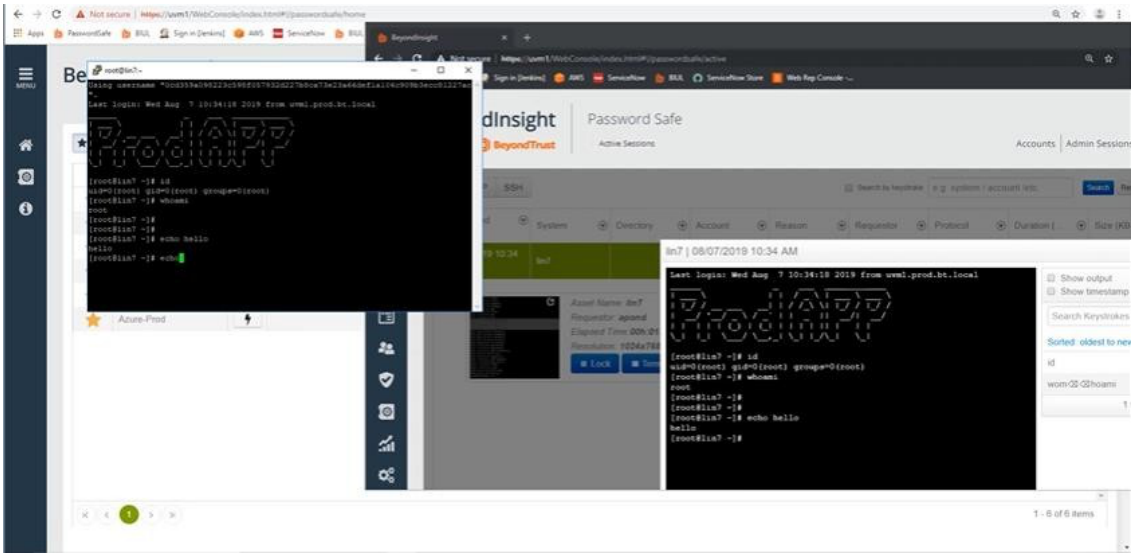

Figura 14. Monitoreo en vivo de la sesión del usuario
Fuente: El autor

Resultado: Todas las actividades son monitoreadas y registradas correctamente, permitiendo a los administradores reproducir sesiones y revisar actividades específicas.

- **Pruebas de Controles de Acceso Basados en Políticas**

Objetivo: Verificar que las políticas de acceso definidas se aplican correctamente y que los usuarios solo pueden acceder a los recursos permitidos.

Descripción: Pruebas de accesos a un servidor, pero solo a una aplicación dentro del servidor, en este ejemplo al Active Directory User Group.

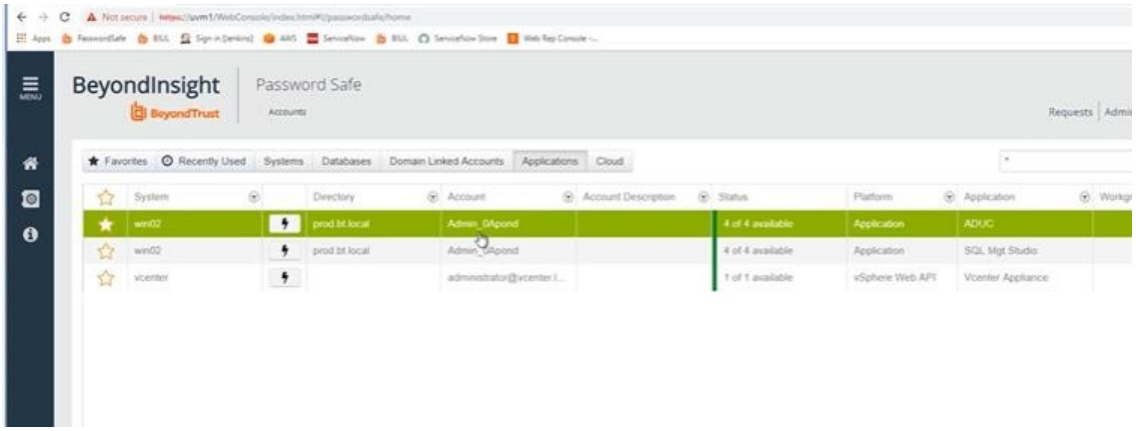

Figura 15. Se modifica el acceso solo a nivel de aplicación (ADUG) dentro del servidor

Fuente: El autor

Figura 16. Ingreso al servidor por medio de PasswordSafe

Fuente: El autor

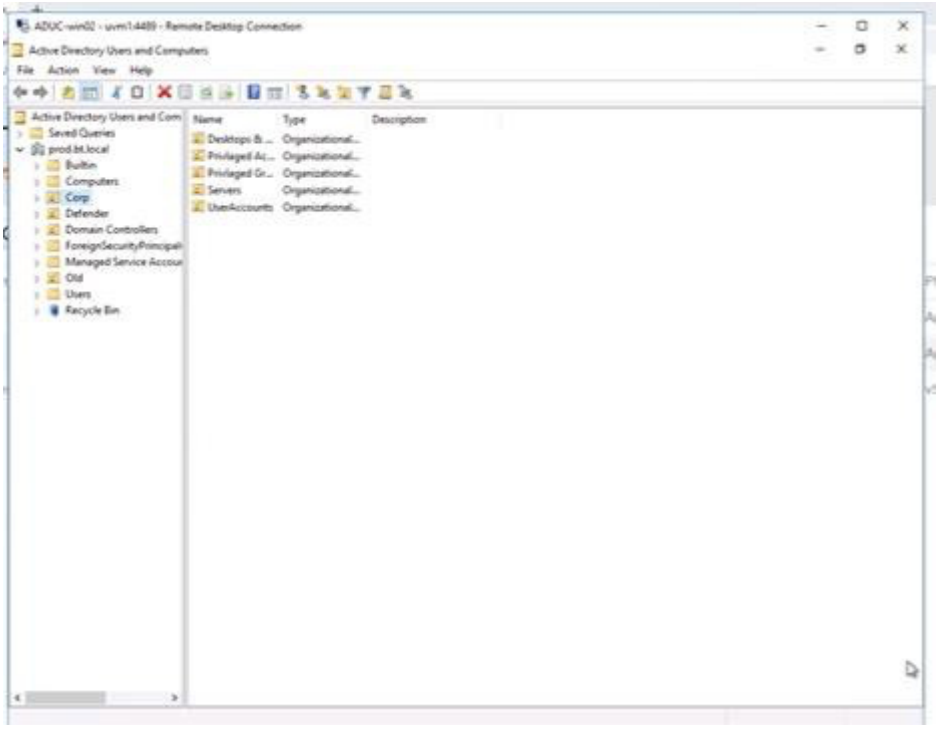

Figura 17.El usuario solo puede visualizar la aplicación con privilegios mínimos

Fuente: El autor

Resultado: Las políticas de acceso se aplican correctamente, y los usuarios solo pueden acceder a los recursos autorizados. Los intentos de acceso no autorizados son denegados y registrados. En esta prueba no puede salir de la aplicación de Active Directory que es a donde se concedió el permiso, tampoco tiene permiso de crear, solo es visualización.

- **Pruebas de Gestión de Contraseñas y Claves**

Objetivo: Verificar que PasswordSafe puede gestionar y rotar contraseñas y claves automáticamente.

Descripción: Se va a mostrar la capacidad de rotar contraseñas y claves SSH automáticamente después de su uso o cuando se alcanza el tiempo configurado.

Figura 18. se valida las políticas de contraseña del activo

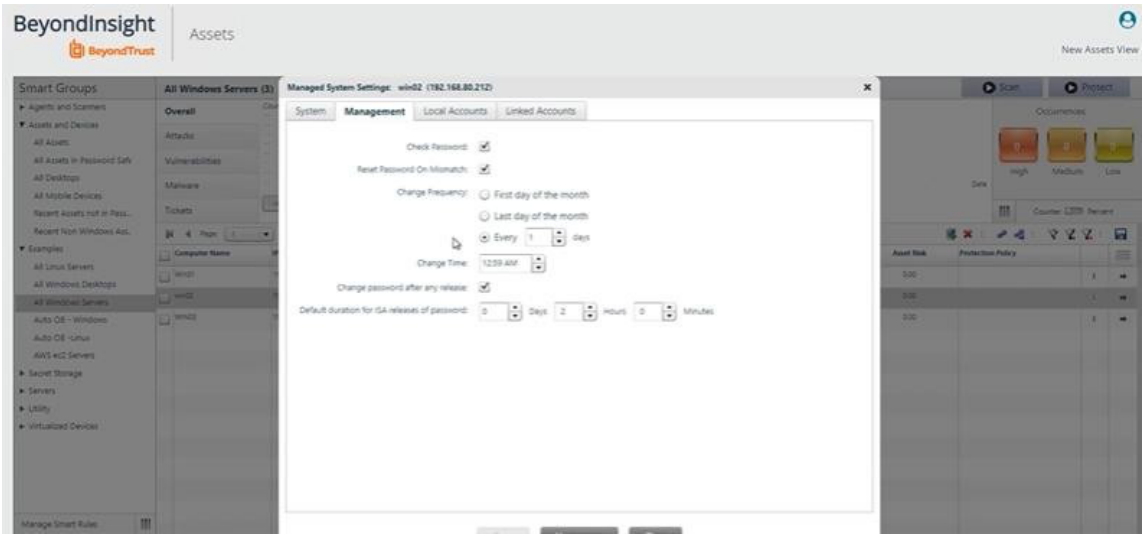

Figura 19. Validación de que la contraseña esté rotando
Fuente: El autor

Resultado: Las contraseñas y claves se rotan automáticamente según las políticas definidas, mejorando la seguridad y reduciendo el riesgo de exposición.

CAPÍTULO 3

EVALUACIÓN DE RESULTADOS

3.1. Accesos y seguridad

Resultado Obtenido:

- Los usuarios pueden acceder a sistemas y aplicaciones configuradas sin conocer las contraseñas.
- Las políticas de acceso basadas en roles permiten un control granular sobre quién puede acceder a qué recursos y cuándo.

Análisis:

- Eficiencia: La capacidad de permitir el acceso sin divulgar contraseñas reduce significativamente el riesgo de exposición de credenciales.
- Seguridad: Las políticas de acceso bien definidas garantizan que solo los usuarios autorizados puedan acceder a los recursos específicos, minimizando el riesgo de accesos no autorizados.
- Conformidad: El cumplimiento de políticas internas y regulaciones se facilita mediante la gestión centralizada de accesos.

3.2. Monitoreo y auditoria

Resultado Obtenido:

- Todas las actividades de los usuarios son monitoreadas y registradas, con capacidades para reproducir sesiones y revisar actividades específicas.

Análisis:

- Transparencia: La capacidad de grabar y revisar sesiones proporciona una visibilidad completa sobre el uso de cuentas privilegiadas.
- Responsabilidad: Los usuarios son conscientes de que sus actividades están siendo monitoreadas, lo que puede disuadir comportamientos indebidos.
- Auditorías Simplificadas: Los registros detallados y la capacidad de generar informes facilitan las auditorías y el cumplimiento de normativas.

3.3. Politicas de acceso

Resultado Obtenido:

- Las políticas de acceso se aplican correctamente, y los intentos de acceso no autorizados son denegados y registrados.

Análisis:

- Control de Acceso Fino: La capacidad de definir políticas detalladas y adaptativas asegura que los accesos se otorguen bajo las condiciones específicas definidas por la organización.
- Reducción de Riesgos: La implementación efectiva de políticas de acceso reduce el riesgo de accesos no autorizados y potenciales brechas de seguridad.

- Flexibilidad: La posibilidad de configurar flujos de autorización y requisitos de aprobación para accesos críticos permite una gestión más segura y controlada.

3.4. Automatización y rotación de contraseñas

Resultado Obtenido:

- *Password safe* gestiona y rota contraseñas y claves automáticamente después de su uso o según el tiempo configurado.

Análisis:

- *Seguridad Mejorada: La rotación automática de contraseñas y claves elimina la posibilidad de que credenciales antiguas sean explotadas por atacantes.*
- *Reducción de Carga Administrativa: La automatización de la gestión de contraseñas y claves libera recursos y reduce el esfuerzo manual necesario para mantener la seguridad de las credenciales.*
- *Conformidad Continua: La rotación regular de contraseñas contribuye al cumplimiento de políticas de seguridad* y regulaciones que exigen la actualización periódica de credenciales.

CONCLUSIONES Y RECOMENDACIONES

CONCLUSIONES

1. Mejora Integral de la Seguridad

La implementación de *Password safe* ofrece una mejora significativa en la seguridad de la gestión de accesos privilegiados. La solución automatiza y centraliza la gestión de contraseñas y claves, reduce el riesgo de exposición de credenciales y garantiza que solo los usuarios autorizados puedan acceder a los recursos críticos.

2. Monitoreo y Auditoría Exhaustiva

Password safe proporciona capacidades avanzadas de monitoreo y auditoría, registrando todas las actividades de los usuarios privilegiados y permitiendo la reproducción de sesiones. Esto no solo asegura la transparencia y la responsabilidad, sino que también facilita el cumplimiento de regulaciones y la realización de auditorías.

3. Automatización de Procesos Críticos

La automatización de la rotación de contraseñas y claves, junto con la gestión de sesiones, reduce la carga administrativa y minimiza el riesgo de errores humanos. La gestión automatizada de credenciales asegura que las políticas de seguridad se apliquen de manera consistente y oportuna.

4. Configuración y Gestión Sencillas

Password safe permite una configuración y gestión centralizadas y unificadas. La integración con sistemas como Active Directory y la capacidad de definir políticas de acceso basadas en roles y

condiciones específicas garantizan un control granular y coherente sobre los accesos a los recursos.

5. Resiliencia y Recuperación ante Desastres

El uso de dos appliances en modalidad activo/pasivo para la recuperación ante desastres garantiza la continuidad del servicio y la disponibilidad de la solución. Esta configuración permite una rápida conmutación por error en caso de fallo del sistema principal, asegurando que la gestión de accesos privilegiados no se vea interrumpida.

6. Escalabilidad y Flexibilidad

Password safe es altamente escalable y puede adaptarse al crecimiento y cambios en la infraestructura de TI de la organización. La capacidad de integrar nuevas aplicaciones y sistemas, junto con la posibilidad de ampliar las políticas de acceso, asegura que la solución siga siendo efectiva a medida que la organización evoluciona.

7. Fomentar una Cultura de Seguridad

La implementación de *Password safe* también contribuye a fomentar una cultura de seguridad dentro de la organización. La capacitación adecuada y la concienciación sobre la importancia de la gestión de credenciales y el cumplimiento de las políticas de seguridad refuerzan las prácticas de seguridad entre los empleados.

RECOMENDACIONES

1. **Planificación Detallada:**

    - Realizar una evaluación exhaustiva del entorno de TI para identificar todas las cuentas y sistemas que requerirán gestión de acceso privilegiado.

    - Definir claramente las políticas de acceso y los roles de usuario para asegurar una implementación exitosa.

2. **Configuración Inicial y Pruebas:**

    - Configurar los appliances en modalidad activo/pasivo para asegurar la recuperación ante desastres y realizar pruebas exhaustivas para garantizar que la configuración es correcta.

    - Asegurarse de que todas las políticas de acceso, monitoreo y auditoría estén correctamente implementadas y funcionando como se espera.

3. **Capacitación y Concienciación:**

    - Proporcionar capacitación adecuada a todos los usuarios privilegiados sobre el uso de *Password safe* y la importancia de seguir las políticas de seguridad.

    - Fomentar una cultura de seguridad dentro de la organización para asegurar que todos los empleados comprendan y respeten las mejores prácticas de seguridad.

4. **Monitoreo y Revisión Continua:**

    - Establecer procedimientos regulares de auditoría y revisión de las políticas de acceso para asegurarse de que se mantengan efectivas y actualizadas.

    - Utilizar las capacidades de análisis de amenazas y detección de anomalías de *Password safe* para identificar y responder rápidamente a cualquier comportamiento inusual o potencialmente malicioso.

5. **Escalabilidad y Mantenimiento:**

    - Planificar la escalabilidad de la solución para adaptarse a futuros crecimientos y cambios en la infraestructura de TI.

    - Realizar un mantenimiento regular y actualizaciones de la plataforma para asegurar que se mantenga al día con las últimas mejoras y parches de seguridad.

BIBLIOGRAFÍA

[1] D. Blum, *Privileged Access Management*, Auerbach Publications, 2020.

[2] J. Andress, *The Basics of Information Security*, Elssevier, 2011.

[3] BeyondTrust, «*What is Privileged Access Management (PAM)?* | *BeyondTrust*,» 2021. [En línea]. Available: https://www.beyondtrust.com/resources/glossary/privileged-access-management-pam.

[4] M. J. H. a. D. Rolls, *Privileged Attack Vectors: Building Effective Cyber-Defense Strategies to Protect Organizations*, Apress, 2018.

[5] T. Radichel, *Cybersecurity for Executives in the Age of Cloud*, Independently published, 2020.

[6] *L. Johnson, Security Controls Evaluation, Testing, and Assessment Handbook, Academic Press, 2019.*