



UNIVERSIDAD DE BURGOS  
ESCUELA POLITÉCNICA SUPERIOR  
Grado en Ingeniería Informática



**TFG del Grado en Ingeniería  
Informática**

**Implementación de una  
Prueba de Concepto (PoC) de  
Manage Engine PAM para la  
Gestión Eficiente de Acceso  
Privilegiado en Organizaciones**



Presentado por Alejandro Villar Solla  
en Universidad de Burgos — 11 de junio  
de 2024

Tutor: Luis Antonio Antolín Sánchez







UNIVERSIDAD DE BURGOS  
ESCUELA POLITÉCNICA SUPERIOR  
Grado en Ingeniería Informática



D. Luis Antonio Antolín Sánchez, profesor del Departamento de Ingeniería Informática, área Lenguajes y Sistemas Informáticos.

Expone:

Que el alumno D. Alejandro Villar Solla, con DNI 35581466Y, ha realizado el Trabajo final de Grado en Ingeniería Informática titulado título de TFG.

Y que dicho trabajo ha sido realizado por el alumno bajo la dirección del que suscribe, en virtud de lo cual se autoriza su presentación y defensa.

En Burgos, 11 de junio de 2024

Vº. Bº. del Tutor:

Vº. Bº. del co-tutor:

D. nombre tutor

D. nombre co-tutor





## Resumen

En el presente Trabajo Fin de Grado se aborda la implementación de una Prueba de Concepto (POC) de la solución PAM360 para la gestión de accesos privilegiados en la empresa NTT Data. La gestión de accesos privilegiados es una necesidad crítica en las organizaciones modernas, dado el creciente número de ciberamenazas y la importancia de proteger la información sensible.

La solución PAM360, desarrollada por ManageEngine, ofrece un conjunto completo de herramientas para administrar y asegurar los accesos privilegiados, garantizando que sólo las personas autorizadas puedan acceder a los recursos críticos de la empresa. Este proyecto se ha llevado a cabo en el contexto de NTT Data, una empresa líder en servicios de consultoría y tecnología, con el objetivo de mejorar su seguridad informática y cumplir con los estándares más exigentes de la industria.

Este proyecto no solo contribuye a fortalecer la seguridad de NTT Data, sino que también ofrece una guía práctica y detallada sobre cómo implementar soluciones de gestión de accesos privilegiados en organizaciones de gran envergadura.

## Descriptores

PAM360, ciberseguridad, gestión de accesos, prueba de concepto (POC), control de privilegios, compliance, Privileged Access Management... .

## **Abstract**

This Final Degree Project addresses the implementation of a Proof of Concept (POC) of the PAM360 solution for privileged access management in the company NTT Data. Privileged access management is a critical necessity in modern organizations, given the growing number of cyber threats and the importance of protecting sensitive information.

The PAM360 solution, developed by ManageEngine, offers a comprehensive set of tools to manage and secure privileged access, ensuring that only authorized individuals can access business-critical resources. This project has been carried out in the context of NTT Data, a leading consulting and technology services company, with the aim of improving its IT security and complying with the most demanding standards in the industry.

This project not only contributes to strengthening NTT Data's security, but also provides practical and detailed guidance on how to implement privileged access management solutions in large organizations.

## **Keywords**

PAM360, cybersecurity, access management, proof of concept (POC), privilege control, compilation, Privileged Access Management...



---

# Índice general

---

<b>Índice general</b>	<b>iii</b>
<b>Índice de figuras</b>	<b>v</b>
<b>Índice de tablas</b>	<b>vi</b>
<b>1. Introducción</b>	<b>1</b>
1.1. Contexto y motivación . . . . .	1
1.2. Justificación del Proyecto . . . . .	2
1.3. Metodología . . . . .	2
1.4. Estructura . . . . .	3
<b>2. Objetivos del Proyecto</b>	<b>5</b>
2.1. Objetivos Funcionales . . . . .	5
2.2. Objetivos Técnicos . . . . .	6
2.3. Objetivos de Mejora y Futuro . . . . .	6
<b>3. Conceptos teóricos</b>	<b>9</b>
3.1. Gestión de Accesos Privilegiados (PAM) . . . . .	9
3.2. Active Directory (AD) . . . . .	9
3.3. Prueba de Concepto (POC) . . . . .	10
3.4. PAM360 . . . . .	10
3.5. Seguridad de la Información . . . . .	10
3.6. Zero Trust . . . . .	10
3.7. Integración de Sistemas . . . . .	11
3.8. Auditoría y Monitoreo de Seguridad . . . . .	11

<b>4. Técnicas y herramientas</b>	<b>13</b>
4.1. Metodologías . . . . .	13
4.2. Herramientas de desarrollo . . . . .	13
4.3. Tecnologías y bibliotecas . . . . .	14
4.4. Comparativas y justificaciones . . . . .	14
<b>5. Aspectos relevantes del desarrollo del proyecto</b>	<b>17</b>
5.1. Aspectos relevantes del desarrollo del proyecto . . . . .	17
5.2. Planificación del proyecto . . . . .	17
5.3. Despliegue de la máquina virtual . . . . .	19
5.4. Instalación de PAM360 . . . . .	19
5.5. Configuración inicial de PAM360 . . . . .	21
5.6. Integración con Active Directory . . . . .	23
5.7. Importación de máquinas de nuestro entorno . . . . .	26
5.8. Gestión de contraseñas y acceso . . . . .	26
5.9. Monitorización y auditoría . . . . .	28
5.10. Resultados y validación . . . . .	29
<b>6. Conclusiones y Líneas de trabajo futuras</b>	<b>33</b>
6.1. Conclusiones . . . . .	33
6.2. Líneas de Trabajo Futuras . . . . .	34
<b>Bibliografía</b>	<b>37</b>

---

## Índice de figuras

---

5.1. Diagrama del proyecto. . . . .	17
5.2. Detalle del diagrama de Gantt. . . . .	18
5.3. Detalle del diagrama de Gantt: fase de desarrollo. . . . .	18
5.4. Detalles de la máquina virtual en vSphere. . . . .	19
5.5. Configuración más detallada de la máquina virtual en vSphere. . . . .	19
5.6. Proceso de instalación de PAM360. . . . .	20
5.7. Proceso de instalación de PAM360, primera página. . . . .	20
5.8. Proceso de instalación de PAM360, segunda página. . . . .	21
5.9. Proceso de instalación de PAM360, tercera y última página. . . . .	21
5.10. Pantalla principal de PAM. . . . .	22
5.11. Configuración del administrador en PAM360. . . . .	22
5.12. Configuración del administrador en PAM360. . . . .	23
5.13. Configuración del administrador en PAM360. . . . .	23
5.14. Importación de usuarios desde Active Directory. . . . .	24
5.15. Configuración del administrador en PAM360. . . . .	24
5.16. AD con la cuenta de pam activo. . . . .	25
5.17. AD con la cuenta de pam activo. . . . .	25
5.18. Gestión de contraseñas en PAM360. . . . .	26
5.19. Gestión de contraseñas en PAM360. . . . .	27
5.20. Selección de usuario. . . . .	27
5.21. Selección de usuario. . . . .	28
5.22. Configuración del administrador en PAM360. . . . .	28
5.23. Monitorización de actividades en PAM360. . . . .	29
5.24. PAM360 configurado y operando. . . . .	29
5.25. Monitorización de actividades en PAM360 en formato HTML. . . . .	30
5.26. Resultados de la validación del sistema. . . . .	31

---

# Índice de tablas

---

4.1. Comparación de PAM360 vs BeyondTrust vs CyberArk . . . . .	14
---	----

---

# 1. Introducción

---

Descripción del contenido del trabajo y de la estructura de la memoria y del resto de materiales entregados.

## 1.1. Contexto y motivación

Hoy en día, la seguridad informática y la gestión de accesos son dos áreas principales que no deben ser subestimadas en una organización, especialmente si se trata de organizaciones que procesan información delicada y requieren la seguridad de la integridad de sus sistemas. NTT Data es una consultoría con una parte de ciberseguridad muy reconocida que se enfrenta al desafío de gestionar sus accesos de una manera segura y eficiente, ya sea de parte de sus empleados u otros clientes externos.

El alto grado de rotación y la necesidad de permitir accesos de manera temporal complican aún más este desafío.

En este contexto, PAM360 [8] es una solución de Gestión de Acceso Privilegiado de extremo a extremo que proporciona un control seguro centralizado de todo el acceso a los recursos empresariales críticos. Ayuda a rastrear todos los movimientos y cambios realizados para la seguridad de un usuario.

He elegido esta tarea que he tenido que realizar en NTT Data porque estoy muy interesado en el área de ciberseguridad. Me gustaría trabajar como pentester<sup>1</sup> en mi futuro laboral, así que creo que es una gran oportunidad para aprender nuevas tecnologías de seguridad informática observando su desarrollo desde dentro.

---

<sup>1</sup>Un pentester es un profesional que realiza pruebas de penetración para identificar y solucionar vulnerabilidades en sistemas de seguridad.

## 1.2. Justificación del Proyecto

La elección de este proyecto es una decisión consensuada con mi tutor en NTT Data, con la sugerencia de implementar una POC para la solución PAM360 en términos de alta seguridad y efectividad en la administración de accesos, ya que la consultora requiere, con sus múltiples clientes y proyectos, un sistema fuerte que soporte la administración de accesos sin comprometer la seguridad.

PAM360 es una solución que puede gestionar y monitorizar los accesos en tiempo real, lo cual es una mejora con respecto a la característica que tenía anteriormente, mediante la cual se solían inscribir a numerosos usuarios dentro del AD de la empresa y estar pendiente de cuándo se expiran cuentas, de los accesos inapropiados, de los cambios de sudoers en linux, etc.

Esta iniciativa está justificada por los beneficios esperados de la implementación de PAM360, que incluyen:

- Mejora en la seguridad: Al permitir un mejor control y monitoreo de los accesos, se minimiza el riesgo de accesos no autorizados y se garantiza la integridad de los sistemas de la organización.
- Eficiencia en la gestión de accesos: La centralización de la gestión de accesos permite una administración más sencilla y eficiente, reduciendo la carga de trabajo del equipo de respuesta y prevención.
- Flexibilidad y escalabilidad: PAM360 permite adaptarse a las necesidades cambiantes de la empresa, facilitando la gestión de usuarios temporales y externos. En caso de que el usuario necesite privilegios adicionales en cualquier sistema, se pueden asignar directamente desde la misma solución en un ambiente controlado. Se pueden asignar o revocar accesos en cualquier momento.

## 1.3. Metodología

Para la realización de este proyecto, se seguirán los siguientes pasos metodológicos:

- Revisión de documentación: Investigación y revisión de la documentación técnica relacionada con el tema de gestión de acceso privilegiado y PAM360, por ejemplo, los manuales de ManageEngine y las experiencias de los usuarios

- Planificación y preparación: Establecimiento del alcance del plan de pruebas, preparación y configuración del entorno de pruebas.
- Implementación: Despliegue y configuración de PAM360, integración con AD y realización de pruebas funcionales y de seguridad.
- Evaluación y análisis: Análisis de los resultados, evaluación de la eficacia y efectividad de PAM360.
- Documentación: Redacción del informe final del proyecto, incluyendo la descripción del proceso, resultados obtenidos, capturas, reportes, conclusiones y recomendaciones.

## 1.4. Estructura

Este documento está organizado de la siguiente manera:

- Introducción: Presenta el contexto, la justificación, los objetivos, la metodología y la estructura del documento.
- Objetivos del Proyecto: Detalla los objetivos específicos y generales del proyecto.
- Conceptos Teóricos: Explica los conceptos teóricos necesarios para entender la gestión de accesos privilegiados y la tecnología subyacente en PAM360.
- Secciones: Desglosa las diferentes partes del tema.
- Referencias: Lista las fuentes y material consultado.
- Imágenes: Presenta diagramas y capturas relevantes.
- Listas de ítems: Enumera elementos clave y funcionalidades.
- Tablas: Ofrece tablas de datos y comparativas.
- Técnicas y Herramientas: Describe las técnicas y herramientas utilizadas durante la implementación y pruebas de PAM360.
- Aspectos Relevantes del Desarrollo del Proyecto: Aborda los desafíos y consideraciones importantes encontrados durante la configuración y pruebas de PAM360.

- Trabajos Relacionados: Revisa otros trabajos y estudios similares para situar el proyecto en un contexto más amplio.
- Conclusiones y Líneas de Trabajo Futuras: Presenta las conclusiones del proyecto y sugiere posibles líneas de trabajo futuras para mejorar y expandir la implementación de PAM360 en NTT Data.
- Anexos: Incluyen el resto de información que no se ha podido incluir en esta memoria



---

## 2. Objetivos del Proyecto

---

El desarrollo de este proyecto tiene como propósito principal implementar y evaluar una Prueba de Concepto (POC) de la solución PAM360 en la infraestructura de NTT Data. Para lograr este propósito, se establecen varios objetivos específicos que abarcan tanto los requisitos funcionales del software como los objetivos técnicos necesarios para llevar a cabo el proyecto de manera satisfactoria. A continuación, se detallan estos objetivos:

### 2.1. Objetivos Funcionales

- **Despliegue de PAM360:**

- Configurar y desplegar PAM360 en una máquina proporcionada por NTT Data, asegurando que funcione correctamente y esté bien integrada dentro de los parámetros de seguridad de la empresa.

- **Gestión de Accesos:**

- Implementar la funcionalidad de PAM360 para gestionar los accesos a las máquinas por parte de los usuarios del Active Directory (AD), tanto internos como clientes, asegurando que todos los accesos sean monitoreados y controlados.

- **Seguridad y Control:**

- Asegurar que PAM360 proporcione un control estricto y seguro de los accesos, minimizando el riesgo de accesos no autorizados y mejorando la seguridad interna de la infraestructura de NTT Data.

## 2.2. Objetivos Técnicos

### ■ Integración con Active Directory:

- Integrar PAM360 con el sistema de Active Directory (AD) de NTT Data para centralizar la gestión de accesos y facilitar la administración de usuarios.

### ■ Configuración y Personalización:

- Realizar la configuración inicial de PAM360, ajustando los parámetros y opciones para que se adapten a las necesidades específicas de la empresa y aseguren un funcionamiento óptimo.

### ■ Pruebas de Funcionamiento y Seguridad:

- Llevar a cabo una serie de pruebas funcionales y de seguridad para verificar que PAM360 opera correctamente, identificando y resolviendo cualquier problema que pueda surgir durante el proceso.

### ■ Documentación del Proceso:

- Documentar detalladamente cada fase del proyecto, desde la configuración y despliegue hasta las pruebas y resultados, recopilando todos los datos al finalizar.

### ■ Evaluación de Resultados:

- Evaluar el rendimiento y la efectividad de PAM360 en la gestión de accesos y la mejora de la seguridad, recopilando datos y métricas que permitan analizar su funcionamiento.

## 2.3. Objetivos de Mejora y Futuro

### ■ Optimización Continua:

- Identificar posibles mejoras en la configuración y uso de PAM360 para optimizar su rendimiento y adaptabilidad a futuros proyectos que se oferten en la empresa.

### ■ Capacitación y Transferencia de Conocimiento:

- Asegurar que el equipo de TI de NTT Data esté capacitado para utilizar y mantener PAM360, proporcionando la formación necesaria y transfiriendo el conocimiento adquirido durante el proyecto.

■ **Propuestas de Mejora:**

- Sugerir posibles mejoras y nuevas funcionalidades para futuras versiones de PAM360, basadas en la experiencia obtenida durante la POC y el feedback propio.

Los objetivos de este proyecto no solo buscan implementar y evaluar la funcionalidad de PAM360, sino también asegurar que la solución se integre de manera eficiente y segura en la infraestructura de NTT Data, proporcionando un control efectivo de los accesos y mejorando la seguridad informática de la empresa.



---

## 3. Conceptos teóricos

---

Este proyecto requiere entender varios conceptos teóricos fundamentales relacionados con la gestión de accesos privilegiados y las herramientas utilizadas, los cuales explicaré a continuación.

### 3.1. Gestión de Accesos Privilegiados (PAM)

La gestión de accesos privilegiados (PAM) es una rama de la ciberseguridad que se centra en controlar y supervisar los accesos de los usuarios con privilegios avanzados a los sistemas críticos de una organización. Estos usuarios privilegiados tienen permisos especiales dados por responsables y en todo momento controlados que les permiten acceder a información sensible, modificar configuraciones del sistema y realizar tareas administrativas. Implementar una solución PAM es esencial para prevenir accesos no autorizados, reducir riesgos de seguridad y cumplir con las normativas (Barrett, 2020) [1] .

### 3.2. Active Directory (AD)

Active Directory (AD) es un servicio desarrollado por Microsoft, utilizado en redes de dominio de Windows. Su función principal es gestionar y almacenar información sobre los recursos de la red y los usuarios, permitiendo a los administradores gestionar permisos y controlar el acceso a los recursos de la red de manera centralizada. En este proyecto, AD es fundamental, ya que se integra con PAM360 para gestionar los accesos de los usuarios (Microsoft, 2024) [9].

### 3.3. Prueba de Concepto (POC)

Una Prueba de Concepto (POC) es una implementación preliminar de una solución destinada a demostrar su viabilidad y efectividad. En este trabajo, la POC se centra en desplegar y configurar PAM360 en un entorno controlado, comprobando que cumple con los requisitos y expectativas de la empresa. Esta etapa es crucial para identificar posibles problemas y asegurar que la solución es adecuada antes de una implementación a mayor escala (Smith, 2019) [12].

### 3.4. PAM360

PAM360 es una solución integral de gestión de accesos privilegiados desarrollada por ManageEngine. Ofrece funcionalidades avanzadas para controlar, auditar y monitorear el acceso de usuarios privilegiados a recursos sensibles de la empresa. Sus características principales incluyen la gestión de contraseñas, sesiones privilegiadas, auditoría de accesos y generación de informes. PAM360 destaca por su capacidad de integración con diversas plataformas y su facilidad de uso (ManageEngine, 2023) [8].

### 3.5. Seguridad de la Información

La seguridad de la información es una disciplina que se ocupa de proteger la información contra accesos no autorizados, modificaciones indebidas y destrucción. Incluye principios fundamentales como la confidencialidad, integridad y disponibilidad. Implementar una solución PAM contribuye correctamente a la seguridad de la información al garantizar que solo los usuarios autorizados puedan acceder a sistemas y datos críticos (Whitman and Mattord, 2022) [14].

### 3.6. Zero Trust

El modelo de seguridad Zero Trust se basa en el principio de que las amenazas pueden provenir tanto del interior como del exterior de la red. En lugar de asumir que las entidades dentro de la red son de confianza, Zero Trust requiere verificación continua de identidad y contexto para otorgar acceso. PAM360 facilita la implementación de este modelo al gestionar y supervisar los accesos privilegiados de manera estricta (Kindervag, 2010) [7].

### 3.7. Integración de Sistemas

La integración de soluciones PAM con otros sistemas de TI, como SIEM (Security Information and Event Management), IAM (Identity and Access Management), y herramientas de monitoreo, es crucial para una gestión de seguridad efectiva. Esta integración permite una visión holística de la seguridad y facilita la detección y respuesta a incidentes (Johnson, 2018) [6].

### 3.8. Auditoría y Monitoreo de Seguridad

La auditoría y el monitoreo continuo son componentes esenciales de una estrategia de ciberseguridad. Registrar y analizar las acciones de los usuarios privilegiados permite detectar actividades sospechosas y responder a incidentes de manera oportuna. PAM360 ofrece capacidades avanzadas de auditoría y generación de informes, proporcionando visibilidad completa sobre el uso de accesos privilegiados (Moore, 2021) [10].

Este apartado ha sintetizado los conceptos teóricos necesarios para comprender el desarrollo del proyecto. La correcta comprensión e implementación de estos conceptos es fundamental para el éxito de la gestión de accesos privilegiados en cualquier organización.





---

## 4. Técnicas y herramientas

---

### 4.1. Metodologías

Para llevar a cabo este proyecto, se utilizó la metodología de diagrama de Gantt [5]. Esta metodología es utilizada en la empresa NTT Data en todos los proyectos, y se aplicó de igual manera en la prueba de concepto (POC) de PAM360. La elección de esta metodología se basó en su eficacia para la gestión del tiempo y las tareas, permitiendo una planificación y seguimiento detallado del proyecto. Al utilizar el diagrama de Gantt, se logró una clara visualización de las distintas fases del proyecto, facilitando la identificación de dependencias y el cumplimiento de los plazos establecidos.

### 4.2. Herramientas de desarrollo

En el desarrollo del proyecto se emplearon diversas herramientas, cada una seleccionada por su idoneidad para las tareas específicas:

- **mRemote** [11]: Se utilizó para conectarse al servidor de PAM. Esta herramienta permite gestionar múltiples conexiones de manera eficiente, lo cual fue crucial para acceder y configurar el servidor de PAM360.
- **Habilitación de puertos**: Se habilitó el puerto 8282 para permitir la conexión desde el PC de la empresa al servidor de PAM. Esta configuración fue esencial para asegurar la comunicación entre los sistemas.
- **Windows**: El sistema operativo utilizado para el servidor de PAM y para las operaciones de configuración.

- **Chrome:** Utilizado para acceder a la interfaz web de PAM360, facilitando la administración y configuración del software.
- **Firewall Fortinet [4]:** Firewall de NTT Data, necesario para conceder permisos de conexión a la máquina de PAM

La elección de estas herramientas se basó en su eficacia para la realización de las tareas y en las pautas establecidas por la empresa.

### 4.3. Tecnologías y bibliotecas

En este proyecto, no se utilizaron lenguajes de programación, frameworks o bibliotecas específicos, dado que el enfoque principal fue la configuración y despliegue de PAM360, en lugar del desarrollo de software.

### 4.4. Comparativas y justificaciones

Durante la fase inicial del proyecto, se realizaron comparativas entre distintas soluciones de gestión de accesos privilegiados (PAM). Algunas de las soluciones evaluadas incluyeron:

- **CyberArk [3]:** Conocida por su robustez y funcionalidades avanzadas en la gestión de accesos privilegiados.
- **BeyondTrust [2]:** Reconocida por su enfoque en la seguridad y la gestión de vulnerabilidades.
- **ManageEngine PAM360:** La solución finalmente elegida, destacada por su integración con otros productos de ManageEngine y su relación contractual con NTT Data.

Características	PAM360	BeyondTrust	CyberArk
Funcionalidades Principales	Control de accesos, gestión de contraseñas, auditorías detalladas	Control de accesos, gestión de contraseñas, auditorías detalladas	Control de accesos, gestión de contraseñas, auditorías detalladas
Integración con AD	Si	Si	Si
Compatibilidad de Sistemas	Windows, Linux, macOS	Windows, Linux, macOS	Windows, Linux, macOS
Implementación	On-premises y Cloud	On-premises y Cloud	On-premises y Cloud
Escalabilidad	Alta	Alta	Alta
Facilidad de Uso	Alta	Media	Media
Soporte y Actualizaciones	Regular, con opción a soporte premium	Regular, con opción a soporte premium	Regular, con opción a soporte premium
Seguridad y Cumplimiento	Cumplimiento de normativas estándar	Cumplimiento de normativas estándar	Cumplimiento de normativas estándar
Costo	Relativamente bajo	Medio-alto	Alto
Características Adicionales	Integración con otras soluciones de ManageEngine	Integración con otras soluciones de BeyondTrust	Integración con otras soluciones de CyberArk

Tabla 4.1: Comparación de PAM360 vs BeyondTrust vs CyberArk

El criterio principal para la selección de PAM360 fue el acuerdo existente entre ManageEngine y NTT Data sobre las cesión de licencias, que facilitó la

implementación y soporte de la solución dentro de la empresa. Este acuerdo no solo simplificó el proceso de adquisición, sino que también garantizó una mayor compatibilidad e integración con las herramientas ya utilizadas por NTT Data.



---

## 5. Aspectos relevantes del desarrollo del proyecto

---

### 5.1. Aspectos relevantes del desarrollo del proyecto

### 5.2. Planificación del proyecto

La planificación del proyecto se llevó a cabo utilizando un diagrama de Gantt, que permitió una gestión detallada y estructurada de todas las fases del proyecto. Este diagrama se actualizó regularmente para reflejar el progreso y realizar ajustes según las necesidades. La planificación detallada ayudó a asegurar que todas las tareas fueran completadas a tiempo y dentro del alcance definido.

Project tasks	Type	Status	Percent Done	Planned Start Date	Planned End Date	Planned Duration	Effective Duration	Father
1.3- Identify Server Requirement	Server Deployment	Completed	100%	2024-03-18 09:00	2024-03-18 17:00	8 hours 0 minutes	0 seconds	1- Phase 1 Deployment
1.1- Network   Assign Subnet		Completed	100%	2024-03-18 09:00	2024-03-18 17:00	8 hours 0 minutes	0 seconds	1- Phase 1 Deployment
1- Phase 1 Deployment		In Progress	60%	2024-03-18 09:00	2024-03-20 17:00	0 seconds	0 seconds	
1.4- Server Deployment			0%	2024-03-18 10:00	2024-03-19 17:00	0 seconds	0 seconds	1- Phase 1 Deployment
1.2- Create Vlan		Completed	100%	2024-03-18 12:00	2024-03-18 17:00	8 hours 0 minutes	0 seconds	1- Phase 1 Deployment
1.5- PAM Solution deployment			0%	2024-03-21 00:00	2024-03-24 00:00	0 seconds	0 seconds	1- Phase 1 Deployment

Figura 5.1: Diagrama del proyecto.

A continuación, se muestran varias capturas detalladas del diagrama de Gantt, destacando las diferentes fases del proyecto:

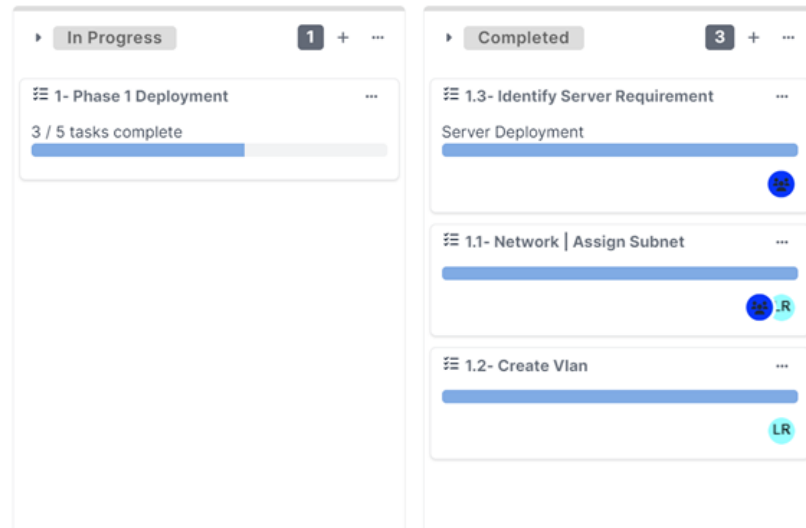


Figura 5.2: Detalle del diagrama de Gantt.

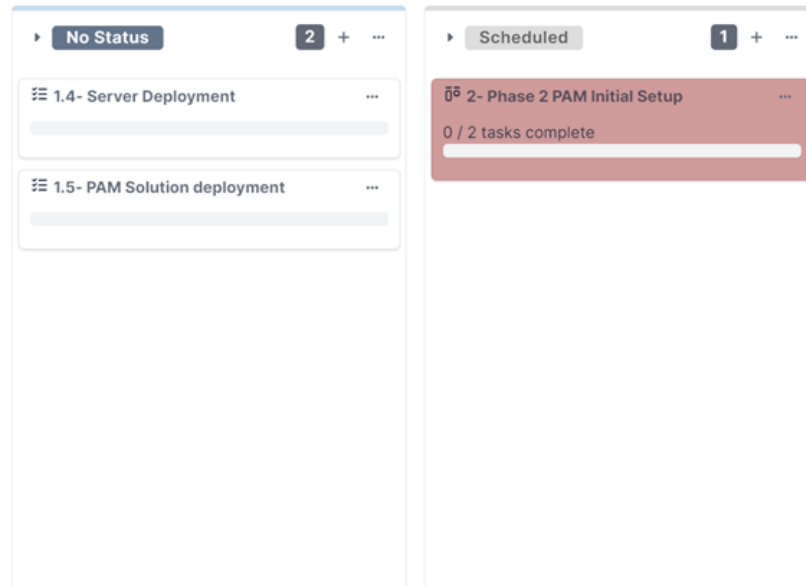


Figura 5.3: Detalle del diagrama de Gantt: fase de desarrollo.

### 5.3. Despliegue de la máquina virtual

El primer paso del proyecto fue la configuración y despliegue de una máquina virtual en vSphere [13]. Esta máquina se ha creado con especificaciones adecuadas para soportar PAM360, incluyendo 16 GB de RAM y un sistema operativo Windows Server 2019.

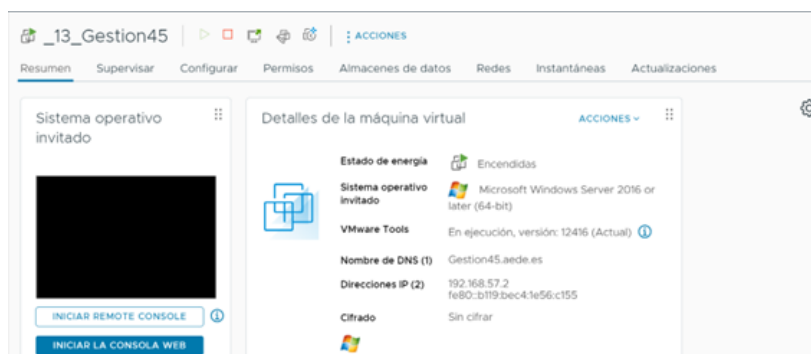


Figura 5.4: Detalles de la máquina virtual en vSphere.



Figura 5.5: Configuración más detallada de la máquina virtual en vSphere.

### 5.4. Instalación de PAM360

La instalación de PAM360 se realizó en la máquina virtual utilizando MRemote para la transferencia de archivos y acceso remoto. El proceso de instalación involucró varios pasos, desde la transferencia del archivo ejecutable hasta la configuración inicial del software.

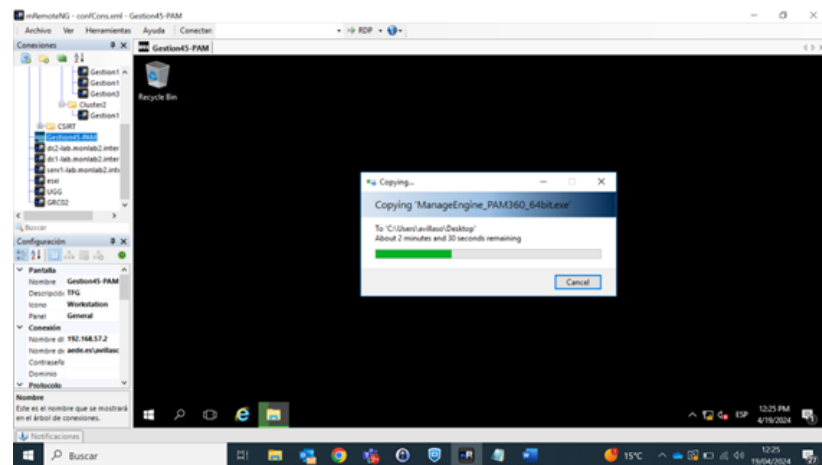


Figura 5.6: Proceso de instalación de PAM360.

## Proceso de instalación

El proceso de instalación de PAM360 fue documentado con varias capturas para asegurar la correcta instalación y configuración inicial del software.

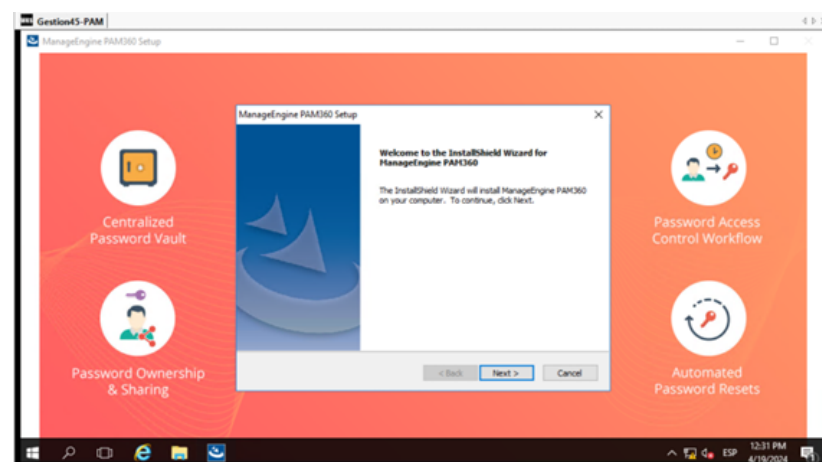


Figura 5.7: Proceso de instalación de PAM360, primera página.



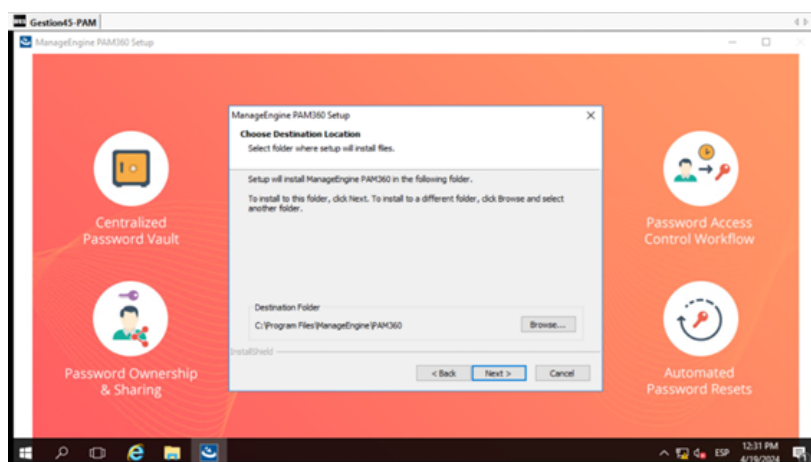


Figura 5.8: Proceso de instalación de PAM360, segunda página.

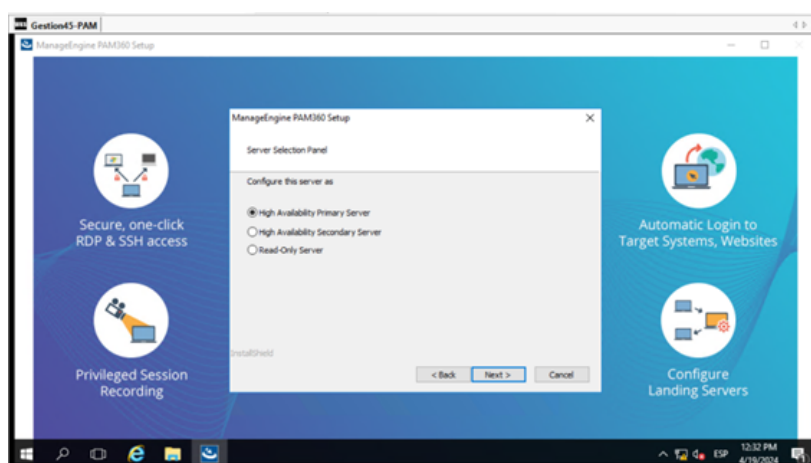


Figura 5.9: Proceso de instalación de PAM360, tercera y última página.

## 5.5. Configuración inicial de PAM360

Una vez instalado PAM360, se procedió a la configuración inicial, que incluyó el cambio de la contraseña del administrador y la configuración de la autenticación y recursos. Esta fase fue crucial para asegurar que PAM360 estuviera configurado de acuerdo con los requisitos de seguridad de NTT Data.

En las siguientes imágenes se puede observar la aplicación funcionando.

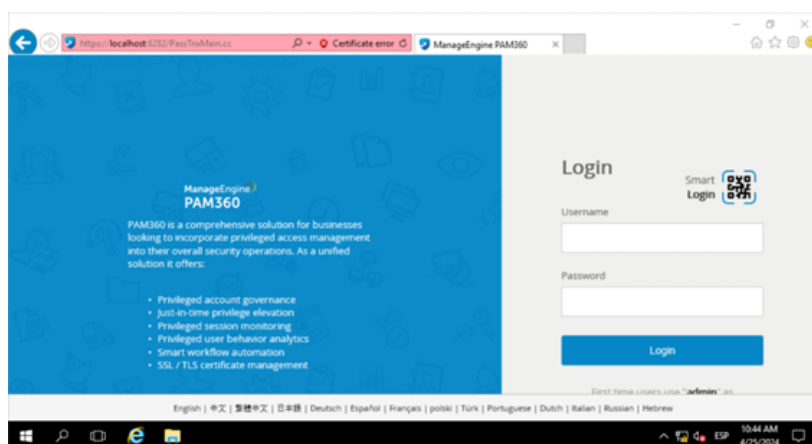


Figura 5.10: Pantalla principal de PAM.

El primer acceso tiene las credenciales por defecto "admin/admin". PAM nos fuerza a que nada más se acceda, se debe cambiar la contraseña por una nueva

Figura 5.11: Configuración del administrador en PAM360.

Una vez cambiada, PAM se conectará automáticamente haciéndonos saber que todo ha sido correcto.

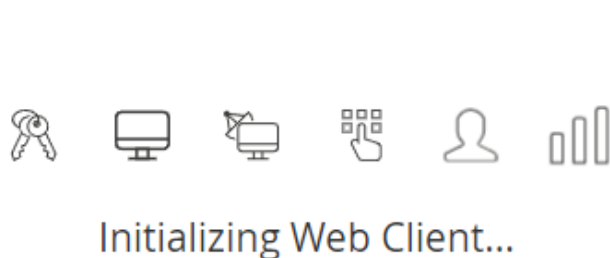


Figura 5.12: Configuración del administrador en PAM360.

Dado que no hay ninguna máquina, contraseña o usuario vinculados a la solución, la página podría presentarse de la siguiente manera:

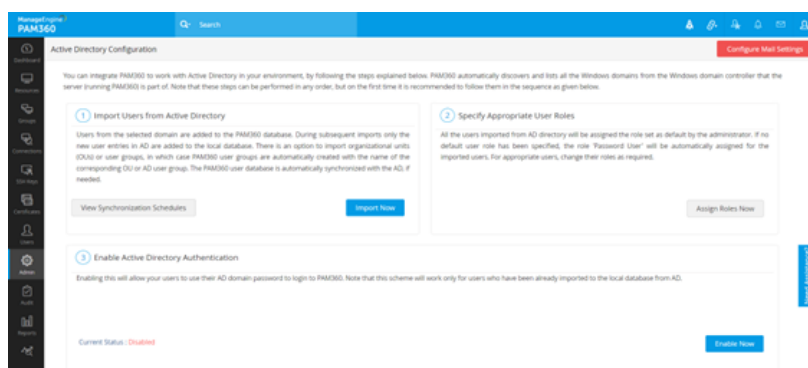


Figura 5.13: Configuración del administrador en PAM360.

## 5.6. Integración con Active Directory

La integración con Active Directory (AD) fue una de las tareas más importantes del proyecto. Este proceso permitió la importación de usuarios y grupos del AD a PAM360, facilitando el control de acceso y la gestión de credenciales. Se configuró el dominio AD "NTTDDATA" y se importaron los usuarios necesarios.

Figura 5.14: Importación de usuarios desde Active Directory.

Debemos crear una política de password para poder añadir el AD, esto es un requisito adicional de PAM como capa extra de seguridad, para cerciorarse que las contraseñas que pongamos cumplan los requisitos estándar de seguridad.

Policy Name	Strength	Policy Description	Set as Default	Edit
<input type="checkbox"/> Low	Weak	Password with less strict constraints	<input type="radio"/>	<a href="#">Edit</a>
<input type="checkbox"/> Medium	Medium	Password with few strict constraints	<input type="radio"/>	<a href="#">Edit</a>
<input type="checkbox"/> Offline Password File	Hard	Policy for offline password access	<input type="radio"/>	<a href="#">Edit</a>
<input checked="" type="checkbox"/> Strong	Strong	Password with strict constraints	<input checked="" type="radio"/>	<a href="#">Edit</a>

Figura 5.15: Configuración del administrador en PAM360.

Cuando se haya integrado correctamente todo, se debería ver así:

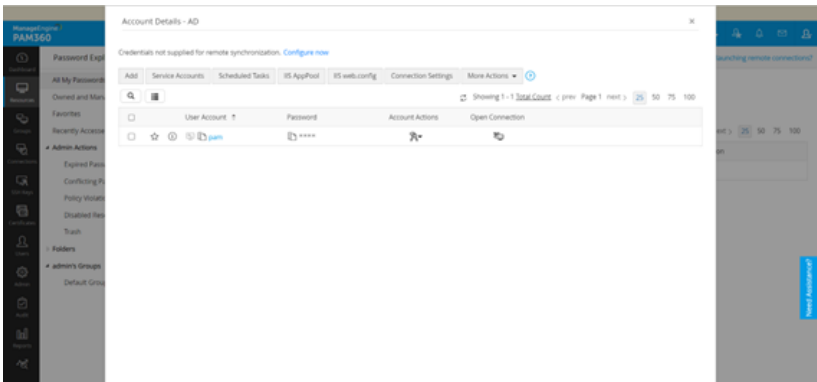


Figura 5.16: AD con la cuenta de pam activo.

Una vez creada la entrada para el AD, el siguiente paso era importar los usuarios del AD a los que se vayan a querer dar acceso a las herramientas y así comprobar que la integración con el AD ha sido exitosa.

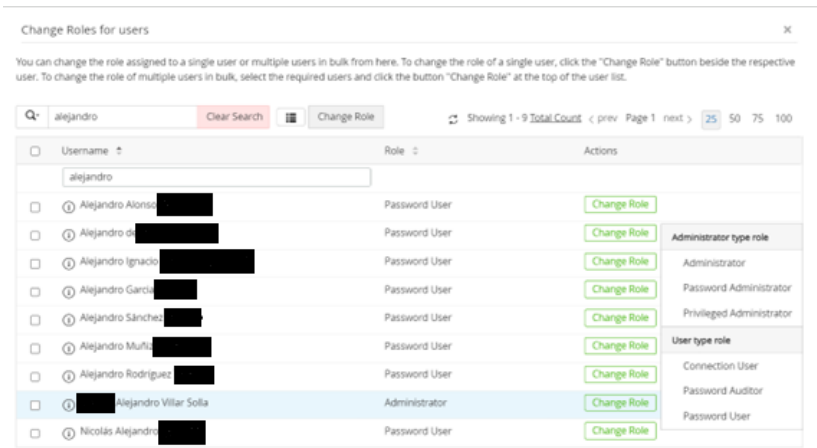
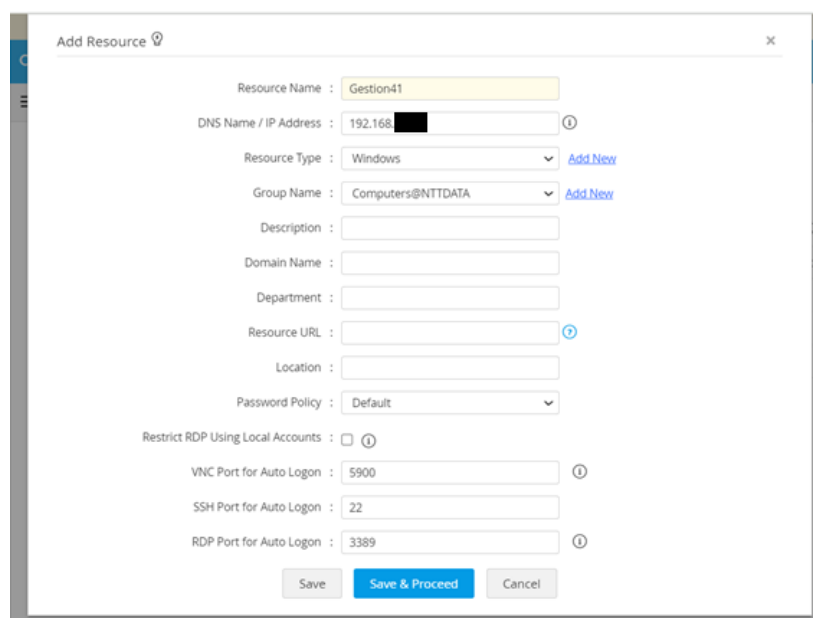


Figura 5.17: AD con la cuenta de pam activo.

Se han censurado los nombres por privacidad de la empresa. Podemos así comprobar que todos los usuarios existentes del AD se han podido traer y vincular correctamente.

## 5.7. Importación de máquinas de nuestro entorno

Cuando tengamos acceso al AD, podremos importar las máquinas que queramos dar acceso a usuarios. En este caso se han importado "Gestión41" y "Gestión42". La se realiza de forma similar, seleccionas el nombre, la IP y el SO que se ejecuta en la máquina y PAM automáticamente configura todo lo necesario para el acceso.



The screenshot shows the 'Add Resource' window in PAM360. The form is filled with the following data:

- Resource Name : Gestion41
- DNS Name / IP Address : 192.168.██
- Resource Type : Windows
- Group Name : Computers@NTTDATA
- Description :
- Domain Name :
- Department :
- Resource URL :
- Location :
- Password Policy : Default
- Restrict RDP Using Local Accounts : ☐
- VNC Port for Auto Logon : 5900
- SSH Port for Auto Logon : 22
- RDP Port for Auto Logon : 3389

At the bottom, there are three buttons: 'Save', 'Save & Proceed' (highlighted in blue), and 'Cancel'.

Figura 5.18: Gestión de contraseñas en PAM360.

## 5.8. Gestión de contraseñas y acceso

PAM360 se utilizó para gestionar contraseñas y controlar el acceso a diferentes recursos. La herramienta permitió la configuración de políticas de contraseñas y la asignación de roles a los usuarios. Esto aseguró que solo los usuarios autorizados pudieran acceder a ciertos recursos.

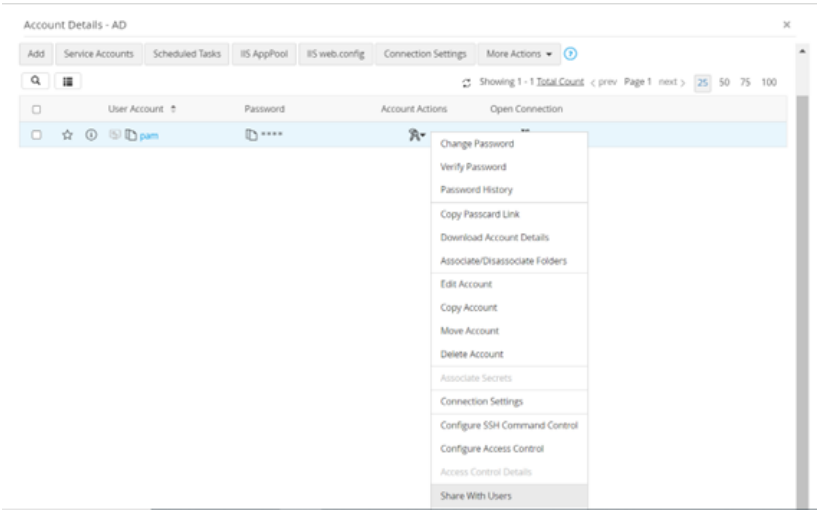


Figura 5.19: Gestión de contraseñas en PAM360.

Para conceder accesos en PAM es sencillo, se elige la cuenta de la máquina, la cual se va a ceder a un usuario. Seleccionamos la opción de "Share with Users". Después, seleccionamos al usuario que le queremos dar acceso (en este caso, mi usuario)

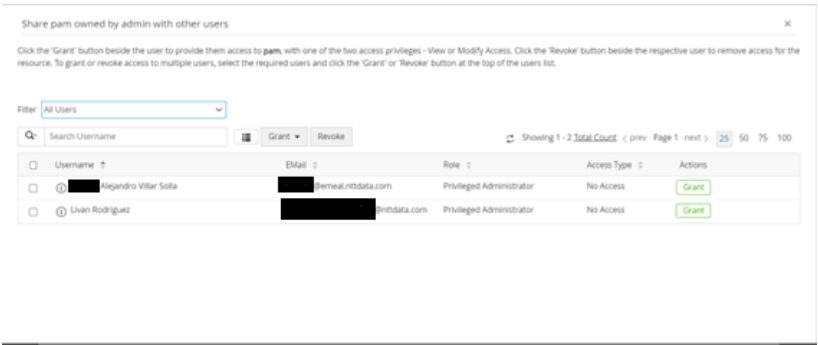


Figura 5.20: Selección de usuario.

y seleccionamos la opción que deseemos, que sólo se pueda conectar a la máquina, que se pueda conectar y ver contraseñas o que pueda hacer todo incluso modificar contraseñas. Esta opciones varían dependiendo del tipo de privilegios que se le hayan concedido al usuario en PAM.

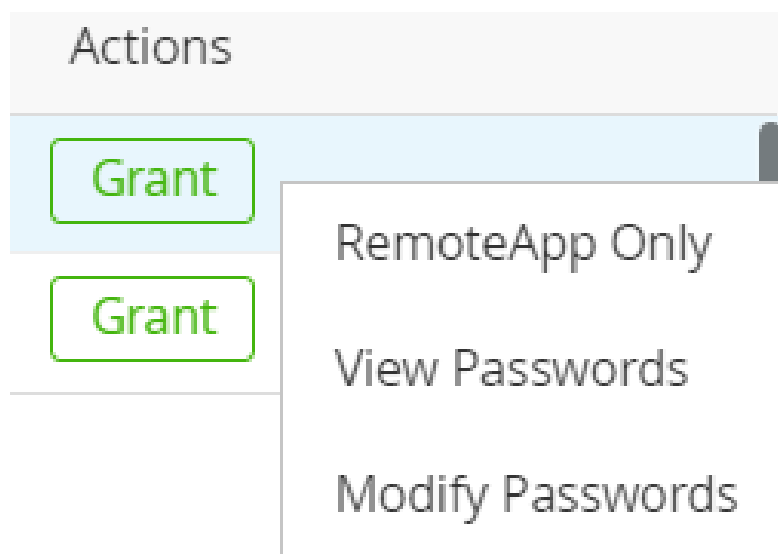


Figura 5.21: Selección de usuario.

Cuando tengamos contraseñas de máquinas guardadas y contraseñas asignadas, la portada de PAM cambiará y nos mostrará la información de nuestros sistemas

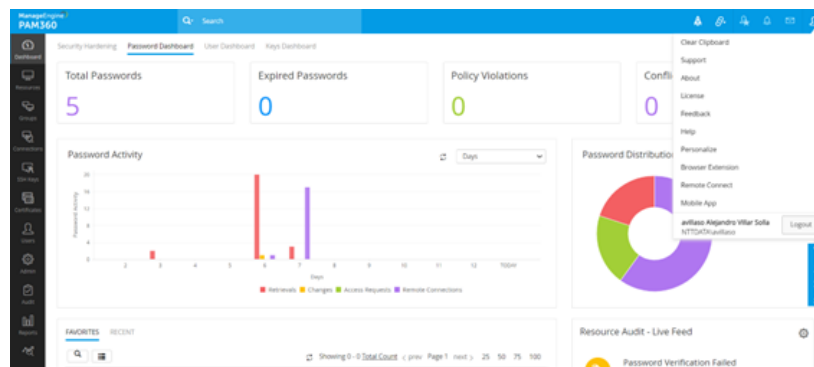


Figura 5.22: Configuración del administrador en PAM360.

## 5.9. Monitorización y auditoría

Una vez configurado, PAM360 proporcionó capacidades de monitorización y auditoría que permitieron registrar todas las actividades de los usuarios.



Esta funcionalidad es esencial para mantener la seguridad y cumplir con las políticas de la empresa.

El usuario accedería a la máquina a la cual tiene permiso. Introduciendo su usuario personal, tendría acceso a la máquina (en este caso Gestion42) como pam-access (cuenta la cual se ha creado para el uso de las máquinas).

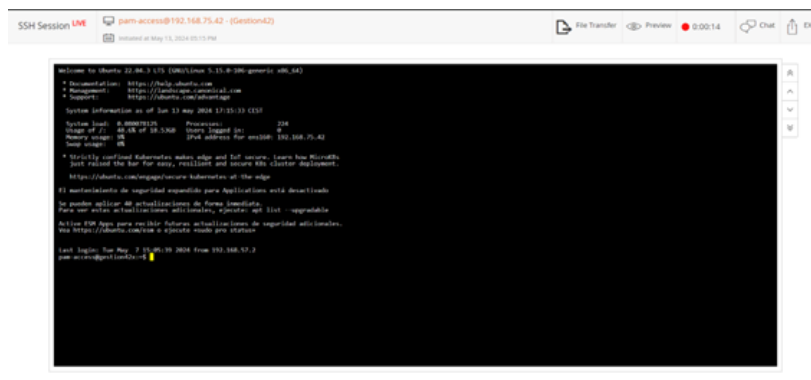


Figura 5.23: Monitorización de actividades en PAM360.

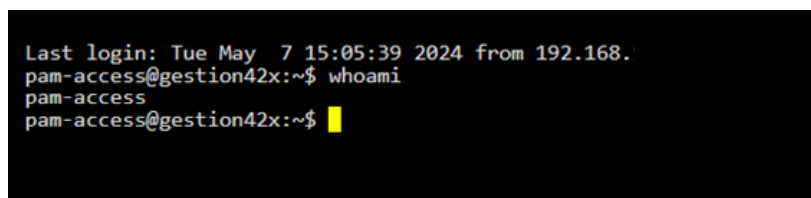


Figura 5.24: PAM360 configurado y operando.

## 5.10. Resultados y validación

Finalmente, se validó el correcto funcionamiento de PAM360 mediante pruebas exhaustivas. Dichas pruebas consistieron en mi tutor de la empresa y yo, cambiándonos los roles uno a otro, haciendo modificaciones en la máquina y el otro reportando dichas modificaciones para ver si se habían grabado correctamente. También se sometió a pruebas de penetración con Nessus y búsqueda de CVEs para PAM360, para comprobar si existía alguna vulnerabilidad. Se verificó que todos los usuarios importados pudieran acceder a los recursos según las políticas establecidas y que todas las actividades fueran registradas adecuadamente. Las acciones del usuario se quedan guardadas.

Al acabar la sesión de uso pam proporciona reportes en modo de: PDF, html y vídeo.

También, el admin puede ver en tiempo real los movimientos que realizan los usuarios en las máquinas dentro de la propia solución.

Primary ServerSecondary ServerRead-Only Server

Operation TypesAudit Actions

Create-- All --

Showing 1 - 50 Total Count < prevPage 1next > 255075100

Resource Name	User Account	Operated By	IP Address	Time Stamp	Operation Type	Username	Reason
Gestion42	pam-access	admin	192.168.1.1	May 13, 2024 05:15 PM	Password Retrieved	N/A	Retrieved by SSH auto login...
AD	pam-access	admin	192.168.1.1	May 13, 2024 05:14 PM	Password Retrieved	N/A	Retrieved by SSH auto login...
AD	pam	admin	192.168.1.1	May 13, 2024 05:14 PM	Password Retrieved	N/A	Retrieved by SSH auto login...
AD	pam	admin	192.168.1.1	May 13, 2024 05:14 PM	Password Retrieved	N/A	Retrieved by SSH auto login...
AD	pam	admin	192.168.1.1	May 13, 2024 05:13 PM	Recorded Session Playb...	N/A	Recorded session has been ...
_75_Gestion41 (Windows)	aida.es/pam-ac...	admin	192.168.1.1	May 13, 2024 05:13 PM	Recorded Session Playb...	N/A	Recorded session has been ...
AD	pam-access	admin	192.168.1.1	May 13, 2024 05:06 PM	Recorded Session Playb...	N/A	Recorded session has been ...
AD	aida.es/pam-ac...	admin	192.168.1.1	May 13, 2024 05:05 PM	Recorded Session Playb...	N/A	Recorded session has been ...
AD	pam-access	admin	192.168.1.1	May 13, 2024 05:03 PM	Recorded Session Playb...	N/A	Recorded session has been ...
AD	pam-access	admin	192.168.1.1	May 13, 2024 04:48 PM	Password Retrieved	N/A	Retrieved by SSH auto login...
Gestion42	pam-access	avilaso Aljan...	192.168.1.1	May 13, 2024 04:43 PM	Password Retrieved	N/A	Retrieved by Telnet auto log...

Figura 5.25: Monitorización de actividades en PAM360 en formato HTML.

Pero la información detallada sale al acabar la sesión

```
Operated by admin
Initiated at May 13, 2024 05:15 PM
Connected from 192.168.██████████

Connecting to the host 192.168.██████████ ....
Authenticated.
Welcome to Ubuntu 22.04.3 LTS (GNU/Linux 5.15.0-106-generic x86_64)

* Documentation:  https://help.ubuntu.com
* Management:    https://landscape.canonical.com
* Support:       https://ubuntu.com/advantage

System information as of lun 13 may 2024 17:15:33 CEST

System load:  0.080078125      Processes:            224
Usage of /:   48.6% of 18.5GB   Users logged in:     0
Memory usage: 9%              IPv4 address for ens160: 192.168.██████████
Swap usage:   0%

* Strictly confined Kubernetes makes edge and IoT secure. Learn how MicroK8s
  just raised the bar for easy, resilient and secure K8s cluster deployment.

  https://ubuntu.com/engage/secure-kubernetes-at-the-edge

El mantenimiento de seguridad expandido para Applications está desactivad

Se pueden aplicar 40 actualizaciones de forma inmediata.
Para ver estas actualizaciones adicionales, ejecute: apt list --upgradable

Active ESM Apps para recibir futuras actualizaciones de seguridad adicionales.
Vea https://ubuntu.com/esm o ejecute sudo pro status

Last login: Tue May  7 15:05:39 2024 from 192.168.██████████
pam-access@gestion42x:~$ whoami

pam-access
pam-access@gestion42x:~$ echo "esto es un testeo"

esto es un testeo
pam-access@gestion42x:~$
```

Figura 5.26: Resultados de la validación del sistema.



---

## 6. Conclusiones y Líneas de trabajo futuras

---

### 6.1. Conclusiones

Desarrollar el proyecto de implementación de PAM360 para NTT Data me ha proporcionado una visión clara de lo que esta herramienta puede hacer para mejorar la gestión de accesos privilegiados. Durante el proyecto, he conseguido cumplir con los principales objetivos, entre los cuales se destacan la mejora de la seguridad y la optimización de la gestión de accesos. A continuación, voy a detallar los objetivos alcanzados y las razones por las que considero que se han cumplido:

- **Mejora de la seguridad:** Se ha implementado un control riguroso sobre el acceso a las máquinas, tanto para usuarios internos como para clientes. Esto ha reducido significativamente los riesgos de accesos no autorizados y ha añadido una capa extra de seguridad en la gestión de credenciales. Las capturas de pantalla que muestran el cambio de contraseña del administrador y la configuración de políticas de autenticación y recursos demuestran que se implementaron medidas de seguridad desde el inicio.
- **Optimización de la gestión de accesos:** PAM360 ha simplificado la administración de usuarios y contraseñas. Ya no es necesario crear cuentas específicas para cada máquina, lo que permite una gestión centralizada y mucho más eficiente, facilitando el trabajo de los administradores del sistema y mejorando la eficiencia operativa. Las imágenes capturadas del proceso de importación de usuarios desde

Active Directory y la asignación de roles muestran cómo se centralizó la gestión de accesos.

- **Transparencia y trazabilidad:** Una de las grandes ventajas de PAM360 es su capacidad para registrar y auditar todas las actividades de los usuarios, asegurando así la transparencia y trazabilidad en el acceso a los recursos, lo cual es fundamental para cumplir con las normativas de seguridad y para las auditorías internas. Las imágenes de los reportes de auditoría y el dashboard de monitorización confirman la capacidad de PAM360 para registrar y auditar actividades.
- **Implementación técnica efectiva:** La instalación y configuración de PAM360 en un entorno virtualizado, utilizando herramientas como vSphere y MRemote, ha demostrado ser efectiva y robusta. Elegimos estas herramientas en la empresa porque facilitan el acceso y la administración remota del servidor PAM360. Las imágenes capturadas de la configuración de la máquina virtual en vSphere y del proceso de instalación de PAM360 evidencian una implementación técnica adecuada.
- **Integración con Active Directory:** La integración de PAM360 con el Active Directory de NTT Data ha permitido una sincronización fluida y efectiva de usuarios y roles, asegurando que los accesos se gestionen de manera centralizada y conforme a las políticas de la empresa. Las capturas que muestran la configuración del conector de Active Directory y la importación de usuarios evidencian una integración exitosa con AD.
- **Gestión segura de contraseñas:** La gestión de contraseñas con PAM360 ha sido intuitiva y segura, y la capacidad de generar reportes y auditorías ha sido especialmente útil para monitorizar y controlar los accesos en tiempo real. Las Instantáneas de pantalla de la configuración de políticas de contraseñas y los reportes de actividades demuestran la eficacia en la gestión segura de contraseñas y monitorización de accesos.

## 6.2. Líneas de Trabajo Futuras

Sería recomendable ampliar el uso de PAM360 a todos los departamentos dentro de NTT Data, incluyendo la integración de todos los sistemas críticos bajo la gestión de PAM360, incrementando así su alcance y los beneficios

que ofrece. Además, es importante explorar la automatización de tareas repetitivas y críticas utilizando las capacidades de scripting y API de PAM360. Esto no solo mejoraría la eficiencia operativa, sino que también reduciría el riesgo de errores humanos en la gestión de accesos.

Mantener una evaluación continua de las políticas de seguridad y las configuraciones de PAM360 es crucial para adaptarse a nuevas amenazas y vulnerabilidades. Actualizar estas políticas constantemente garantizará que la empresa se mantenga protegida contra posibles ataques. Finalmente, implementar programas de formación y capacitación para el personal técnico y administrativo de NTT Data sobre el uso y administración de PAM360 es fundamental. Una mejor comprensión y manejo de la herramienta contribuirán a maximizar su eficacia y a asegurar que todos los usuarios sigan las mejores prácticas de seguridad.

En resumen, el proyecto ha cumplido con sus objetivos iniciales y ha demostrado ser una solución efectiva para la gestión de accesos privilegiados en NTT Data. Las líneas de trabajo futuras propuestas permitirán no solo mantener, sino también mejorar y expandir las capacidades de seguridad y gestión de accesos en la empresa.





---

## Bibliografía

---

- [1] Michael Barrett. *Privileged Access Management: A Comprehensive Guide*. Cybersecurity Press, 2020.
- [2] BeyondTrust. Beyondtrust: Privileged access management. <https://www.beyondtrust.com/>, 2024. [Internet; descargado 30-mayo-2024].
- [3] CyberArk. Cyberark: Identity security solutions. <https://www.cyberark.com/>, 2024. [Internet; descargado 30-mayo-2024].
- [4] Fortinet. Fortinet: Security-driven networking for a hyperconnected world. <https://www.fortinet.com/>, 2024. [Internet; descargado 30-mayo-2024].
- [5] Henry L. Gantt. *Work, Wages, and Profits*. The Engineering Magazine Co., 1916.
- [6] Andrew Johnson. *Integrating PAM with SIEM and IAM Systems*. Security Insights Publishing, 2018.
- [7] John Kindervag. No more chewy centers: Introducing the zero trust model of information security. <https://www.forrester.com/report/No-More-Chewy-Centers-Introducing-The-Zero-Trust-Model-Of-Information-Security/RES57182>, 2010. [Internet; descargado 30-mayo-2024].
- [8] ManageEngine. Pam360: Comprehensive privileged access management solution. <https://www.manageengine.com/pam360/>, 2023. [Internet; descargado 30-mayo-2024].

- [9] Microsoft. Introducción a active directory domain services | microsoft learn. <https://learn.microsoft.com/es-es/windows-server/identity/ad-ds/get-started/virtual-dc/active-directory-domain-services-overview>, 2024. [Internet; descargado 30-mayo-2024].
- [10] Richard Moore. *Continuous Monitoring and Auditing in Cybersecurity*. InfoSec Books, 2021.
- [11] MRemoteNG. Mremoteng: The next generation of mremote, open source, tabbed, multi-protocol, remote connections manager. <https://mremoteng.org/>, 2024. [Internet; descargado 30-mayo-2024].
- [12] John Smith. *The Role of Proof of Concept in IT Projects*. Tech Publishing, 2019.
- [13] VMware. vsphere: Server virtualization platform. <https://www.vmware.com/products/vsphere.html>, 2024. [Internet; descargado 30-mayo-2024].
- [14] Michael E. Whitman and Herbert J. Mattord. *Principles of Information Security*. Cengage Learning, 2022.