



Universidad Nacional Mayor de San Marcos

Universidad del Perú. Decana de América

Facultad de Ingeniería de Sistemas e Informática

Escuela Profesional de Ingeniería de Software

**Implementación de un privileged access management
para el acceso a servidores en una entidad bancaria**

TESIS

Para optar el Título Profesional de Ingeniero de Software

AUTOR

Kenny Bill GAMARRA ESCALERA

ASESOR

Nilo Eloy CARRASCO ORE

Lima, Perú

2024



Reconocimiento - No Comercial - Compartir Igual - Sin restricciones adicionales

<https://creativecommons.org/licenses/by-nc-sa/4.0/>

Usted puede distribuir, remezclar, retocar, y crear a partir del documento original de modo no comercial, siempre y cuando se dé crédito al autor del documento y se licencien las nuevas creaciones bajo las mismas condiciones. No se permite aplicar términos legales o medidas tecnológicas que restrinjan legalmente a otros a hacer cualquier cosa que permita esta licencia.

Referencia bibliográfica

Gamarra, K. (2024). *Implementación de un privileged access management para el acceso a servidores en una entidad bancaria*. [Trabajo de suficiencia profesional de pregrado, Universidad Nacional Mayor de San Marcos, Facultad de Ingeniería de Sistemas e Informática, Escuela Profesional de Ingeniería de Software]. Repositorio institucional Cybertesis UNMSM.

Metadatos complementarios

Datos de autor	
Nombres y apellidos	Kenny Bill Gamarra Escalera
Tipo de documento de identidad	DNI
Número de documento de identidad	73136535
URL de ORCID	https://orcid.org/0009-0004-1256-9306
Datos de asesor	
Nombres y apellidos	Nilo Eloy Carrasco Ore
Tipo de documento de identidad	DNI
Número de documento de identidad	09342780
URL de ORCID	https://orcid.org/0000-0001-5664-9309
Datos del jurado	
Presidente del jurado	
Nombres y apellidos	William Martin Enríquez Maguiña
Tipo de documento	DNI
Número de documento de identidad	06179457
Miembro del jurado 1	
Nombres y apellidos	Joel Fernando Machado Vicente
Tipo de documento	DNI
Número de documento de identidad	40476778
Datos de investigación	
Línea de investigación	No aplica
Grupo de investigación	No aplica
Agencia de financiamiento	Sin financiamiento
Ubicación geográfica de la investigación	País: Perú Departamento: Lima Provincia: Lima

	Distrito: Cercado de Lima Jr. Carlos Amezaga No. 375 Universidad Nacional Mayor de San Marcos Latitud: -12.0564232 Longitud: -77.0843327
Año o rango de años en que se realizó la investigación	2023
URL de disciplinas OCDE	2.02.04 -- Ingeniería de sistemas y comunicaciones https://purl.org/pe-repo/ocde/ford#2.02.04



UNIVERSIDAD NACIONAL MAYOR DE SAN MARCOS
FACULTAD DE INGENIERÍA DE SISTEMAS E INFORMÁTICA
Escuela Profesional de Ingeniería de Software

Acta Virtual de Sustentación
del Trabajo de Suficiencia Profesional

Siendo las 19:47 horas del día 30. de enero del año 2024, se reunieron virtualmente los docentes designados como Miembros de Jurado del Trabajo de Suficiencia Profesional, presidido por el Mg. Enríquez Maguiña William Martin (Presidente), Mg. Machado Vicente Joel Fernando (Miembro) y el Ing. Carrasco Ore Nilo Eloy (Miembro Asesor), usando la plataforma Meet (<https://meet.google.com/ets-flxi-urx?hs=224>), para la sustentación virtual del Trabajo de Suficiencia Profesional intitulado: **“IMPLEMENTACIÓN DE UN PRIVILEGED ACCESS MANAGEMENT PARA EL ACCESO A SERVIDORES EN UNA ENTIDAD BANCARIA”**, por el Bachiller **Gamarra Escalera Kenny Bill**; para obtener el Título Profesional de Ingeniero de Software.

Acto seguido de la exposición del Trabajo de Suficiencia Profesional, el Presidente invitó al Bachiller a dar las respuestas a las preguntas establecidas por los miembros del Jurado.

El Bachiller en el curso de sus intervenciones demostró pleno dominio del tema, al responder con acierto y fluidez a las observaciones y preguntas formuladas por los señores miembros del Jurado.

Finalmente habiéndose efectuado la calificación correspondiente por los miembros del Jurado, el Bachiller obtuvo la nota de **17 (DIECISIETE)**.

A continuación el Presidente de Jurados el Mg. Enríquez Maguiña William Martin, declara al Bachiller **Ingeniero de Software**.

Siendo las 20:42 horas, se levantó la sesión.

Presidente

Mg. Enríquez Maguiña William Martin

Miembro

Mg. Machado Vicente Joel Fernando

Miembro Asesor

Ing. Carrasco Ore Nilo Eloy



Universidad Nacional Mayor de San Marcos

Universidad del Perú. Decana de América

Vicerrectorado de Investigación y Posgrado



CERTIFICADO DE SIMILITUD

Yo NILO ELOY CARRASCO ORE en mi condición de asesor acreditado con la Resolución Decanal N° 001246-2023-D-FISI y Oficio N° 008-PTTSP-FISI-2023 del Trabajo de Suficiencia Profesional cuyo título es IMPLEMENTACIÓN DE UN PRIVILEGED ACCESS MANAGEMENT PARA EL ACCESO A SERVIDORES EN UNA ENTIDAD BANCARIA, presentado por el bachiller GAMARRA ESCALERA KENNY BILL para optar el título de Ingeniero de Software CERTIFICO que se ha cumplido con lo establecido en la Directiva de Originalidad y de Similitud de Trabajos Académicos, de Investigación y Producción Intelectual. Según la revisión, análisis y evaluación mediante el software de similitud textual, el documento evaluado cuenta con el porcentaje de 8% de similitud, nivel **PERMITIDO** para continuar con los trámites correspondientes y para su **publicación en el repositorio institucional**.

Se emite el presente certificado en cumplimiento de lo establecido en las normas vigentes, como uno de los requisitos para la obtención del título correspondiente.

Firma del Asesor _____

DNI: 09342780

Nombres y apellidos del asesor: NILO ELOY CARRASCO ORE



FICHA CATALOGRÁFICA

IMPLEMENTACIÓN DE UN PRIVILEGED ACCESS MANAGEMENT PARA EL ACCESO A SERVIDORES EN UNA ENTIDAD BANCARIA

AUTOR: GAMARRA ESCALERA, KENNY BILL

ASESOR: DR. NILO CARRASCO ORÉ

LIMA – PERÚ, 2023

TÍTULO PROFESIONAL: Título Profesional de Ingeniero de Software

ÁREA / PROGRAMA / LÍNEA DE INVESTIGACIÓN:

Ingenierías / Tecnología de Información y Comunicación / Ingeniería de Software

PREGRADO: Universidad Nacional Mayor de San Marcos – Facultad de Ingeniería de Sistemas e Informática – Escuela Profesional de Ingeniería de Software

Formato 29.7 x 21 cm

Páginas x, 69

DEDICATORIA

A mis padres y a mi hermana, por todo su esfuerzo y sacrificio al siempre impulsarme a ser mejor persona y apoyarme a culminar con éxito mi carrera profesional. A mi compañera de vida Gianella por estar conmigo en todo momento y a mi hija Antonella por ser mi motivo de vida.

AGRADECIMIENTOS

Me gustaría expresar mi más sincero agradecimiento al Dr. Frank Edmundo Escobedo Bailón por sus valiosas y constructivas sugerencias durante la planificación y desarrollo de este trabajo de suficiencia profesional. Su disposición a dar su tiempo tan generosamente ha sido muy valioso y apreciado.

Agradezco al Pablo Jesús Romero Naupari por brindarme la gran oportunidad de poder desarrollar este trabajo de suficiencia profesional que me permitirá obtener el título profesional de Ingeniero de Software.

Agradezco adicionalmente a la ingeniera Joselin Moreyra por haberme apoyado durante todo mi período laboral y así también poder apoyarme con la información necesaria para poder realizar el presente trabajo.

UNIVERSIDAD NACIONAL MAYOR DE SAN MARCOS
FACULTAD DE INGENIERÍA DE SISTEMAS E INFORMÁTICA
ESCUELA PROFESIONAL DE INGENIERÍA DE SOFTWARE

**Implementación de un Privileged Access Management para el acceso a servidores
en una entidad bancaria**

Autor: Gamarra Escalera, Kenny Bill

Asesor: Carrasco Oré, Nilo

**Título: Trabajo de Suficiencia Profesional para optar el Título Profesional de
Ingeniero de Software**

Fecha: Octubre de 2023

RESUMEN

El problema detectado es que existía un proceso manual y poco controlado para la gestión y uso de accesos privilegiados en los servidores de entorno productivo implementados dentro de la infraestructura de la entidad bancaria. Por lo cual se tenía como objetivo mejorar este proceso y adicionar controles que brinden una capa adicional de seguridad. El presente trabajo trata de la implementación de una tecnología integral de seguridad como es el caso del sistema Privileged Access Management (PAM) para lo cual se tuvo que realizar una reingeniería de los procesos actuales que abarcaba la gestión de accesos en general. Así también, se tuvo que trabajar en la obtención de información de los diferentes tipos de sistemas operativos que tenían instalados los servidores para poder adaptarlos hacia el uso de esta nueva tecnología. La implementación trajo consigo el poder manejar ahora estas cuentas privilegiadas de una manera centralizada y automatizada, así como poder supervisar, limitar y controlar el acceso y uso de estas cuentas de una mejor manera. Esto conllevó en mejora en los tiempos de atención para todos los requerimientos de gestión de accesos y también en el cumplimiento sobre el gobierno de estas cuentas.

Palabras clave: PAM, cuentas privilegiadas, autenticación, autorización, servidor.

MAJOR NATIONAL UNIVERSITY OF SAN MARCOS
FACULTY OF SYSTEMS AND INFORMATICS ENGINEERING
PROFESSIONAL SCHOOL OF SOFTWARE ENGINEERING

**Implementation of a Privileged Access Management for access to servers in a
banking institution.**

Author: Gamarra Escalera, Kenny Bill

Advisor: Carrasco Oré, Nilo

**Title: Professional Sufficiency Work to opt for the Professional Title of Software
Engineer**

Date: October 2023

ABSTRACT

The problem detected was that there was a manual and poorly controlled process for the management and use of privileged access in the productive environment servers implemented within the bank's infrastructure. Therefore, the objective was to improve this process and add controls that provide an additional layer of security. The present work deals with the implementation of an integral security technology such as the Privileged Access Management (PAM) system, for which a reengineering of the current processes covering access management in general had to be carried out. It was also necessary to work on obtaining information on the different types of operating systems installed on the servers to adapt them to the use of this new technology. The implementation brought with it the ability to manage these privileged accounts in a centralized and automated way, as well as to supervise, limit and control the access and use of these accounts in a better way. This led to improved turnaround times for all access management requirements as well as improved compliance on the governance of these accounts.

Keywords: PAM, privileged accounts, authentication, authorization, server.

TABLA DE CONTENIDO

INTRODUCCION.....	1
CAPÍTULO I – TRAYECTORIA PROFESIONAL.....	3
CAPÍTULO II – CONTEXTO EN EL QUE SE DESARROLLA LA IDEA	8
2.1. La empresa	8
2.2. Propósito	8
2.3. Aspiración	8
2.4. Organización de la empresa.....	9
2.5. Área, cargo y funciones desempeñadas	9
2.6. Experiencia profesional realizada en la organización.....	10
CAPÍTULO III – ACTIVIDADES DESARROLLADAS	12
3.1. Situación Problemática	12
3.2. Definición del problema	14
3.3. Solución	14
3.2.1. Objetivos	15
3.2.2. Alcance.....	16
3.2.3. Etapas y metodología.....	16
3.2.4. Fundamentos utilizados	20
3.2.5. Implementación de las áreas, procesos, sistemas y buenas prácticas.....	26
3.4. Evaluación.....	52
3.3.1. Evaluación económica / Evaluación costo-beneficio	52
CAPÍTULO IV – REFLEXIÓN CRÍTICA DE LA EXPERIENCIA.....	57
CAPÍTULO V – CONCLUSIONES Y REFLEXIONES	59
4.1. Conclusiones.....	59
4.2. Recomendaciones	61
FUENTES DE INFORMACIÓN	63
ANEXOS	65

ÍNDICE DE FIGURAS

Figura 1 – Organigrama empresa	9
Figura 2 – Etapas del proyecto.	18
Figura 3 – Arquitectura propuesta para la solución PAM.	28
Figura 4 – Grupo de red usado para acceder a PAM.	30
Figura 5 – Usuario enlace Active Directory y sistema PAM.	30
Figura 6 – Configuración de usuario para enlace entre AD y PAM.	31
Figura 7 – Extracto de Línea Base de Seguridad de servidor RHEL con detalle de la creación de los usuarios de PAM.	33
Figura 8 – Ingreso a módulo SCAN en el sistema PAM.	34
Figura 9 – Ingreso de datos del servidor en módulo SCAN	34
Figura 10 – Ingreso de credenciales para escaneo de servidor dependiendo del SO del servidor.	35
Figura 11 – Selección de servidor para procesar escaneo.	35
Figura 12 – Definición de nombre y hora de inicio de escaneo.	36
Figura 13 – Validación de estado de escaneo de servidor.	36
Figura 14 – Usuarios de dominio enlazados a un servidor Windows.	36
Figura 15 – Búsqueda de servidor en opción “Assets”, visibilidad de cuentas locales escaneadas por PAM.	37
Figura 16 – Búsqueda de servidor en opción Managed Systems.	37
Figura 17 – Configuración de usuario local y su credencial en servidor AIX/RHEL.	38
Figura 18 – Configuración de rotación de credenciales a usuario manager.	38
Figura 19 – Validación de usuarios locales de servidores AIX/RHEL configurados en PAM.	38
Figura 20 – Creación y configuración de Address Group	40
Figura 21 – Asociación de smart rule tipo asset con Address Group.	40
Figura 22 – Acciones configuradas en un smart rule tipo asset.	41
Figura 23 – Password Policies configurados en PAM.	41
Figura 24 – Asociación de usuario manager con smart rule tipo account.	42
Figura 25 – Acciones a realizar del smart rule tipo account.	42
Figura 26 – Asociación del grupo de red a smart rule tipo account.	42
Figura 27 – Asociación de política de acceso (Access policies) a smart rule tipo account.	43
Figura 28 – Access Policies en PAM.	44
Figura 29 – Configuración Connection profile.	45
Figura 30 – Login sistema PAM	46
Figura 31 – Ingreso a sistema PAM y pestañas	47

Figura 32 – Búsqueda de un servidor Linux o AIX opción Systems.	48
Figura 33 – Open SSH Session.	48
Figura 34 – Start SSH Session.	49
Figura 35 – Sesión iniciada en el servidor seleccionado.	49
Figura 36 – Búsqueda de un servidor Linux o AIX opción Applications.	50
Figura 37 – Application Session.....	50
Figura 38 – Archivo rdp descargado.	50
Figura 39 – Acceso a servidor terminal con aplicación WINSCP abierta con sesión iniciada de usuario manager	51
Figura 40 – Búsqueda de servidores Windows Server en la pestaña Domain Linked Accounts.	51
Figura 41 – Archivo rdp descargado.	51
Figura 42 – Sesión iniciada de usuario manager en servidor Windows Server	51
Figura 43 – Detalle riesgo asociado (FAIR).....	53
Figura 44 – Pérdidas Primarias asociadas al riesgo.	54
Figura 45 - Pérdidas Secundarias asociadas al riesgo.	54
Figura 46 – Resumen de tiempos de atención para acceso a todo el parque de servidores a una persona teniendo en cuenta la implementación de PAM.	60
Figura 47 – Reporte incidentes de acceso a servidores cuando no se tenía implementado PAM.	60
Figura 48 – Reporte incidentes de acceso a servidores con PAM implementado.	60

ÍNDICE DE TABLAS

Tabla 1 – Experiencia profesional y certificaciones.....	3
Tabla 2 – Número de servidores usados por proveedores en la organización.	27
Tabla 3 – Número de servidores usados por áreas dentro de la organización.	28
Tabla 4 – Detalle de tipo de cuentas creados por Sistema Operativo de servidor.....	32
Tabla 5 – Costo proyecto implementación PAM.....	55
Tabla 7 – Cuadro resumen de costos.....	55

INTRODUCCION

Hoy en día los términos autenticación y autorización vienen siendo recurrentes en el área de TI. Organizaciones como OWASP incluyen dentro de sus 10 principales vulnerabilidades lo siguiente: “Identification and Authentication Failures”, haciendo referencia a las fallas en la autenticación y autorización de identidades que pueden presentar las aplicaciones en general. En este contexto surgen términos como “Cuentas con accesos con privilegios o Cuentas privilegiadas”, en este punto la compañía (Cyberark, 2023) nos dice lo siguiente “En un entorno empresarial, el acceso privilegiado es un término que utilizado para designar el acceso o las capacidades especiales por encima de las de un usuario regular. El acceso privilegiado permite a las organizaciones proteger su infraestructura y aplicaciones, gestionar su entorno de manera eficiente y mantener la confidencialidad de los datos sensibles y la infraestructura crítica.”. Otra organización involucrada en el manejo de este tipo de identidades como lo es BeyondTrust (2023) nos dice lo siguiente: “Se considera una cuenta con privilegios a cualquier cuenta que proporcione acceso y privilegios superiores a los de las cuentas no privilegiadas. Un usuario con privilegios es cualquier usuario que actualmente aprovecha el acceso privilegiado. Debido a sus elevadas capacidades y accesos, los usuarios y/o cuentas privilegiadas plantean riesgos considerablemente mayores que las cuentas y/o usuarios no privilegiados.”

En el Perú y el mundo las empresas como las entidades bancarias manejan bastantes activos de información relacionados al área de TI. Uno de ellos y tal vez principales serían los ordenadores o servidores en donde se almacenan y procesan todo tipo de información relevante para la organización que los usa. A raíz de ello surge la necesidad de que diferentes actores cuenten con el acceso privilegiado hacia estos equipos para poder cumplir diferentes roles dentro de la organización (soporte, administración, etc.), pero ¿cómo controlamos las acciones realizadas por estas identidades o de qué manera podemos hacer prevalecer el principio de mínimo privilegio sobre estos activos? Para responder este tipo de necesidades es que hoy en día existen nuevas tecnologías integrales de seguridad, como es el caso de los sistemas Privileged Access Management (o por sus siglas “PAM”) para el manejo de estas cuentas privilegiadas y que nos brindan,

entre otros beneficios, el poder mejorar el manejo de la gestión de accesos privilegiados trabajando de una manera centralizada, automatizada y controlada.

El presente trabajo ha sido estructurado en los siguientes capítulos para una mejor comprensión:

- En el CAPÍTULO I - TRAYECTORIA PROFESIONAL, se detalla la experiencia laboral lograda y formación académica del autor, las cuales sirven de base para conocer su perfil académico y profesional para poder llevar a cabo el proyecto descrito en el presente trabajo.
- En el CAPÍTULO II - CONTEXTO EN EL QUE SE DESARROLLA LA EXPERIENCIA, se describe el contexto en el que se implementó el proyecto presentado, describiendo a la empresa beneficiada por la solución. Así mismo, se da a conocer su misión, su visión y su organización. Además, se listan las funciones que desempeñó el autor y la experiencia adquirida dentro de la organización.
- En el CAPÍTULO III - ACTIVIDADES DESARROLLADAS, se detalla las actividades realizadas al llevar a cabo la implementación del proyecto presentado. Se aborda con mayor amplitud la situación problemática, la solución presentada, los objetivos, la metodología implementada y los resultados finales.
- En el CAPÍTULO IV - REFLEXIÓN CRÍTICA DE LA EXPERIENCIA, se expone la experiencia y las enseñanzas alcanzadas, así como las deficiencias y/o limitaciones que se presentaron al momento de llevar a cabo la implementación de la solución.
- En el CAPÍTULO V - CONCLUSIONES Y RECOMENDACIONES, se detallan las conclusiones y recomendaciones del proyecto implementado descrito en el presente trabajo en base a la experiencia y resultados obtenidos.

CAPÍTULO I – TRAYECTORIA PROFESIONAL

El autor del presente trabajo, al momento de su elaboración, es bachiller de la carrera de Ingeniería de Software de la Universidad Nacional Mayor de San Marcos. Durante la elaboración del presente trabajo me encuentro laborando en la entidad bancaria Banco de Crédito del Perú desempeñando el puesto de Infrastructure Security Specialist Senior. Asignado al Squad de Identity and Access Management Platform como ingeniero responsable de las siguientes tecnologías de seguridad de información: Identity Access Management (IAM) y Privileged Access Management (PAM). Dentro de mis principales funciones se encuentra el poder realizar evaluaciones de vulnerabilidades, brindar soporte, propuestas de mejoras y respuestas ante incidentes de las tecnologías de seguridad de la información (TSI) de las cuales me encuentro como responsable. Así como asegurar el cumplimiento de las TSI de acuerdo con los lineamientos internos de la organización y dar respuestas a las auditorías internas y externas.

Tabla 1 – Experiencia profesional y certificaciones

PUESTO	EMPRESA	PRINCIPALES FUNCIONES	FECHAS
INFRASTRUCTUR E SECURITY SPECIALIST SENIOR	BANCO DE CRÉDITO DEL PERÚ	- Definir las configuraciones de seguridad recomendadas para las plataformas en uso y coordinar el proceso de actualización permanente de las mismas.	01/01/2023 - Al presente
		- Apoyar a la División de Auditoría y Área de Seguridad y Prevención de Fraudes en la ejecución de trabajos especiales a su solicitud.	
		- Asignado al SQ de Identidades, responsable de herramientas IAM (Identity access management) y PAM (privileged access management)	

SOFTWARE SECURITY SPECIALIST SENIOR	BANCO DE CRÉDITO DEL PERÚ	- Remediación de vulnerabilidades asociadas a los Ethical Hacking realizado a la aplicación a cargo.	01/12/2021 - 01/01/2023
		- Evaluar la efectividad y eficiencia de las medidas de seguridad y control establecidos, buscando en lo posible implementar sistemas de alerta automáticos y de revisión centralizada.	
		- Investigar y analizar nuevas debilidades descubiertas en plataformas y software de base utilizado en la red CREDICORP, evaluar la posibilidad de materialización de los riesgos y determinar las medidas preventivas y de control necesarias para evitarlo, coordinando la implementación de estas.	
		- Definir las configuraciones de seguridad recomendadas para las plataformas en uso y coordinar el proceso de actualización permanente de las mismas.	
SOFTWARE SECURITY SPECIALIST ADVANCED	BANCO DE CRÉDITO DEL PERÚ	- Colaborar con los usuarios responsables y otras unidades de apoyo en analizar y evaluar los procesos del negocio; comprendidos en el ámbito de responsabilidad del departamento al que pertenece; en cuanto a niveles de seguridad (confidencialidad,	01/02/2020 - 01/12/2021

		integridad, disponibilidad) y riesgo, de los recursos de información involucrados en los mismos (redes, sistemas, aplicaciones, bases de datos, plataformas, etc.). - Ayudar a determinar y definir los requerimientos específicos de seguridad y proponer las medidas necesarias para corregir debilidades explotables. - Evaluar la efectividad y eficiencia de las medidas de seguridad y control establecidos, buscando en lo posible implementar sistemas de alerta automáticos y de revisión centralizada. - Supervisor del equipo de Pases - Gestión de Accesos, a cargo de 9 personas.	
SUPERVISOR DE PASES - GESTION DE ACCESOS	BANCO DE CRÉDITO DEL PERÚ	- Coordinación directa con las diferentes jefaturas de TI. - Participación en los pases de aplicativos en ambiente productivo aprobados por el área de Seguridad TI (Análisis, revisión y ejecución).	01/12/2018 - 01/02/2020
ADMINISTRADOR DE ACCESOS PRINCIPAL	BANCO DE CRÉDITO DEL PERÚ	- Participación en los pases de aplicativos en ambiente productivo aprobados por el área de Seguridad TI (Análisis, revisión y ejecución). - Administración de todos los aplicativos estándares usados en el	01/08/2018 - 01/12/2018

ADMINISTRADOR DE ACCESOS	BANCO DE CRÉDITO DEL PERÚ	banco con el fin de llevar el control sobre los mismos, manteniendo la seguridad y confidencialidad de acuerdo con las normas establecidas.	
		- Administración de portal AZURE (VM, SQL SERVER y BD, etc).	
		- Participación en la definición de flujos para la aplicación de las diferentes políticas y normas de seguridad en los proyectos de TI.	
		- Administración de todos los aplicativos estándares usados en el banco con el fin de llevar el control sobre los mismos, manteniendo la seguridad y confidencialidad de acuerdo con las normas establecidas.	
		- Gestión de matriz de roles aplicados a cada puesto dentro de la empresa. - Administración de los diferentes tipos de servidores y base de datos utilizados para la infraestructura de la empresa (LINUX, WINDOWS, ORACLE, AZURE). - Administración del Directorio Activo y de sistema de correo electrónico corporativo (EXCHANGE y OFFICE365).	01/02/2016 - 01/08/2018

OPERADOR HELPDESK ACCESOS		- Encargado de brindar asistencia técnica remota a los diferentes colaboradores del banco.	
	BANCO DE CRÉDITO DEL PERÚ	- Administración de active directory.	01/08/2014 - 01/02/2016
		- Manejo de sistemas operativos (windows, aix, linux).	
		- Elaboración de reportes con métricas para el control de indicadores de satisfacción de atención.	

CAPÍTULO II – CONTEXTO EN EL QUE SE DESARROLLA LA IDEA

2.1. La empresa

La empresa sobre la cual se desarrolló el presente trabajo es una de las principales entidades bancarias peruanas. Entre los principales servicios que ofrece se encuentran los financiamientos para comercio exterior, arrendamiento, seguros y asesoría financiera.

2.2. Propósito

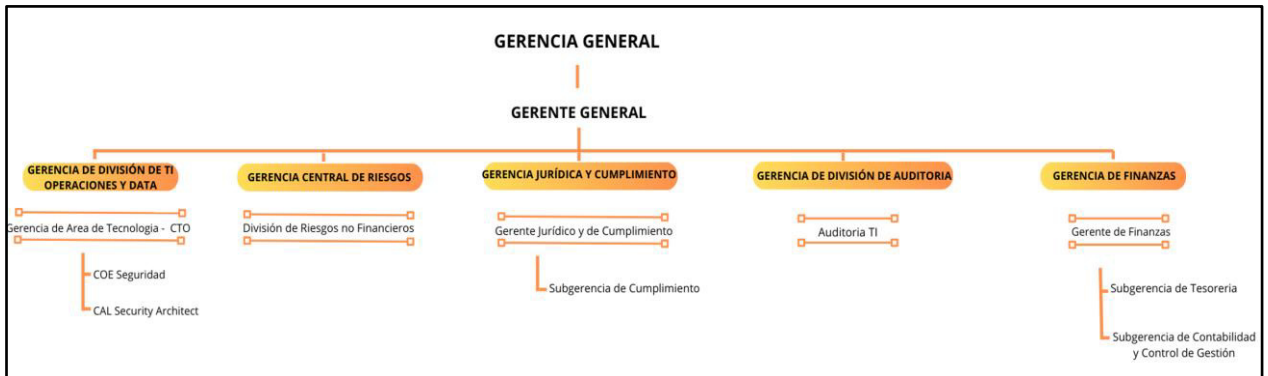
El propósito de la entidad bancaria es estar siempre con sus clientes, alentando y transformando sus sueños y planes en realidad y con el Perú, construyendo su historia de desarrollo y superación. (BCP, 2023)

2.3. Aspiración

- Ser la empresa peruana que brinda la mejor experiencia a los clientes. Simple, cercana y oportuna.
- Ser la comunidad laboral de preferencia en el Perú, que inspira, potencia y dinamiza a los mejores profesionales.
- Ser referentes regionales en gestión empresarial potenciando nuestro liderazgo histórico y transformador de la industria financiera en el Perú. (BCP, 2023)

2.4. Organización de la empresa

Figura 1 – Organigrama empresa



Nota: Se presenta el organigrama de la empresa con las principales gerencias.

2.5. Área, cargo y funciones desempeñadas

Al momento de la implementación de la solución desarrollada en el presente trabajo, me encontraba laborando como Infrastructure Security Specialist en el área de Seguridad TI.

Dentro de mis principales funciones se encontraban:

- Colaborar con los usuarios y otras unidades de apoyo en analizar y evaluar los procesos del negocio; en cuanto a niveles de seguridad y riesgo de los recursos de información involucrados en los mismos (sistemas, aplicaciones, bases de datos, etc.).
- Ayudar a determinar y definir los requerimientos específicos de seguridad y proponer las medidas necesarias para corregir debilidades explotables.
- Evaluar la efectividad y eficiencia de las medidas de seguridad y control establecidos.
- Investigar y analizar nuevas debilidades descubiertas en plataformas y software de base utilizado en la red de la organización, evaluar la posibilidad de materialización de los riesgos y determinar las medidas preventivas y de control necesarias para evitarlo, coordinando la implementación de estas.

- Definir las configuraciones de seguridad recomendadas para las plataformas en uso y coordinar el proceso de actualización permanente de las mismas.
- Apoyar a la División de Auditoría y Área de Seguridad y Prevención de Fraudes en la ejecución de trabajos especiales a su solicitud.

2.6. Experiencia profesional realizada en la organización

Al momento de la realización del presente trabajo cuento con más de 9 años de experiencia laboral dentro de la misma organización desempeñándome en los siguientes puestos:

Operador de Helpdesk, en el cual dentro de mis principales funciones se encontraba el poder brindar soporte técnico a todos los colaboradores del banco mediante su central de Helpdesk.

Administrador de accesos, dentro de mis principales funciones era manejar toda la gestión de accesos de los colaboradores del banco en todos los sistemas en producción.

- Administrador de accesos principal, dentro de mis principales funciones se encontraba el participar en los releases o pases a producción de los diferentes sistemas participando desde el frente del manejo de accesos.
- Supervisor de pases – Gestión de accesos, en esta posición estuve a cargo de un equipo de 8 personas encargados de participar en los pases a producción, resolución de incidentes siempre desde el frente de gestión de accesos.
- Software security specialist advanced, dentro de mis principales funciones se encontraba el acompañar a los Squad en donde me encontraba asignado analizando y evaluando continuamente los diferentes procesos de negocios en cuanto a niveles de seguridad. En este punto me encontraba asignado a la aplicación YAPE la cual es, hoy en día, una de las principales Fintech del país.
- Software security specialist senior, en esta posición obtuve un grado de seniority por mi experiencia demostrada en mis diferentes labores.
- Infrastructure security specialist senior, dentro de mis principales funciones se encuentra el ser responsable de tecnologías de seguridad de información

como el sistema Privileged Access Management (PAM) sobre el cual se desarrolla el presente trabajo.

Acompañado de mi buen desempeño laboral, estuve en constante capacitación la cual es avalada por las certificaciones. Dentro de las principales certificaciones se encuentran las relacionadas a Microsoft Azure: AZ900 (Fundamentals), AZ104 (Administrator), AZ500 (Security Engineer). Así también, cuento con certificaciones referentes a la ISO27001 y al área de ciberseguridad.

CAPÍTULO III – ACTIVIDADES DESARROLLADAS

3.1. Situación Problemática

Como contexto para la definición de la situación problemática se puede indicar que dentro de la entidad bancaria existe el área de Gestión de Accesos compuesta por aproximadamente 20 personas. Esta área es la encargada de toda la parte de gestión de accesos (altas, bajas y modificaciones) de todos los colaboradores de la organización (más de 27000 colaboradores).

Uno de los requerimientos que ellos atienden son los accesos privilegiados a los diferentes tipos de servidores con sistemas operativos, tales como, AIX, RHEL, Windows Server (aproximadamente el banco maneja más de 1300 servidores en entorno productivo). En este punto es que existía la problemática sobre la gestión de accesos en general en los servidores ya que al ser un proceso completamente operativo y manual había muchas deficiencias claramente visibles por el mismo equipo y la organización. Uno de los principales problemas eran los tiempos de atención de los requerimientos que manejaba esta área ya que el brindar el acceso a un colaborador sobre un servidor llevaba aproximadamente 5 minutos, ahora imaginemos que ese colaborador pertenece a un área de soporte dentro de la organización y que por su rol necesita el acceso sobre todo el parque de servidores para cumplir con sus funciones. Estamos hablando de alrededor 125 horas que tomaría para una sola persona el poder brindar este acceso, lo cual se volvía inmanejable ya que además luego de terminar esta tarea se tenía reportes de incidentes por falta de accesos o errores en el aprovisionamiento de estos.

El escenario mencionado anteriormente se repite cuando se tenía el caso en que uno de estos colaboradores dejaba de laborar en la organización o cambiaba de puesto y se le debía modificar o retirar estos permisos.

Debido a estos escenarios es que en reiteradas ocasiones se tenían observaciones por parte de las diferentes áreas que velan por el debido cumplimiento de los lineamientos internos de la organización, por ejemplo, el área de auditoría, al encontrar accesos que ya no correspondían o accesos mal

brindados. Era algo reiterativo dentro del área de Gestión de Accesos el que se impongan observaciones porque se encontraban cuentas de colaboradores que ya no laboraban en el banco o que ya no tenían justificación del porqué de sus accesos (posiblemente porque en algún momento cambió de puesto). En otras ocasiones tal vez sí le correspondía el acceso a un servidor, pero no tenían el nivel de privilegio necesario. En muchas ocasiones se encontraban permisos del tipo “Administrador” sin sustento alguno, que posterior a la observación eran retiradas por el área de Gestión de Accesos (nuevamente de manera manual).

Otro problema que se presentaba es que en los servidores con sistemas operativos AIX y RHEL se creaban los usuarios de manera local lo cual hacía que un mismo usuario pueda tener diferentes claves en cada servidor, lo cual conllevaba muchas veces a olvido de credenciales, generando mayor demanda en los requerimientos del tipo cambio de clave. Adicionalmente, se presentaba problemas con las credenciales ya que no se rotaban de manera periódica y en muchos casos eran estáticas por lo cual quedaban expuestas a malas prácticas.

Un punto adicional que sumó al poder buscar alguna solución tecnológica que nos ayude en toda esta parte es que, luego de brindarse estos permisos privilegiados no se tenía un control sobre ellos. Los usuarios eran libres de hacer y deshacer con dichos permisos sin que haya un tipo de restricción, seguimiento o monitoreo.

Muchas veces cuando se tenía alguna acción que debía ser investigada, se tenía que recurrir a los logs de los propios servidores los cuales muchas veces no se almacenaban de manera correcta.

Es por todo lo detallado que de manera conjunta entre el área de Seguridad TI, el área de Arquitectura de TI y el área de Gestión de accesos llevaron a cabo el proyecto de poder implementar un sistema integral de seguridad que cubra con todas (o en su defecto con la mayoría) de las necesidades de las diferentes áreas impactadas por todos estos problemas.

3.2. Definición del problema

Problema Principal

- Deficiencia en el manejo de la gestión de accesos en los servidores productivos de una entidad bancaria.

Problemas Secundarios

- Demora en tiempos de atención relacionado a accesos en servidores.
- Incidentes por falta o errores en accesos sobre servidores.
- Observaciones reiteradas por parte de equipos que velan el nivel de cumplimiento (como auditoría interna) por presencia de accesos sobre servidores que no se encuentran justificados.
- Manejos de varias cuentas y credenciales por usuario para el acceso a los servidores.
- No se presentaba controles o monitoreo del uso post aprovisionamiento de los accesos privilegiados a servidores.
- Deficiencia en la gestión de credenciales de usuarios que cuentan con acceso a servidores.

3.3. Solución

Teniendo en cuenta que el problema principal era el manejo de cuentas privilegiadas sobre servidores es que el área de Arquitectura de TI basándose en diferentes estudios e investigaciones publicados por empresas de renombre para estos casos, como ejemplo Gartner que es uno de los principales referentes en cuanto a consultoría e investigación de tecnologías de información, definió que la mejor tecnología que se adaptaba a las necesidades presentadas era un Privileged Access Management.

Como una etapa previa se realizaron diferentes POC's (Proof of concept) con diferentes empresas proveedoras que participaron de la licitación. En este punto se basaron en el cuadrante mágico elaborado por la empresa Gartner para

tener una referencia de los principales postores referentes a PAM, entre las principales empresas que se presentaron se encuentran:

- BeyondTrust
- CyberArk
- Okta

Luego de ello se validó que la mejor opción era la propuesta presentada por la empresa BeyondTrust, por lo cual se seleccionó la herramienta presentada por dicha empresa para su implementación dentro de la organización.

3.2.1. Objetivos

El objetivo principal de todo este proyecto definido por las áreas de Seguridad TI, Arquitectura de TI y Gestión de Accesos fue:

- Implementar un sistema Privileged Access Management para mejorar la gestión de accesos sobre los servidores implementados en entorno productivo dentro de la entidad bancaria.

Dentro de los objetivos en específico podemos detallar los siguientes:

- Centralizar la gestión de accesos a servidores mediante grupos de red de Active Directory.
- Limitar el nivel de acceso en los servidores en base a reglas y políticas.
- Tener un mejor control y monitoreo del uso de las cuentas privilegiadas sobre los servidores.
- Inicio de sesión único para el usuario para que cuente con el acceso a servidores con diferentes sistemas operativos.
- Gestión automatizada de contraseñas de todas las cuentas privilegiadas.

3.2.2. Alcance

Alcance funcional. El alcance funcional fue implementar un sistema Privileged Access Management de la marca BeyondTrust que cubra la gestión de accesos en todos los servidores de entorno productivo que cuenten con sistemas operativos AIX, RHEL y Windows Server, aproximadamente 1300 servidores en total. Las áreas responsables de cumplir con el alcance definido fueron las áreas de Gestión de Accesos y Seguridad TI.

En el alcance funcional se incluye lo siguiente:

- Creación de flujos de procesos para los requerimientos asociados a este nuevo sistema.
- Modificación de los flujos actuales de aprovisionamiento de servidores para que se adapten al nuevo sistema.
- Definición de reglas y políticas internas dentro del sistema para el control de los accesos.

Alcance organizacional. A su vez el alcance organizacional fue la Gerencia de División de TI, Operaciones y Data dentro de la entidad bancaria.

3.2.3. Etapas y metodología

Metodología

La entidad bancaria donde se realizó el presente proyecto de implementación define dentro de su proyecto de transformación ágil el uso de SCRUM como uno de los frameworks que se pueden emplear para el desarrollo de sus diferentes proyectos.

Originalmente, Agile era una metodología de gestión de proyectos descrita en el Manifiesto Ágil. Este enfoque pretendía permitir a los desarrolladores de software:

- Adaptarse rápidamente a los cambios.
- Ver mejor las oportunidades.
- Ganar transparencia en los procesos.

- Detectar bloqueos en el camino hacia la eficiencia.

Aunque se utiliza ampliamente en el desarrollo de software, la metodología Agile puede aplicarse a casi cualquier proceso que pueda planificarse y gestionarse. La ciberseguridad no es una excepción, ya que requiere flexibilidad y mejoras periódicas para proporcionar el nivel necesario de eficacia y protección.

Al ser el núcleo de la ciberseguridad de una organización, la gestión de identidades también necesita un método de entrega eficiente, rápido y flexible. Una forma de establecer dicho método de entrega es enfocar la estrategia de la gestión de identidades desde una perspectiva de Agilidad. (Ekran, 2023)

Los proyectos de gestión de identidades se consideran complejos porque hay que dar muchos pasos antes de completar el proyecto, como la configuración del producto, la recopilación de información, las integraciones y otras configuraciones.

Ahora, imagine que en el paso de integraciones se descubre que un conector no se ha implementado siendo necesario para el negocio. En este punto un marco de desarrollo ágil nos ayudaría a poder incluir este cambio de forma más precisa y rápida mediante su metodología.

Es por estos casos que, para realizar entregas más precisas y rápidas relacionadas a proyectos de identidades, se aplica un marco de desarrollo ágil, o Scrum. (Security Intelligence, 2023)

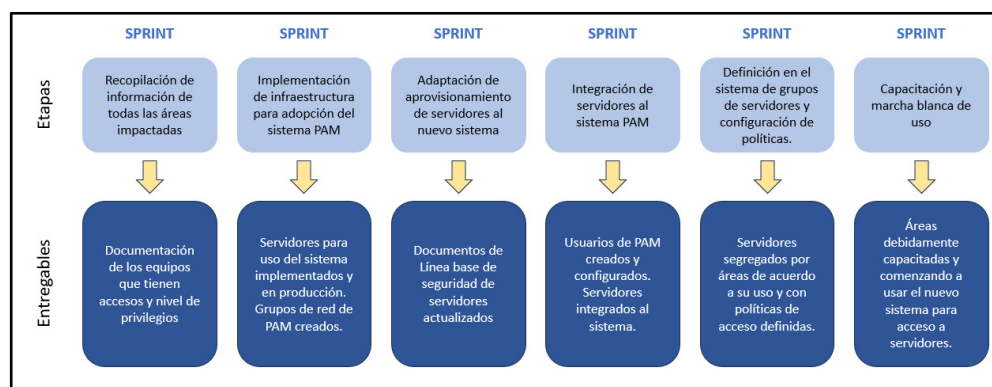
La transformación digital y la optimización de las empresas requieren una prestación de servicios de IAM rápida y progresiva. Los líderes de seguridad y gestión de riesgos responsables de IAM deben responder a estas expectativas; DevOps y las metodologías ágiles proporcionan enfoques que contribuyen al desarrollo de soluciones con capacidad de respuesta. (Gartner, 2023)

Por todas estas razones es que se optó por usar la metodología ágil SCRUM para la implementación de este proyecto, siendo SCRUM una metodología que se adaptó de forma eficiente a las características particulares de este proyecto de gestión de cuentas privilegiadas.

Para la implementación del proyecto, se tuvo en cuenta las siguientes consideraciones descritas:

- El tiempo para la implementación de la solución fue de 3 meses.
- Se consideraron 6 sprints cada uno de 15 días de duración.
- Se consideraron 6 fases que van desde el levantamiento de información de todas las áreas involucradas hasta la implementación final validada por los diferentes actores que interactuaron con el sistema.

Figura 2 – Etapas del proyecto.



NOTA: Se detallan las etapas que se consideraron en el proyecto.
Elaboración propia.

En la primera etapa “Recopilación de información de las áreas impactadas”, se contempló reunirse con todas las áreas impactadas que en su momento tenían o contaban con el acceso a servidores productivos de la organización para recopilar información referente a los casos de uso que manejaba cada área y el nivel de privilegios, con el fin de tener un panorama más general de en qué momentos o cuales eran las principales casuísticas del uso de estos permisos. En esta primera etapa el entregable

sería contar con la documentación de los equipos que tienen accesos y el nivel de privilegios.

En la segunda etapa “Implementación de infraestructura para adopción del sistema PAM”, se contempló el poder gestionar el aprovisionamiento de la infraestructura necesaria (servidores, bases de datos, etc.) para que el nuevo sistema PAM pueda operar dentro de la organización, para ello se trabajó de la mano con la empresa proveedora owner de esta tecnología para que se brinde el acompañamiento del caso y validar que las características con las que se implementaron estos sistemas sean los necesarios para un correcto funcionamiento de la aplicación PAM. En esta segunda etapa el entregable sería contar con los servidores para el uso del sistema correctamente implementado; así como, tener ya creados los grupos de red en active directory.

En la tercera etapa “Adaptación de aprovisionamiento de servidores al nuevo sistema”, se contempló el poder revisar el flujo de aprovisionamiento de los servidores productivos con la finalidad de actualizarlo y que contemple la integración del servidor al sistema PAM desde su aprovisionamiento, para ello tuvimos que revisar la documentación de Líneas Base de Seguridad de los diferentes Sistemas Operativos de los servidores de la organización. En esta tercera etapa el entregable sería contar con los documentos de Línea Base de Seguridad correctamente actualizados.

En la cuarta etapa “Integración de servidores al sistema PAM”, se contempló la integración de los servidores productivos existentes en dicho momento dentro de la organización al nuevo sistema PAM, para ello se tuvo que realizar la creación de varios activos (usuarios, grupos, etc.) y su correcta configuración en el sistema PAM. El entregable en esta cuarta etapa sería tener los usuarios de PAM creados y configurados; así como, los servidores ya integrados con el sistema.

En la quinta etapa “Definición en el sistema de grupos de servidores y configuración de políticas”, se contempló el poder crear grupos para asociar los servidores de acuerdo con la necesidad que tenía cada área y poder crear políticas de acceso con definiciones que limite el uso de las cuentas privilegiadas de la mejor manera sin interrumpir la operativa de las diferentes áreas. En esta etapa el entregable sería contar con los servidores segregados por área de acuerdo con su uso y con las políticas de acceso correctamente definidas.

En la sexta etapa “Capacitación y marcha blanca de uso”, se contempló el poder tener diferentes sesiones de capacitación con las diferentes áreas que interactuarían con el sistema PAM para explicarles cómo es que funciona el nuevo sistema y su correcto uso, adicionalmente despejar todas las dudas que puedan surgir. En esta etapa el entregable sería contar con las diferentes áreas debidamente capacitadas y comenzando a usar el nuevo sistema PAM.

3.2.4. Fundamentos utilizados

Privileged Access Managment

Gartner define la gestión de acceso privilegiado (PAM) como herramientas que gestionan y protegen cuentas, credenciales y comandos que ofrecen un nivel elevado de acceso técnico, es decir, administran o configuran sistemas y aplicaciones en general. Disponibles como software, SaaS o dispositivos de hardware, las herramientas de gestión de acceso privilegiados (PAM) gestionan el acceso privilegiado de personas (administradores de sistemas y otros), sistemas y aplicaciones. (2023)

La gestión de acceso privilegiado (PAM) es una solución de seguridad de identidades que ayuda a proteger a las organizaciones contra las ciberamenazas mediante la supervisión, detección y prevención del acceso privilegiado no autorizado a recursos críticos. PAM funciona a través de una combinación de personas, procesos y tecnología y le da visibilidad sobre quién está utilizando cuentas privilegiadas y lo que están haciendo mientras están

conectados. Limitar el número de usuarios que tienen acceso a funciones administrativas aumenta la seguridad del sistema, mientras que las capas adicionales de protección mitigan las violaciones de datos por parte de los actores de amenazas. (Microsoft, 2023)

Aunque la gestión de privilegios abarca muchas estrategias, un objetivo central es la aplicación del mínimo privilegio, definido como la restricción de derechos de acceso y permisos para usuarios, cuentas, aplicaciones, sistemas, dispositivos y procesos informáticos al mínimo necesario para realizar actividades rutinarias y autorizadas.

PAM permite a las diferentes organizaciones administrar de manera centralizada determinado grupo de cuentas privilegiadas, en vez de tener un gran número de estas mismas cuentas por cada usuario.

Cuando un usuario autorizado requiere el acceso a estas cuentas, simplemente se dirige hacia el sistema PAM que tiene implementado, pudiendo así usar la cuenta privilegiada sobre la cual puede definir un tiempo límite de la sesión, especificar la necesidad de su uso y entre otras cosas, dependiendo de las reglas que tiene adoptada la organización.

A su vez los sistemas PAM se pueden integrar a otros sistemas para hacer más funcional su uso y poder integrarse de una mejor manera a los diferentes flujos de trabajo presentes en cada organización. Un ejemplo de ello sería la capacidad de integrarse con las IT Service Management (o por sus siglas en inglés “ITSM”) para una adecuada gestión de servicios. O también integrarse con otras soluciones de seguridad como los Security Information and Event Management (o por sus siglas en inglés “SIEM”) para una adecuada administración de eventos que pueda generar el sistema PAM.

Cada plataforma PAM, dependiendo de la empresa desarrolladora, proporciona una amplia variedad de integraciones con diferentes aplicaciones para así enriquecer las ventajas que de por sí ya traen estos tipos de sistemas.

Otro punto resaltante de las herramientas PAM de acuerdo con Antti Kuokkanen (2020) este tipo de soluciones presentan una lista extensiva de componentes, dentro de las más comunes y principales podemos encontrar:

- Almacenamiento de contraseñas.
- Gestión de contraseñas.
- Gestión de privilegios.
- Gestión de sesiones.
- Cumplimiento.
- Integración de sistemas.
- Reportes y analítica.

Algunos ejemplos referentes a cuentas con accesos privilegiados manejados por personas son:

- Cuentas de superusuarios: Cuenta con un nivel alto de privilegios utilizado principalmente por los administradores de sistemas informáticos.
- Cuenta administradora de dominio: Cuenta que proporciona acceso administrativo privilegiado a todas las estaciones de trabajo y servidores de dominio de una red.
- Cuenta administrativa local: Esta cuenta se ubica en un endpoint o estación de trabajo. Generalmente utiliza una combinación de nombre de usuario y contraseña.

Algunos beneficios de la gestión de accesos privilegiados son:

- Impulsa el principio de mínimo privilegio permitiendo el acceso y uso a las cuentas privilegiadas sólo cuando sea completamente necesario.
- Ayuda con el cumplimiento de las regulaciones mediante diferentes controles como preventivos, correctivos y de monitoreo constante.
- Mejora la productividad y experiencia al usuario al tener automatizado la gestión de accesos a cuentas privilegiadas que son compartidas.

- Establece un límite al uso de las cuentas mediante la adopción de políticas de acceso.

Hoy en día existen varios casos de uso de implementación de estos sistemas en diferentes sectores, dentro del trabajo de Karen Waltermire (2018) podemos ver una guía práctica de PAM enfocado al sector financiero consistente con los principios del marco NIST 337 para mejorar la ciberseguridad de infraestructuras críticas. Vemos claramente como nos detalla una guía completa que abarca desde un alto nivel la arquitectura, diseño y ejemplos de casos de usos en donde aborda diferentes escenarios y soluciones a dichos escenarios con el uso de PAM y sus beneficios e integraciones a otras plataformas como SIEM para abordar estos casos y darles una solución adecuada.

SCRUM

Scrum es un marco de trabajo ágil mediante las personas pueden abordar problemas complejos en un entorno cambiante sobre el cual se entregan productos de forma eficiente y creativa con el máximo valor posible.

Amazon describe a SCRUM como un marco de administración que los equipos utilizan para organizarse por su propia cuenta y trabajar para poder alcanzar un objetivo en común. Describe un conjunto de sesiones, herramientas y funciones para entregar valor de forma eficiente. Las prácticas de Scrum permiten a los diferentes equipos de trabajo manejarse por cuenta propia, ganar aprendizaje a partir de la experiencia y poder adaptarse al cambio. (2023)

El funcionamiento de la metodología SCRUM pasa por diferentes fases:

- Planificación. Dentro de la planificación podemos hablar del producto backlog. En esta fase se establecen las tareas prioritarias, obteniéndose información de ellas para su desarrollo. Tener en cuenta que no es necesario definir los objetivos desde un inicio ya que la metodología te

permite cambiar el alcance sobre la marcha. En esta fase se realiza un documento a alto nivel con los requisitos del proyecto a ejecutarse, así como las descripciones detalladas de las funcionalidades esperadas siendo priorizadas de acuerdo con su valor y retorno de inversión.

- Ejecución. En esa fase podemos hablar de los “sprints”. En esta etapa se produce el desarrollo de un producto que termina como un entregable. El equipo de trabajo se centra en la ejecución de tareas para llegar al objetivo previamente definido en la fase de planificación
- Control. En la última fase se mide y controla el avance del proyecto para ver su progreso. Dentro de esta fase el responsable, generalmente el Scrum Master, es quién actualiza y mide el avance de acuerdo con la finalización de las tareas dependiendo del criterio de aceptación previamente establecido.

Ventajas del uso de Scrum:

- Fomenta el trabajo en equipo, los miembros del equipo se mantienen interesados en las tareas a realizar teniendo en claro su prioridad.
- Resultados anticipados ya que de cada etapa del proceso se obtiene resultados. Por lo que al cierre de cada sprint ya puede visualizarse ciertos logros y ya no es necesario esperar al final del proyecto.
- Es una metodología flexible ya que es adaptable a las dificultades o cambios que puedan surgir sobre la marcha del proyecto. También se entiende que es flexible porque se puede adaptar a empresas, disciplinas, y otros sectores.

Desventajas del uso de Scrum:

- Puede necesitar cambios dentro de la organización donde se implemente debido a su modelo de trabajo en sus diferentes departamentos o áreas.

- Las tareas y plazos deben estar siempre correctamente definidos para que se pueda aplicar correctamente la metodología.
- No es recomendable para equipos nuevos ya que el éxito de la implementación de la metodología depende mucho de la experiencia y capacidades que tengan los integrantes de estos equipos para poder sobrellevar las exigencias presentes.

Active Directory

Active Directory (AD) es un servicio de directorio desarrollado por Microsoft para redes Windows. Active Directory (AD) desempeña un rol importante para las diferentes empresas que tienen recursos informáticos complejos, derechos de usuario y grupos de trabajo jerárquicos: Active Directory puede considerarse básicamente como una guía de datos como direcciones y teléfonos, pero con muchas más opciones para que los administradores realicen diferentes funciones con los datos de usuarios y objetos almacenados como gestionar, editar, consultar y estructurar. La estructura informática de una organización puede dividirse en los denominados dominios con ayuda del servicio de directorio. (IONOS, 2023)

Windows Server

Windows Server es una plataforma o sistema operativo de la empresa Microsoft que sirve para compilar una infraestructura de aplicaciones, redes y servicios web conectados desde el grupo de trabajo hasta el centro de datos. Establece un nexo entre los entornos locales y diferentes plataformas y añade capas adicionales de seguridad al tiempo que ayuda a modernizar las diferentes aplicaciones y la infraestructura. (Microsoft, 2023)

Hoy en día se tienen muchas versiones de este sistema operativo enfocado para el manejo de servidores, desde su primer versión Windows Server 2000 hasta su más reciente versión Windows Server 2022. Teniendo en cuenta que actualmente Microsoft sólo brinda soporte a versiones Windows Server 2016 y superior.

Dentro del presente trabajo veremos que este sistema operativo es usado dentro de la mayoría de los servidores de la organización.

Linux

Linux es un sistema operativo (SO) de código abierto ampliamente reconocido a nivel mundial. En 1991, Linus Torvalds lo diseñó y creó como hobby. Mientras estudiaba en la universidad, intentó crear una versión de código abierto, alternativa y gratuita del sistema operativo MINIX, que a su vez se basaba en los principios y el diseño de Unix. Ese hobby logró convertirse en el sistema operativo con mayor base de usuarios, el más utilizado en servidores de Internet de acceso público y el único empleado en los 500 superordenadores más rápidos. (Red Hat, 2023)

Este sistema operativo tiene un gran número de casos prácticos, distribuciones y dispositivos basándose en las necesidades y cargas de trabajo del usuario final.

Incluso dentro de los diferentes entornos de nube como Azure de Microsoft, Amazon Web Service de Amazon y Google Cloud Platform de Google, podemos encontrar hoy en día varias imágenes disponibles al público para su uso.

3.2.5. Implementación de las áreas, procesos, sistemas y buenas prácticas

Antes de comenzar a explicar el proceso de implementación, es necesario detallar que para este caso la entidad organizó un proceso de licitación para ver dentro del mercado las mejores propuestas referente a sistemas de Privileged Access Management. Dando como resultado final la firma de contrato con la marca BeyondTrust para el acompañamiento de su sistema PAM dentro de la organización.

Primera etapa: Recopilación de información de las áreas impactadas

En esta etapa se tuvieron diferentes reuniones con todas las áreas involucradas (que contaban en ese momento con acceso a los servidores productivos del banco) como por ejemplo los equipos de Middleware, Batch Operaciones, Storage&Backup, Gestión de accesos, Seguridad TI, Ciberseguridad, entre otros. En este punto se hizo una diferencia sobre los equipos que formaban parte del equipo de proveedores y las áreas internas del banco.

Se recopiló la información de la cantidad de servidores con sistemas operativos AIX, RHEL y Windows Server a las que tenían el acceso y el nivel de privilegio que manejaban en cada uno de ellos para realizar sus funciones, en este punto se logró validar que en la mayoría de los casos los equipos contaban con permisos del tipo administrador sobre los servidores. Se validó también que el acceso esté de acuerdo con matriz de roles, dentro de la organización el término “Matriz de Roles” corresponde a un listado de permisos asociados a un puesto en particular, los cuales han sido validados previamente por diferentes áreas como el área de Seguridad TI, Gestión de accesos y la propia área afectada para poder definir los permisos que tendrían dentro de su matriz de roles basándose en los lineamientos interno de la organización y viendo que no haya ninguna afectación en particular.

De los resultados obtenidos en esta etapa se muestran los siguientes gráficos que resumen la información recopilada.

Tabla 2 – Número de servidores usados por proveedores en la organización.

Proveedores	AIX	LINUX	WINDOWS
Batch Operaciones	287	-	767
Middleware_WME	287	316	767
Middleware Base de datos	287	316	767
Storage&Backup	287	316	767
Midrange UNIX	287	316	-
Release Management	287	316	767
Release Aprovisionamiento	287	316	767
Midrange Win	-	-	767
Monitoring CDM	-	-	767
Monitoring TL	287	-	767
Tool&Standars	-	-	767
T&S Content Managers	287	316	767
Innovation	287	316	767

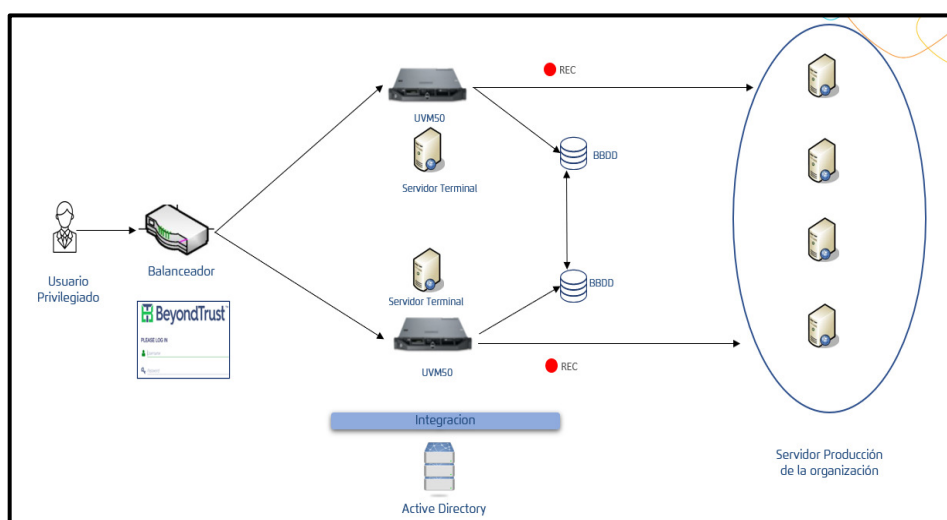
Tabla 3 – Número de servidores usados por áreas dentro de la organización.

Áreas internas	AIX	LINUX	WINDOWS
Gestion acceso - AP		287	316
Gestion acceso - PC		287	316
Seguridad TI		287	316
Ciberseguridad		287	316

Segunda etapa: Implementación de infraestructura para adopción del sistema PAM.

La finalidad de esta etapa era aprovisionar toda la infraestructura necesaria para que el sistema PAM pueda desplegarse de manera correcta, para ello se diseñó el diagrama de arquitectura con la finalidad de tener un mejor entendimiento de cómo trabajaría el sistema y su alcance con los servidores de la organización.

Figura 3 – Arquitectura propuesta para la solución PAM.



Para este caso la arquitectura contemplaba un balanceador interno, ya implementado en la organización, que redirigiría la conexión hacia alguno de los 2 UVM's que se tendrían. En este caso se implementaron 2 servidores del tipo UVM's que eran servidores web IIS (SO: Windows Server) administrados por la propia marca BeyondTrust (las imágenes para el aprovisionamiento de estos equipos habían sido proporcionados por la propia marca).

También se implementaron en la infraestructura productiva de la organización los siguientes equipos:

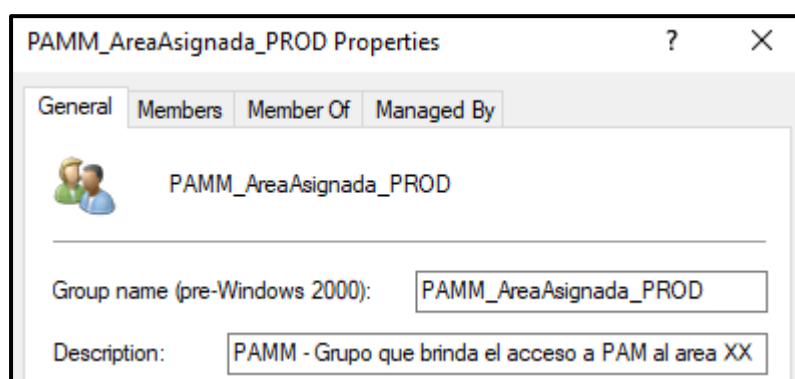
- 2 Servidores Terminal: Estos servidores (SO: Windows Server) tenían como funcionalidad el poder brindar el acceso a aplicaciones virtualizadas desde la web del sistema PAM. Básicamente se utilizó para virtualizar aplicaciones como Putty o WinSCP para el acceso a servidores AIX y RHEL desde la misma web de PAM. Esto hacía que cuando se quisiera acceder a este tipo de servidores desde la web de PAM no fuese necesario que la persona que acceda tenga instaladas estas aplicaciones en su estación para poder trabajar, lo cual hubiese sido una dependencia.
- 2 Servidores de base de datos: Estos servidores (SO: Windows Server) alojan la Base de datos funcional del sistema PAM, para ellos se aprovisionó un SQL Server Management desde donde se trabajó toda la integración con base de datos. Cabe resaltar que ambas bases de datos trabajaban con un sistema Always On configurado.

Dentro del diagrama también se detalló la integración con el Active Directory (AD) de la organización, para este punto el sistema PAM utilizaría el AD de la entidad bancaria tanto para la autenticación como para la autorización manejados y controlados a través de grupos de red que debían ser previamente creados y configurados.

Para el caso de los grupos de red que brindaban la autenticación y autorización se utilizó la nomenclatura “PAMM_AreaAsignada_PROD”

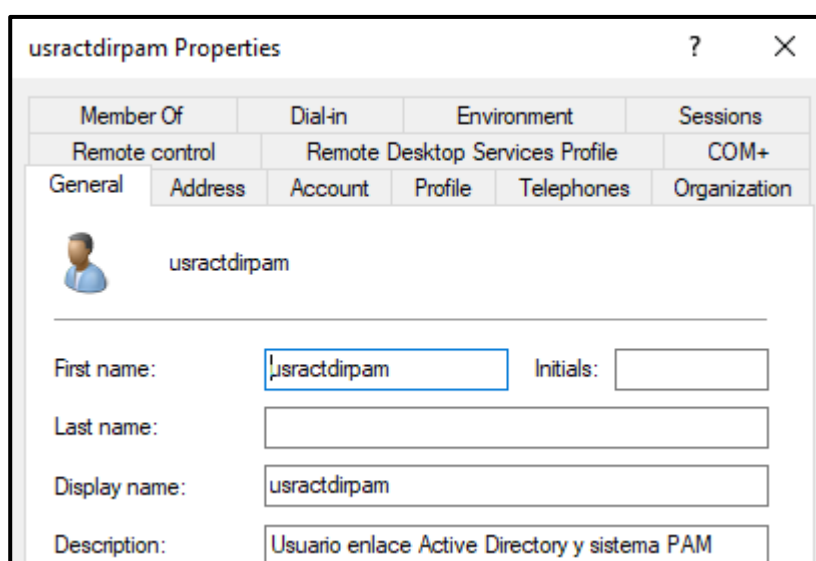
En donde “AreaAsignada” correspondería al nombre o siglas del equipo que tendría el acceso a PAM por medio de ese grupo de red.

Figura 4 – Grupo de red usado para acceder a PAM.



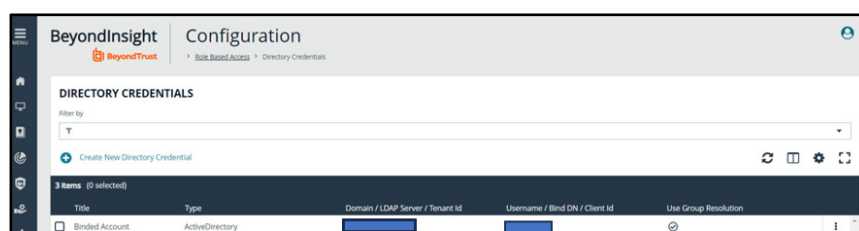
En esta parte, también se consideró la creación de un usuario a nivel de dominio para que funja de enlace entre el sistema PAM y el Active Directory de la organización.

Figura 5 – Usuario enlace Active Directory y sistema PAM.



Una vez creado el usuario se procedió a configurar en el sistema PAM en la opción “Directory credentials” de esta manera se establecía la conexión entre PAM y el AD de la organización para poder tener lectura de los activos que estén creados a nivel de AD y que PAM los pueda identificar.

Figura 6 – Configuración de usuario para enlace entre AD y PAM.



Tercera etapa: Adaptación de aprovisionamiento de servidores al nuevo sistema

En esta etapa se debía adaptar el proceso de aprovisionamiento de servidores para que cuando sean implementados tengan las configuraciones necesarias para poder adaptarse a al sistema PAM.

Para el debido funcionamiento y configuración de los servidores en el sistema PAM es necesario indicar que se debían crear 4 tipos de cuentas privilegiadas detalladas de la siguiente manera:

- Usuario funcional (Nomenclatura: usrfunpro). Usuario principal usado por el sistema PAM para la administración funcional del servidor. Esta cuenta es la encargada de realizar entre otras funciones la gestión de las cuentas que tenga el servidor pudiendo realizar cambios de credenciales, validación de credenciales, entre otras por lo cual tenía un nivel de permisos privilegiados en los servidores (permisos de administrador).
- Usuario para escaneo (Nomenclatura: usrscanpro). Usuario usado para que el sistema PAM pueda escanear el servidor en donde se encuentra creado la cuenta, pudiendo así obtener datos relevantes del servidor para posteriormente ser guardado a nivel de base de datos, por ejemplo, el hostname, dirección ip, entre otros.
- Usuario Manager (Nomenclatura: usrpamxxxx, donde “xxxx son correlativos numéricos). Usuario usado para la conexión hacia los servidores, este es el usuario intermedio entre el sistema PAM y el servidor al que se quiere acceder. Este usuario es el que activa el inicio de sesión y el que tiene el nivel de privilegio en el servidor al que se quiere acceder.

- Usuario contingencia (Nomenclatura: USRPAMPRO). Este usuario no tiene relación directa con el sistema PAM, pero se coordinó su creación en los servidores para que se use en casos de contingencia cuando no se pueda ingresar por medio de PAM al servidor.

La creación de las cuentas se realizó tanto localmente en los servidores como a nivel de dominio en el Active Directory dependiendo del Sistema Operativo del servidor. En el caso de las cuentas locales se tuvo que crear una por cada servidor y en el caso de las cuentas de dominio solo se creó una de cada tipo de cuenta dentro del AD.

Tabla 4 – Detalle de tipo de cuentas creados por Sistema Operativo de servidor.

Sistema operativos	Cuentas Locales	Cuenta de dominio
AIX	x	
RHEL	x	
Windows Server		x

Una vez definido los tipos de cuentas que se tenían que crear se procedió a realizar las coordinaciones debidas para la actualización de las Líneas Base de Seguridad asociadas a estos tipos de servidores. Dentro de la organización nos referimos a Líneas Base de Seguridad al documento en donde se especifica el paso a paso de las diferentes configuraciones a nivel de sistema operativo que se realizan dentro de los servidores para asegurar así las mínimas configuraciones de seguridad que debe tener un servidor al momento de ser provisionado. En este documento por ejemplo se deshabilitan protocolos inseguros, se configuran los diferentes agentes para el monitoreo del servidor y se crean los usuarios que tendrán el acceso al servidor desde un primer momento, entre otro tipo de configuraciones.

Así pues, dentro de estos documentos se logró que se incluyera como un paso adicional la creación de las cuentas asociadas a PAM (usuario funcional, usuario para escaneo, usuario manager y usuario de contingencia) para que posteriormente sean configurados dentro del sistema PAM.

Figura 7 – Extracto de Línea Base de Seguridad de servidor RHEL con detalle de la creación de los usuarios de PAM.

```
3.1.2.11. Crear los usuarios de herramienta PAMM y asignar la clave definida previamente (custodiada por Gestión de accesos). Gestión de accesos (TRIBU ACCESOS)
#Ejecutar los siguientes comandos:

useradd -c "usrfunpro" -g GADMIN -G GADMIN usrfunpro
chage -E -1 -M -1 -1 -1 -1 usrfunpro
passwd usrfunpro
#ingresar el password custodiado

useradd -c usrscanpro -g GSOORTE -G GSOORTE usrscanpro
chage -E -1 -M -1 -1 -1 -1 usrscanpro
passwd usrscanpro
#ingresar el password custodiado

useradd -c USRPAMPRO -g GADMIN -G GADMIN USRPAMPRO
chage -E -1 -M -1 -1 -1 -1 USRPAMPRO
passwd USRPAMPRO
#ingresar el password custodiado
```

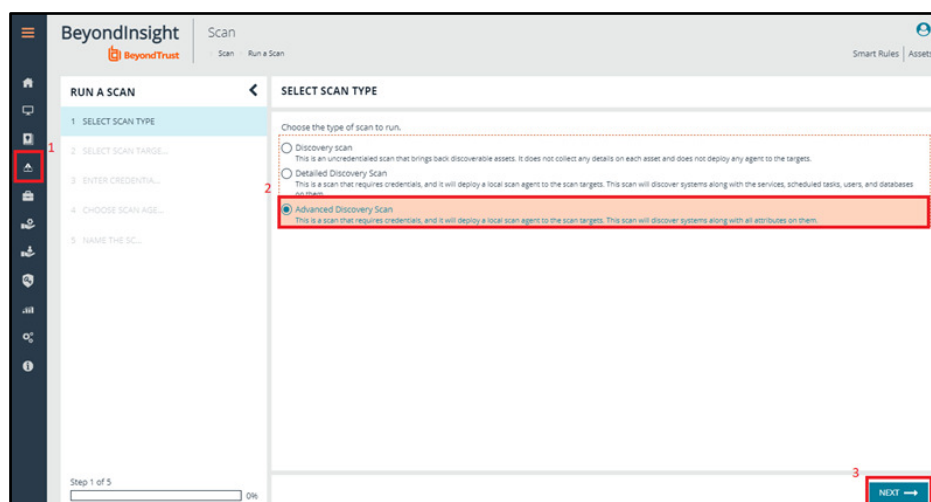
Tener en cuenta que para los casos de los servidores con sistema operativo AIX y RHEL se tenían ya previamente grupos creados detallados en el archivo “sudoers” del servidor con el perfilamiento necesario para las funciones requeridas.

Cuarta etapa: Integración de servidores al sistema PAM

En esta etapa, luego de que ya los servidores contaban con todos los usuarios creados para la integración con el sistema PAM, lo que proseguía era el poder ingresar al sistema PAM que ya se encontraba habilitado dentro de la organización para poder configurarlos.

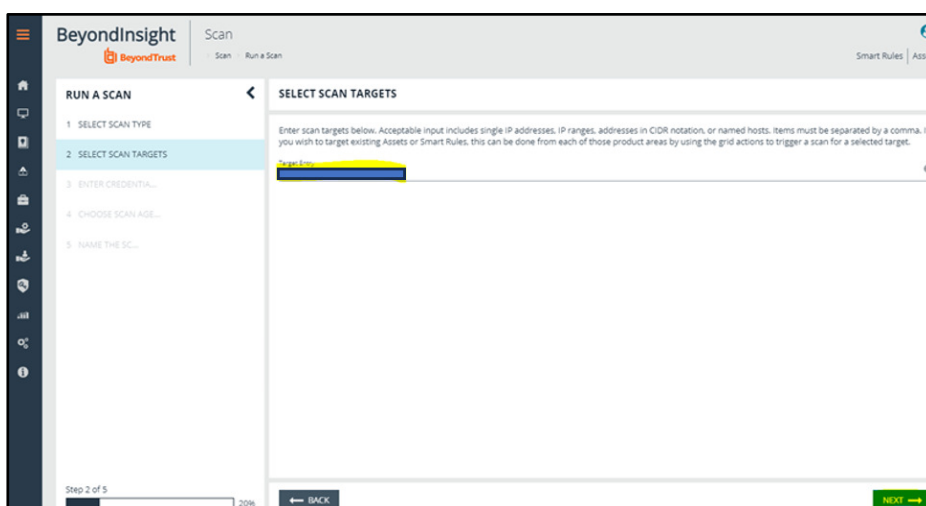
Para ello se ingresa al sistema PAM en la opción “SCAN” y se selecciona la opción “Advanced Discovery Scan”.

Figura 8 – Ingreso a módulo SCAN en el sistema PAM.



Ingresamos el hostname del servidor que será escaneado en este caso.

Figura 9 – Ingreso de datos del servidor en módulo SCAN



Ingresamos las credenciales para realizar el escaneo, en este punto esta credencial fue configurado en el aprovisionamiento del portal PAM.

Figura 10 – Ingreso de credenciales para escaneo de servidor dependiendo del SO del servidor.

The screenshot shows the 'ENTER CREDENTIALS' step in the BeyondInsight interface. On the left, a sidebar lists five steps: 1. SELECT SCAN TYPE, 2. SELECT SCAN TARGETS, 3. ENTER CREDENTIALS (highlighted), 4. CHOOSE SCAN AGENT, and 5. NAME THE SC... The main panel is titled 'ENTER CREDENTIALS' and contains a 'Credential List' section. It has a checkbox for 'Use the same key for all selected credentials (Disabled)' and a 'Choose Existing Credentials (1 Selected)' section. Below this is a search bar and a table of credentials. The first row is selected: 'Usuario scan Linux AIX PROD' with version 'SSH'. Other rows include 'PIB27_scan' and 'user win internet.bcp'. To the right is a 'Custom Credential' form with fields for 'Username', 'Password', and 'Domain (optional)', along with a 'TEST CREDENTIAL' button. At the bottom, there are 'BACK' and 'NEXT' buttons.

Luego seleccionamos un servidor, en este caso se trata de los UVM's implementados en la arquitectura del sistema PAM. Seleccionamos uno de ellos el cual se usará para procesar el escaneo y posteriormente podemos indicar un nombre para el escaneo realizado en esta oportunidad, así como la hora de inicio. Por default tenemos la opción de “inmediate” para que sea un escaneo de inmediato.

Figura 11 – Selección de servidor para procesar escaneo.

The screenshot shows the 'CHOOSE SCAN AGENT' step in the BeyondInsight interface. The sidebar shows step 4, 'CHOOSE SCAN AGENT', is active. The main panel is titled 'CHOOSE SCAN AGENT' and includes a 'Scan Agents' section. It has a 'Filter by' dropdown and a table of agents. The table has columns: 'Agent Name', 'Version', 'Asset', 'Workgroup', and 'Time Zone'. Two items are selected: 'PIB27' (version 6.5.7.3537) and 'PIB28' (version 6.7.8.3735). Both are in the 'BEYONDTRUST WORKGROUP' and have a 'GMT-05:00 -05:00' time zone. At the bottom, there are 'BACK' and 'NEXT' buttons.

Figura 12 – Definición de nombre y hora de inicio de escaneo.

Automáticamente luego, nos aparecerá un registro con fecha y hora del momento y con estado activo. Una vez que se complete el escaneo (tiempo aproximado de 5 minutos) dicho registro dejará de estar activo para pasar a un estado Completado.

Figura 13 – Validación de estado de escaneo de servidor.

Agent Name	Workgroup	Scan State	Scan Name	Status	Hosts Found	Last Updated
BEYONDTRUST WORKGROUP	BEYONDTRUST WORKGROUP	Active	AdvancedDiscoveryScan (GAS)	Schedule Request Issued	0	0:12 PM

Para el caso de los servidores con sistema operativo Windows Server, PAM te da la visibilidad directa de los usuarios de dominio (Linked account) al estar enlazado con el Active Directory del banco, por lo cual no es necesario realizar alguna otra configuración.

Figura 14 – Usuarios de dominio enlazados a un servidor Windows.

Account Name	Platform	Domain	Forest	Status
...	Active Directory	...	...	Linked
...	Active Directory	...	...	Linked
...	Active Directory	...	...	Linked
...	Active Directory	...	...	Linked
...	Active Directory	...	...	Linked

Para los servidores AIX o RHEL se tiene que terminar de configurar los usuarios de PAM (Local Accounts). Para ello buscamos el servidor dentro de la opción “Managed Systems”, tener en cuenta que PAM al momento del escaneo ya te reconoce los usuarios locales creados en el servidor; sin embargo, tenemos que terminar de configurarlos.

En este punto para todo tipo de servidor, se configuran los usuarios manager para que puedan tener la rotación de credenciales ya definidos, en este caso se definió que las credenciales de los usuarios manager usados en PAM rotaría cada 30 días.

Figura 15 – Búsqueda de servidor en opción “Assets”, visibilidad de cuentas locales escaneadas por PAM.

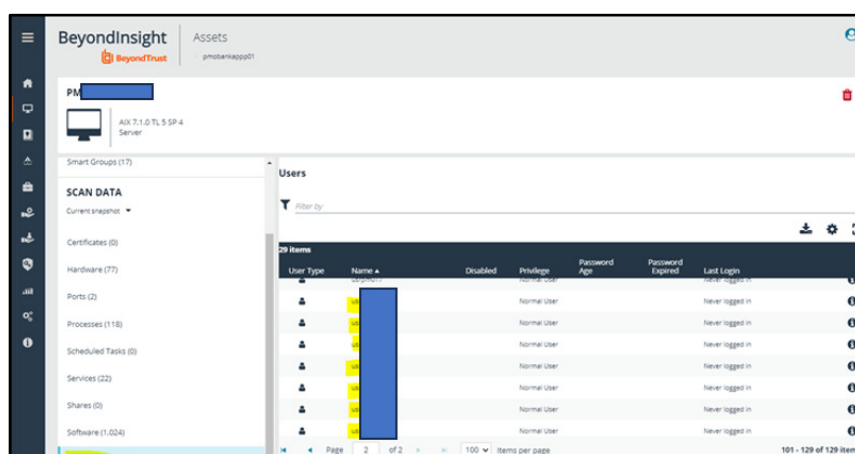


Figura 16 – Búsqueda de servidor en opción Managed Systems.

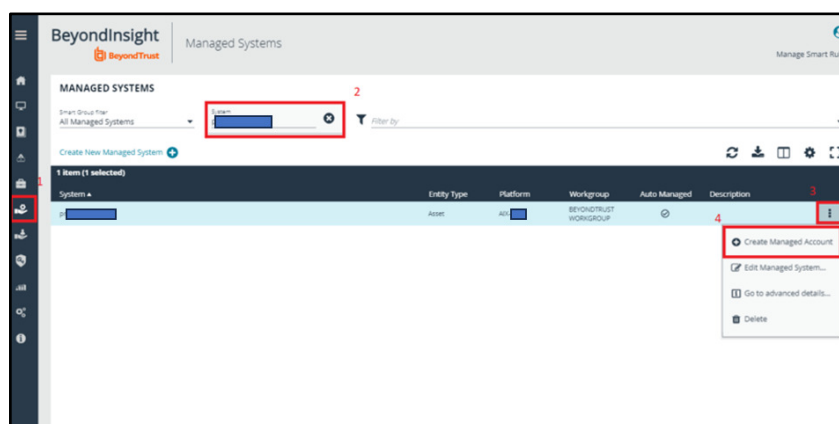


Figura 17 – Configuración de usuario local y su credencial en servidor AIX/RHEL.

The screenshot shows a user configuration window with two main sections: 'Identification' and 'Credentials'. In the 'Identification' section, there are fields for 'Name', 'Description', and 'Workgroup'. The 'Name' and 'Description' fields contain the text 'us'. The 'Workgroup' field is set to 'None'. In the 'Credentials' section, there are fields for 'Password' and 'Confirm Password', both containing masked text. Below these fields is a dropdown for 'Authentication Type' set to 'Password'. At the bottom, there are two checkboxes: 'Allow Fallback to Password (no)' and 'Login Account For SSH Sessions (no)', both of which are unchecked.

Figura 18 – Configuración de rotación de credenciales a usuario manager.

The screenshot shows the 'Automatic Password Change Options' dialog. It has a title bar with a minus button. The dialog contains several settings: a toggle switch for 'Enabled' which is turned on; a 'Password Policy' dropdown menu; a 'Change Password Frequency' dropdown menu set to 'First day of the month'; a 'Change Password Starting From' section with a calendar icon and a time field set to '23:30'; a 'Next Scheduled Change' field showing '11:30 PM'; and three more toggle switches at the bottom: 'Check Password' (turned on), 'Reset Password On Mismatch' (turned on), and an unlabeled one (turned on).

Figura 19 – Validación de usuarios locales de servidores AIX/RHEL configurados en PAM.

The screenshot shows the 'Managed Accounts' window. On the left is a sidebar with 'Advanced Details' and a list of options: 'Details & Attributes', 'Managed Accounts' (selected), 'Smart Groups', 'Linked Accounts', 'Server Keys', and 'Functional Account'. The main area is titled 'Managed Accounts' and has a 'Filter by' dropdown. Below the title bar is a 'Create New Managed Account' button. A table lists the managed accounts. The table has columns: 'Account Name', 'Description', 'Workgroup', 'Auto Managed', 'Last Changed Date', and 'Next Change'. There is one row with the account name 'us', description 'us', workgroup 'BEYONTRUST W...', and 'Auto Managed' checked. The 'Last Changed Date' is '3:42 PM' and 'Next Change' is 'No'.

Account Name	Description	Workgroup	Auto Managed	Last Changed Date	Next Change
us	us	BEYONTRUST W...	☒	3:42 PM	No

Quinta etapa: Definición en el sistema de grupos de servidores y configuración de políticas.

Una vez que ya se han configurado en el sistema PAM los servidores, era el turno de agruparlos de acuerdo con la necesidad de cada equipo de la organización. Tener en cuenta que cada equipo tenía el acceso a ciertos números de servidores (no todos) por lo cual debíamos hacer esa asociación en PAM.

Para este punto es necesario tener en claro ciertos conceptos definidos de la siguiente manera:

- Smart Rule. Pueden ser del tipo Account o del tipo Asset.
- Smart Rule tipo Account. Son reglas inteligentes en el sistema PAM, las cuales te permiten asociar cuentas locales y/o cuentas de dominio de manera masiva.
- Smart Rule tipo Asset. Son reglas inteligentes en el sistema PAM, las cuales aplican para los servidores.
- Address Group. Son conjunto de servidores agrupados.

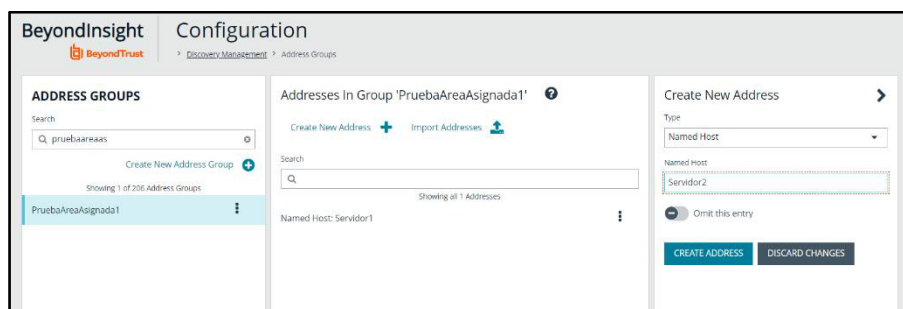
Una vez que se tengan en claro los conceptos anteriores, se debe entender cómo se llega a configurar los grupos de red que brindan accesos a PAM (detallados en la segunda etapa con nomenclatura PAMM_AreaAsiganda_PROD).

En primer lugar, ya se tenían definidos por cada equipo el listado de servidores a los cuales tendrían el acceso y el nivel de privilegios, los cuales son brindados a los usuarios manager de PAM (nomenclatura usrpamxxxx). Por ejemplo, si un usuario quiere tener acceso al servidor “X” con un nivel de privilegio administrador, el usuario manager (usrpamxxxx) debe tener el acceso como administrador en el servidor “X” y este usuario manager posteriormente es configurado al grupo de red asignado al área del usuario.

La configuración en este caso parte creando un Address Group por cada equipo, en los cuales se agregan los servidores a los cuales tendrán el acceso. Para este caso al momento de la creación del Address Group se colocó el

nombre del área y para los servidores se agregaron los hostname (también se puede agregar indicando la ip del servidor).

Figura 20 – Creación y configuración de Address Group



Este Address Group es asociado a un smart rule de tipo asset sobre el cual se aplican ciertos criterios de selección para los servidores y sobre ellos se aplican ciertas acciones. En las siguientes imágenes podemos visualizar que se selecciona un grupo de servidores en este caso de sistema operativo Windows Server y sobre el cual se ejecutan ciertas acciones como, por ejemplo, se configura la cuenta funcional de PAM, el tipo de plataforma aceptada, el tiempo de timeout esperado, entre otros.

Figura 21 – Asociación de smart rule tipo asset con Address Group.

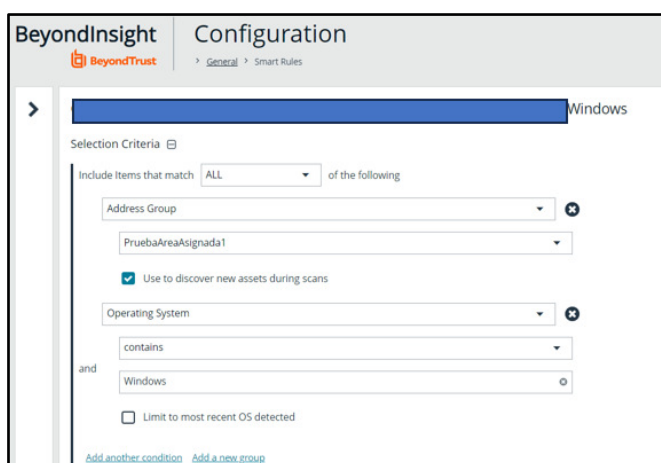


Figura 22 – Acciones configuradas en un smart rule tipo asset.

Manage Assets using Password Safe

Platform: Windows

Change Agent: Password Safe

Account Name Format: Domain\Username

Functional Account: us

Enable Automatic Password Management: yes

Enable Accounts For AD Queries: no

Password Rule: Windows Password Rule

Connection Timeout: 30

En esta etapa también se configuraron unas políticas de contraseñas (password policies) las cuales fueron asociados en el smart rule de tipo asset en el ítem “Password rule”. Estas políticas de contraseñas permitían configurar ciertos criterios para el manejo de credenciales, por ejemplo, te permitía establecer una longitud de caracteres mínimo y máximo para la contraseña usada, definir los tipos de caracteres que podía aceptar la contraseña, permitir el uso de mayúsculas y definir caracteres especiales los cuales se podían detallar.

Figura 23 – Password Policies configurados en PAM.

Password Rule Details

Password Policy Name: Password Rule

Description (Optional): Regla de contraseñas para servidores

Minimum length: 20

Maximum length: 25

Allow use for Secrets Safe: ☐

First Character Value: ☐ Alpha Characters Only ☐ AlphaNumeric Permitted ☒ Any Character Permitted

Uppercase Characters: ☒ Permit uppercase characters (yes)

Numeric Characters: ☒ Permit numeric characters (yes)

Minimum number of required numeric characters: 1

Allow only the following numeric characters: 1 2 3 4 5 6 7 8 9 0

Non-Alphanumeric Characters: ☒ Permit non-alphanumeric characters (yes)

Minimum number of required non-alphanumeric characters: 1

Allow only the following non-alphanumeric characters: # \$ % & ' () * + , - . : ; [\] ^ _ { | } ~

SAVE CHANGES DISCARD CHANGES

Posteriormente el smart rule tipo asset es configurado a un smart rule tipo account. Para ello en el smart rule tipo account se define los criterios de selección en donde se especifica el usuario manager de PAM (usrpamxxxx) que usará ese grupo de servidores. La acción que realiza este smart rule account es justamente asociar este usuario manager hacia el smart rule tipo asset en donde está definido nuestros servidores.

Figura 24 – Asociación de usuario manager con smart rule tipo account.

BeyondInsight Configuration

> General > Smart Rules

> [Redacted] Win

Selection Criteria

Include Items that match ALL of the following

Managed Account Fields

Account Name

equals (=)

usrpamXXX

Platforms

Active Directory

Managed Account Fields

Figura 25 – Acciones a realizar del smart rule tipo account.

Actions

Link domain accounts to Managed Systems

Asset or Managed System Smart Group [Redacted] - (Asset group)

Como último paso, se asocia el smart rule de tipo account al grupo de red que brinda el acceso a PAM (PAMM_AreaAsignada_PROD). Dentro de la asociación se puede indicar una política de acceso para aquellos que vayan a tener este grupo de red asociado.

Figura 26 – Asociación del grupo de red a smart rule tipo account.

BeyondInsight Configuration

> User Management > Group: credits.bcp.com.pammm_AreaAsignada_PROD

GROUP: C [Redacted] PAMM [Redacted] PROD

Has 5,6003 Active (last synced on Dec 02, 2022, 11:57 AM)

Group Details

Details & Attributes

Features

Smart Groups (81)

Users (0)

Smart Groups Permissions

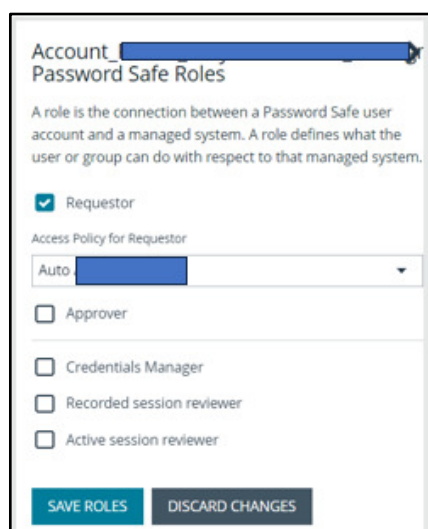
Show: Enabled Smart Groups

Filter by:

81 Items (0 selected)

Smart Group Name	Type	Organization	Permission	Safe Rules
Account, [Redacted]	PROD_win	Managed Account	Global	Read only

Figura 27 – Asociación de política de acceso (Access policies) a smart rule tipo account.



The screenshot shows a configuration window titled "Account [redacted] Password Safe Roles". Below the title is a descriptive text: "A role is the connection between a Password Safe user account and a managed system. A role defines what the user or group can do with respect to that managed system." The window contains several options: "Requestor" is checked, and "Access Policy for Requestor" is set to "Auto" in a dropdown menu. Below these are four unchecked checkboxes: "Approver", "Credentials Manager", "Recorded session reviewer", and "Active session reviewer". At the bottom are two buttons: "SAVE ROLES" and "DISCARD CHANGES".

En el sistema PAM se manejan Accesos Policies o políticas de acceso, las cuales son reglas de accesos, por ejemplo, dentro de esta opción se pueden definir lo siguientes:

- Rango de horario en el cual se puede solicitar el acceso sobre los servidores donde aplica esta política.
- Ver la credencial que tiene el usuario manager (para casi todos los casos esta opción se tiene deshabilitada).
- Habilitar las conexiones por RDP, SSH o aplicaciones. (Ej. WinSCP)
- Habilitar la grabación de sesiones.
- Habilitar el registro de pulsaciones de tecla (Keystroke Logging).
- Asociar un tipo de Connection profile.

Figura 28 – Access Policies en PAM.

The image displays four panels of the PAM Access Policies configuration interface, arranged in a 2x2 grid. Each panel is titled 'Edit All Day'.

- Top Left Panel:** Contains a 'DELETE SCHEDULE' button, 'Time Range' (Start Time: 9:00 AM, End Time: 5:00 PM, Total Time: All Day (24hrs)), 'Date Range' (Start Date: August 6, 2018, End Date: disabled), and 'Recurrence' (Repeat: enabled, Every day, Allow multi-day check-outs of accounts: enabled).
- Top Right Panel:** Contains 'Location Restrictions' (disabled), 'Policy Types' (View Password: enabled, RDP: enabled), and 'Approvals' (1 approver, Auto Approve: disabled, Allow API Rotation Override: disabled).
- Bottom Left Panel:** Contains 'SSH: enabled', 'Approvals' (1 approver, Auto Approve: disabled), 'Concurrent' (1 concurrent, Unlimited: disabled), 'Record: enabled', 'Keystroke Logging', 'Force Termination', and 'Connection Profile' (None).
- Bottom Right Panel:** Contains 'Application: enabled', 'Approvals' (1 approver, Auto Approve: disabled), 'Concurrent' (1 concurrent, Unlimited: disabled), 'Record: enabled', 'Keystroke Logging', 'Enhanced Session Auditing', 'Logoff On Disconnect', 'Force Termination', and 'Connection Profile' (None).

Each panel has a 'Manage Connection Profiles...' link at the bottom.

Referente al Connection profile o perfil de conexión, son un conjunto de reglas aplicables a la conexión realizada. Dentro de ellas podemos aplicar reglas relacionadas a un servidor en específico ya sea por hostname o ip, como a palabras claves o “Keyword” sobre las cuales podemos definir acciones en específico como bloqueos, termino de la sesión, entre otros. Para la implementación dentro de la organización se configuraron Connection profiles en donde se definieron una serie de “keywords” las cuales contenían el valor de comandos que no estaban permitidos de acuerdo con cada equipo, para lo cual la acción a realizar era el bloqueo de estos comandos, no permitiendo su ejecución, pero sin terminar la sesión. El Connection profile también nos permite reportar estas acciones mediante un email de notificación hacia el correo que nosotros configuremos, para este proyecto se usó un email relacionado al equipo de CSIRT los cuales realizaban las validaciones e investigaciones relacionadas a incidentes.

Figura 29 – Configuración Connection profile.

Email Notification Settings (1)

Optional. Recipients may receive a large number of email notifications. Selective use is strongly advised.

[Add A New Item To This List](#)

SAVE CHANGES **DISCARD CHANGES**

Match Conditions
This connection profile will action the match conditions you set below.

[Create Match Condition](#)

12 items

Match ▲	Value	Session Control	Alert	
Keyword	ssh	Block	Yes	
Keyword	scp	Block	Yes	
Keyword	sftp	Block	Yes	
Keyword	telnet	Block	Yes	

Sexta etapa: Capacitación y marcha blanca de uso

En esta sexta etapa, al ya tener configurados los servidores dentro del sistema PAM y debidamente agrupados para cada equipo que haría uso de ellos, lo que quedaba pendiente era el poder realizar la debida capacitación a cada equipo para poder explicar el funcionamiento que tendría el sistema para lo cual se explicó como debían hacer uso del sistema para poder ingresar a los diferentes servidores.

Como primer punto se les brindó la URL mediante la cual ingresaban directamente al Login del sistema PAM, en el cual debían ingresar su id de empleado asociado a su cuenta de Active Directory junto con su credencial.

Figura 30 – Login sistema PAM

Al momento de ingresar al sistema se mostrará la siguiente pantalla con el título “Password Safe” en donde el usuario podrá ver los servidores a los cuales tiene acceso. En este punto cabe recordar que el grupo de servidores los cuales podrá visualizar lo gana mediante un grupo de red en Active Directory el cual ya fue asignado previamente ya que es un requisito para poder interactuar con el sistema.

En la siguiente imagen presentada se muestran varias pestañas las cuales detallaremos:

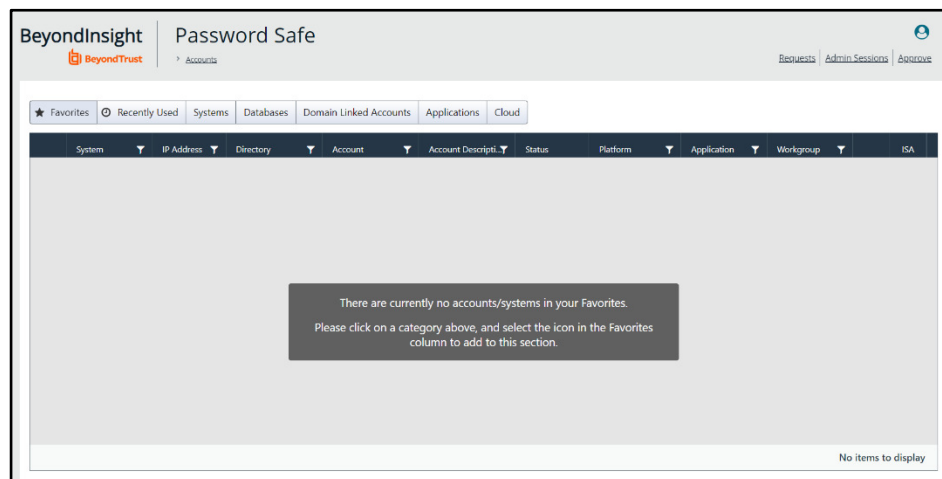
- Favorites. En donde se mostrará la lista de servidores que el usuario haya marcado como favoritos.
- Recently Used. En donde se muestra el listado de servidores a los cuales el usuario ha ingresado recientemente.
- Systems. En este punto se muestra los servidores de sistema operativo AIX y Linux para que el usuario pueda ingresar por la herramienta Putty vía conexión SSH.
- Databases. Esta pestaña no será usada ya que es para mostrar las bases de datos que se encuentran integradas en el sistema PAM, en este punto las bases de datos no formaban parte del alcance del proyecto.
- Domain Linked Account. En este punto se muestra el listado de servidores con sistema operativo Windows Server para poner hacer conexión vía RDP.

- Applications. En este punto se muestra los servidores a los cuales se pueden conectar mediante aplicaciones que se encuentran instalados en los servidores terminales. Para el presente proyecto solo se contó con el aplicativo WINSCP para el acceso a servidores Linux y AIX.
- Cloud. Esta pestaña tampoco será usada ya que en ella se puede adaptar sistemas y servidores que se encuentran en nube.

A su vez también se muestra un cuadro con diferentes columnas detalladas de la siguiente manera:

- System. Es el nombre o hostname del servidor.
- IP Address. Dirección IP del servidor.
- Directory. Si está asociado a un directorio, en el caso de los servidores Windows se muestra el nombre del dominio al cual están integrados en Active Directory.
- Account. Se muestra el usuario manager que se está usando (usrpamxxxx).
- Account Description. Se muestra la descripción asociada al usuario manager.
- Platform. Se muestra la plataforma o sistema operativo del servidor.
- Application. Se detalla la aplicación que se usará para conectarse al servidor, en este caso muestra información solo en la pestaña “Applications”.
- Workgroup. Se muestra el detalle del workgroup asociado al servidor. En este proyecto no es usado.

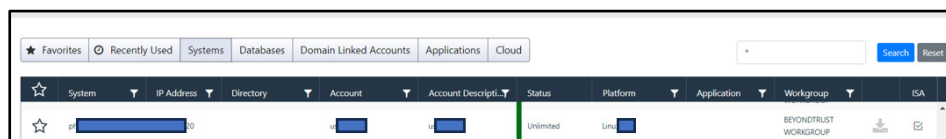
Figura 31 – Ingreso a sistema PAM y pestañas



Para el caso de servidores AIX y Linux si queremos acceder a ellos nos dirigimos a la pestaña “Systems”, aquí podemos buscar un servidor ingresando el nombre sino simplemente se desplegará toda la lista de servidores a los cuales se tiene el acceso. Luego de ello damos clic sobre el servidor al que se requiere ingresar.

Como dato adicional, al costado del nombre del servidor aparecerá una estrella a la cual podemos darle clic para poder marcar el servidor como favorito.

Figura 32 – Búsqueda de un servidor Linux o AIX opción Systems.



Luego de ello se mostrará información referente al acceso al servidor como el nombre del usuario manager que se está usando y el nombre del servidor. Así mismo, nos aparecerá un corto formulario el cuál se puede completar de manera opcional. En esta parte se debe seleccionar la opción “Open SSH Session”.

También habrá una opción “Retrieve Password” la cual te permitirá ver el password actual del usuario manager, esta opción sólo está habilitada para los administradores de la plataforma más no para los usuarios de otros equipos.

Figura 33 – Open SSH Session.

A screenshot of the 'BeyondInsight Password Safe' dialog box. The title bar shows 'BeyondInsight' and 'Password Safe'. Below the title bar, there is a 'Requests' link. The main content area displays the account information: 'Account: usr[redacted] on p[redacted]'. Below this is a 'Reason: (Optional)' text box. Then, there is a 'Ticket System: (None)' dropdown menu. Below that is a 'Ticket Number: (Optional)' text box. At the bottom, there are three buttons: 'Retrieve Password' (with a key icon), 'Open SSH Session' (with a power icon), and 'Cancel'.

Luego de ello se mostrará otra ventana en donde mostrará 2 datos:

- Command. Es un comando sobre el cual se puede copiar y usarlo para conectarse al servidor usando otra aplicación que permita conexión ssh como Gitbash.
- Username/IP. Es una cadena tipo string cifrada que contiene la información de usuario y la ip del servidor al que se requiere acceder.

En este punto aparecerá también el botón Start SSH Session, al darle clic el sistema abrirá el aplicativo Putty (que debe estar instalado previamente en el equipo del usuario) con la sesión iniciada del usuario manager. En esta parte ya se ingresó al servidor y ya se están aplicando las diferentes políticas de control de acceso por el sistema PAM.

Figura 34 – Start SSH Session.

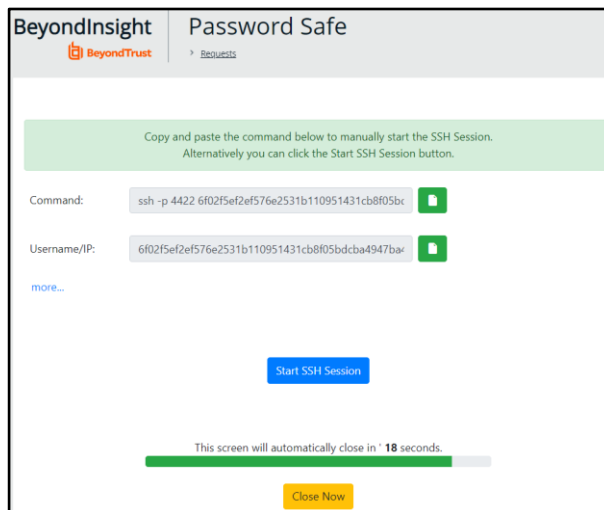
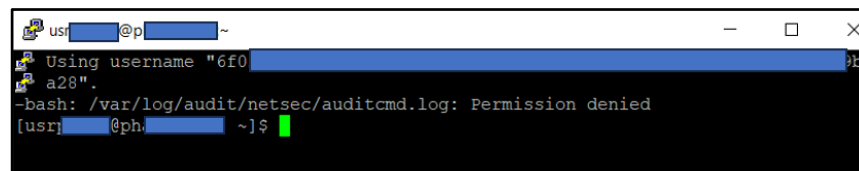
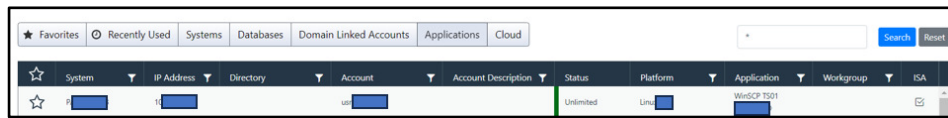


Figura 35 – Sesión iniciada en el servidor seleccionado.



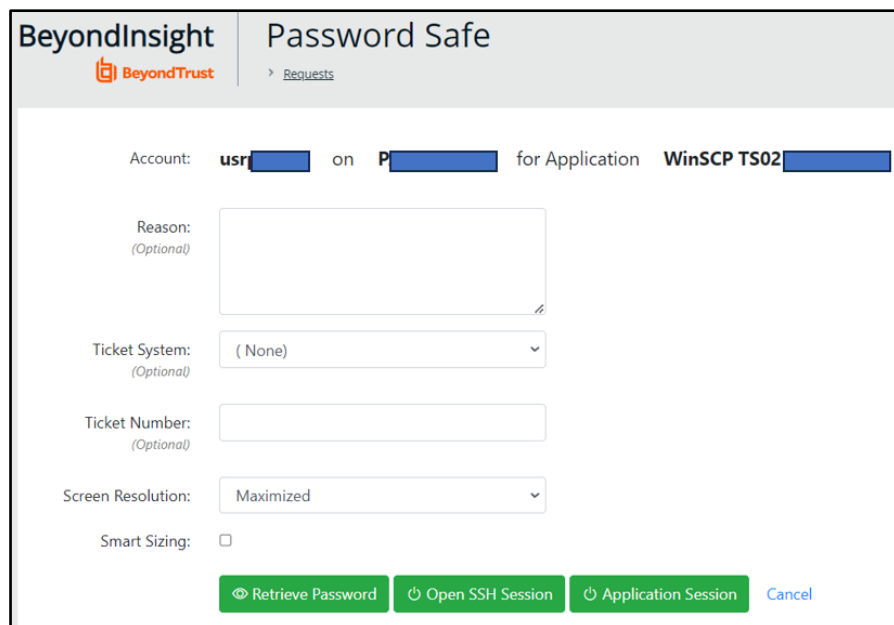
Para el caso de servidores AIX y Linux también tenemos la opción de abrir el acceso al servidor usando la aplicación WINSOCP mayormente usado para poder copiar y pegar archivos al servidor. Para este caso los usuarios debían seleccionar la pestaña “Applications” y seleccionar el servidor al que requieren ingresar.

Figura 36 – Búsqueda de un servidor Linux o AIX opción Applications.



Luego de seleccionar el servidor aparecerá una ventana con más información sobre el acceso al servidor. En la parte inferior nos aparecerá un nuevo botón con el nombre “Application Session” el cual seleccionaremos.

Figura 37 – Application Session



Al darle clic en el botón “Application Session” se descargará automáticamente un archivo el cual realizará una conexión RDP hacia los servidores terminal de el cual no mostrará más información ya que se encuentra limitado a que solo proporcione visibilidad al aplicativo WINSCP que se encuentra instalado en el servidor terminal.

Figura 38 – Archivo rdp descargado.

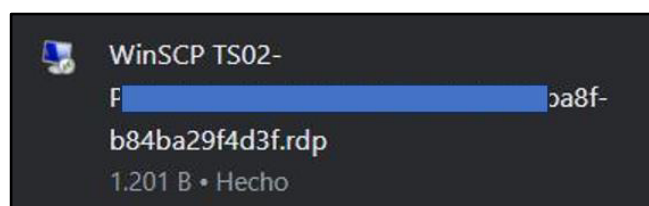
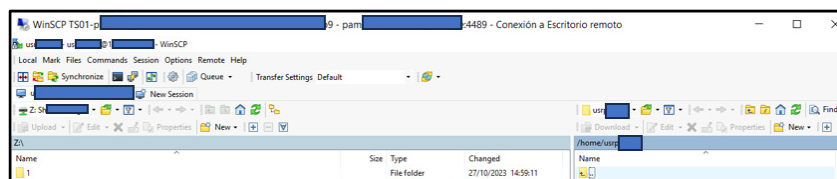


Figura 39 – Acceso a servidor terminal con aplicación WINSCP abierta con sesión iniciada de usuario manager



Para el caso de los servidores Windows Server se indicó a los usuarios que debían seleccionar la opción “Domain Linked Accounts” en el cual les aparecerá el listado de servidores sobre los cuales tienen acceso y a los cuales pueden ingresar. Para poder ingresar vía RDP los usuarios solo deben seleccionar el servidor al cual requieren ingresar y darle clic en el botón de descarga ubicado en la parte derecha del nombre del servidor. Luego de ello se descargará de manera automática un archivo rdp el cual debemos abrir para que se apertura la conexión al servidor con la sesión iniciada del usuario manager.

Figura 40 – Búsqueda de servidores Windows Server en la pestaña Domain Linked Accounts.

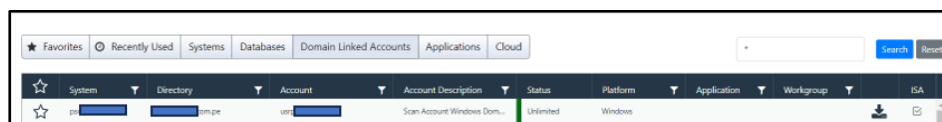


Figura 41 – Archivo rdp descargado.

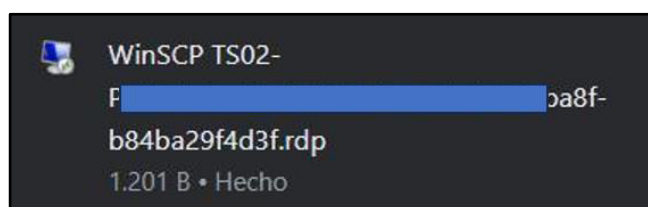


Figura 42 – Sesión iniciada de usuario manager en servidor Windows Server



Una vez capacitados que se brindó capacitaciones a los equipos que usarían el nuevo sistema PAM con los pasos a seguir para que puedan ingresar a los diferentes servidores se procedió a informar a todos los equipos mediante correo electrónico que se estaría iniciando un proceso de marcha blanca sobre el cual se iniciaría el despliegue formal de uso del sistema PAM. Cabe resaltar que en esta marcha blanca como ingeniero responsable del sistema PAM quedé a cargo de absolver cualquier duda que pudiera surgir por parte de los usuarios.

3.4. Evaluación

3.3.1. Evaluación económica / Evaluación costo-beneficio

En este caso la propuesta fue impulsada por un tema de cumplimiento ya que la División de TI, Operaciones y Data contaba con un riesgo asignado que asumía por la deficiencia en la gestión de accesos hacia recursos críticos de la organización, siendo los más importantes los servidores en entorno productivo ya que ahí se aloja información relevante para la organización.

El riesgo fue evaluado de manera cuantitativa usando la metodología FAIR (por sus siglas en inglés Factor Analysis of Information Risk), modelo estándar internacional que sirve para cuantificar riesgos de ciberseguridad. En este caso la entidad bancaria adoptó esta metodología para la medición de riesgos de ciberseguridad.

El área de Riesgos Operativos fue la encargada de la evaluación y registro de este riesgo la cual se ingresó con la siguiente descripción:

“Posibilidad de pérdida de confidencialidad debido a que un insider malicioso privilegiado afecte la confidencialidad de la organización al hacer un uso indebido de la información que se tiene alojada en los servidores productivos al contar con permisos elevados sobre estos y no tener controles asociados.”

Al ser una metodología cuantitativa se tuvo el detalle de como afectaría la materialización de este riesgo de manera económica a la organización bajo el siguiente detalle:

Figura 43 – Detalle riesgo asociado (FAIR).



Del riesgo registrado podemos detallar los siguientes datos relevantes:

- La organización se expone a una pérdida promedio de 1.8 millones de dólares anuales por este riesgo asociado.
- La probabilidad que se materialice el riesgo es cada 1.67 años teniendo una pérdida promedio por evento de 3.1 millones de dólares.
- Las pérdidas primarias de respuesta se asocian a los equipos de la organización que se involucran para dar tratamiento al incidente y las pérdidas primarias por reemplazo se asocian al costo de reemplazo de activo y/o personal que se tiene que realizar para subsanar el incidente, en este caso la suma de ambas pérdidas era en promedio 40.3 mil dólares.
- Las pérdidas secundarias se asociaban a daños reputacionales, multas y sanciones por parte de un regulador externo sumado al costo que involucra sumar a los equipos de la organización que dan respuesta al regulador externo de materializarse el riesgo. Siendo en este caso, a un 97.16% de probabilidad, una pérdida de 3.1 millones de dólares.

Figura 44 – Pérdidas Primarias asociadas al riesgo.

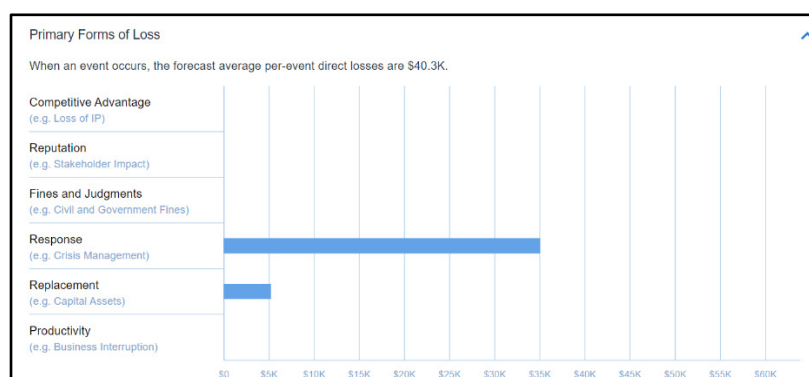
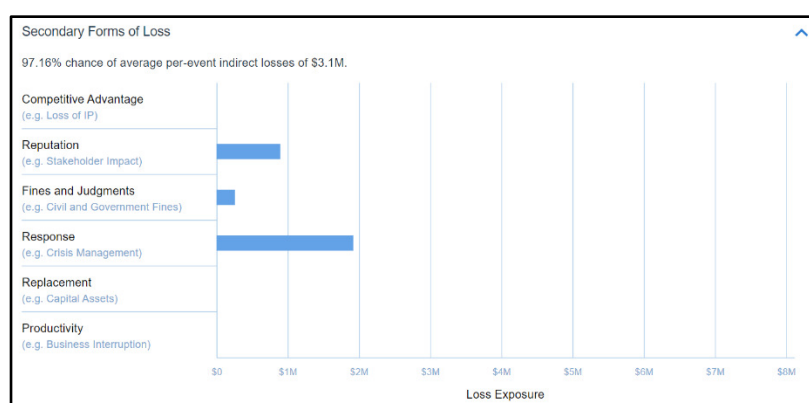


Figura 45 - Pérdidas Secundarias asociadas al riesgo.



Teniendo en cuenta los datos presentados sobre el riesgo asociado es que se llevó a cabo la implementación del sistema PAM dentro de la organización para mitigar este riesgo.

En este caso el coste que tuvo que asumir la organización por el proyecto llevado a cabo para la implementación del sistema PAM se detalla dentro de las siguientes tablas:

Tabla 5 – Costo proyecto implementación PAM.

Nro.	Rubro	Proveedor	Monto (\$) con IGV	2021	2022	2023
1	Licencias adicionales por implementación	Securesoft	\$20,443.50	\$20,443.50		
2	Servicio de horas implementación de Securesoft	Securesoft	\$81,995.84	\$59,344.56	\$22,651.28	
3	Ambiente de pruebas Project	Securesoft / IBM	\$30,444.29	\$30,444.29		
4	Manager Tercerizado	Accenture	\$158,025.60	\$64,380.80	\$93,644.80	
			\$290,909.23	\$174,613.15	\$116,296.08	

Tabla 6 – Costo de soporte y mantenimiento de PAM.

Nro.	Rubro	Proveedor	Monto (\$) con IGV	2021	2022	2023
1	Mantenimiento y soporte de licencias	Securesoft	\$25,548.99	\$6,051.73	\$9,256.16	\$9,256.16
2	Soporte al ambiente de pruebas	Securesoft	\$21,938.10	\$7,312.70	\$7,312.70	\$7,312.70
			\$47,487.09	\$13,364.43	\$16,568.86	\$16,568.86

El costo total de la implementación de PAM en la organización fue de \$338,396.32 por un periodo de 3 años, es decir, por cada año el banco asumía un costo de \$112,798.77.

Resumiendo la parte de costos, tenemos el monto que asumía la organización por el riesgo del cual era responsable y el costo de la implementación de PAM dentro de la entidad bancaria, llevados al siguiente cuadro resumen.

Tabla 7 – Cuadro resumen de costos.

Descripción costos	Monto	Tiempo	Anualizado
Riesgo asumido por la División de TI	\$1,800,000.00	Anual	\$1,800,000.00
Total de implementación y soporte PAM	\$338,396.32	3 años	\$112,798.77
			\$1,687,201.23

Concluyendo así que como organización se presentaba un balance positivo anual de \$ 1,687,201.23.

CAPÍTULO IV – REFLEXIÓN CRÍTICA DE LA EXPERIENCIA

Dentro de las principales reflexiones que se lograron obtener después de la implementación del sistema Privileged Access Management dentro de la entidad bancaria puedo deducir lo siguiente:

Rechazo al cambio. Muchas áreas ya estaban acostumbradas a la manera anterior de trabajo que era contar con el acceso directo a los servidores sin un sistema de por medio, por lo cual mostraron cierto rechazo al cambio al momento de tener que usar el nuevo sistema PAM. En este caso se tuvieron diferentes sesiones de concientización y capacitación para hacer más amable el cambio. Así también, se establecieron diferentes flujos de apoyo ante cualquier duda y/o incidente que pueda surgir con el sistema durante su despliegue. Tengamos en cuenta que como en todo sistema pueden surgir diferentes incidentes o contratiempos. PAM no fue la excepción, por lo cual surgieron algunos inconvenientes durante la marcha blanca, pero todo fue controlado y solucionado a tiempo.

Dependencia de otras áreas. Dentro de una entidad grande como en la que se implementó el sistema PAM, muchas veces realizar este tipo de implementaciones trae dependencias con otras áreas lo cual conlleva en un mayor tiempo en las coordinaciones. Este proyecto no fue la excepción ya que en muchos casos se presentaron dependencias o retrasos con las atenciones que debían realizar otras áreas para lograr la implementación del proyecto, principalmente en la parte de la implementación de la infraestructura sobre la cual se desplegaría el sistema PAM. Para ello se tuvo que priorizar la atención de varias tareas por medio de las jefaturas de las áreas involucradas, gracias a ello no se dilató el proyecto más de lo previsto, en este punto el haber adoptado una metodología ágil en el que es aceptable los cambios durante la marcha ayudó bastante al desarrollo del proyecto.

Obsolescencia tecnológica y limitantes técnicas. No se logró adaptar todos los servidores productivos de la organización a PAM, esto debido a que la organización contaba con servidores cuyos sistemas operativos se encontraban obsoletos y fuera de soporte como es el caso de los sistemas operativos Windows Server 2018. Para estos casos se relevó la información correspondiente en un reporte que posteriormente fue entregada a las jefaturas owners de dichos servidores para que realicen la actualización de sus sistemas operativos a una versión más reciente. Esto iba a conllevar más tiempo

del ya programado en las etapas del despliegue del proyecto ya que se debía analizar el impacto de realizar el upgrade del sistema operativo para validar que no afecte ninguna aplicación o recurso interno, por lo cual se tuvo que descartar en su momento la integración de dichos servidores en PAM.

Flujos desactualizados. Durante la implementación del sistema PAM se tuvo que revisar varios flujos con los cuales se interactuaba de manera directa e indirecta, en este punto es que se encontraron flujos que se encontraron desactualizados a la fecha, por lo cual se tuvo contratiempos durante la implementación del proyecto. Lo que se realizó para poder avanzar respecto a estas adversidades es voltear con las áreas owners de estos flujos y procesos para que actualizaran la documentación pertinente y así no tener contratiempos posteriores, de igual manera se indicó que estos flujos deben mantenerse en constante revisión y actualización de acorde a la situación de la organización. Para esta parte se generaron diferentes reuniones de las cuales posteriormente se documentaron las actas de lo acordado en ellas para así tener una constatación de que se realizó la revisión y de quienes estaban asumiendo la responsabilidad de cada punto expuesto en las diferentes reuniones.

Falta de información o información incompleta de servidores. Otro de los puntos limitantes era que no se contaba con información actualizada de los servidores, si bien la organización tiene un inventario de activos en donde se puede visualizar la información de los servidores, esta no se encontraba actualizada y presentaba algunos inconvenientes, por lo cual se tuvo que conversar con el área encargada de este inventario para que pueda realizar la actualización correspondiente. Esto fue muy importante ya que luego de la actualización logramos tener una mejor visibilidad de los servidores y sus principales características como el tipo de sistema operativo ya que con ello clasificamos mejor los servidores que se podían integrar con PAM y cuáles no.

CAPÍTULO V – CONCLUSIONES Y REFLEXIONES

4.1. Conclusiones

La implementación llevada a cabo del sistema Privileged Access Management puede ser considerada crítica para toda organización que requiere asegurar el uso de sus diferentes recursos y datos que manejen. Dentro de la implementación realizada dentro de la entidad bancaria podemos concluir principalmente lo siguiente:

- *Mejor manejo en la gestión de accesos.* La implementación de PAM permitió que mejorara el manejo de la gestión de accesos al momento de habilitar, modificar o retirar un acceso a un usuario sobre los servidores productivos de la organización al tener un sistema que permitió centralizar todos los accesos.

Dentro de las conclusiones secundarias podemos detallar:

- *Mejora de la productividad.* En este caso hemos visto como los tiempos de atención relacionados directamente a la operativa del área de Gestión de accesos disminuyeron significativamente con la implementación del sistema PAM pasando a brindar accesos a todo el parque de servidores para un solo usuario en un tiempo promedio de 2 minutos ya que solo se le debe asociar un grupo de red a nivel de Active Directory (anteriormente, el acceso era brindado servidor por servidor).

En el siguiente gráfico se resume los tiempos de atención que manejaba el equipo de Gestión de accesos para brindar el acceso a todo el parque de servidores para una sola persona sin la implementación del sistema PAM y con la implementación del sistema, viendo así la mejora en la productividad.

Figura 46 – Resumen de tiempos de atención para acceso a todo el parque de servidores a una persona teniendo en cuenta la implementación de PAM.

SIN PAM		CON PAM	
Atención acceso a servidor	Tiempo	Atención acceso a servidor	Tiempo
Nuevo acceso	5 horas	Nuevo acceso	2 minutos
Modificación	5 horas	Modificación	2 minutos
Retiro acceso	8 horas	Retiro acceso	2 minutos

- *Disminución de incidentes de gestión de accesos.* Se disminuyeron los incidentes presentados por error o falta de accesos. En este caso al centralizar todos los accesos por medio de un grupo de red y ya no por cada servidor, era más fácil que el área de gestión de accesos pueda brindar, modificar o retirar los accesos y evitar incidentes relacionados a estos casos, lo que trajo una mejor experiencia al usuario.

En el siguiente gráfico podemos visualizar un reporte con los números de incidentes por temas de accesos a servidores de cuando no se tenía PAM y de cuando ya se implementó el sistema para una mejor visualización.

Figura 47 – Reporte incidentes de acceso a servidores cuando no se tenía implementado PAM.

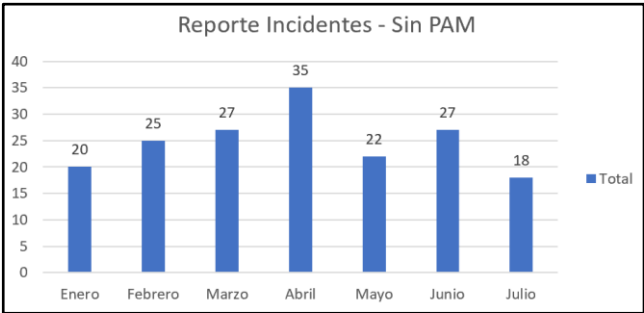
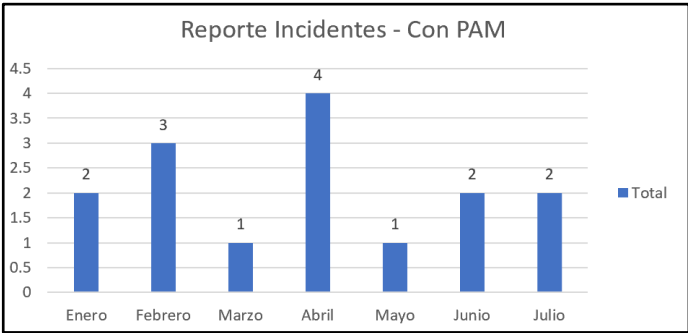


Figura 48 – Reporte incidentes de acceso a servidores con PAM implementado.



- *Aumento de la Seguridad.* La implementación del sistema PAM permitió restringir el acceso los usuarios que tenían cuentas privilegiadas dentro de los servidores productivos de la organización. Teniendo ahora un acceso que puede ser monitoreado y debidamente controlado en base a políticas implementadas en PAM; así también, con el sistema PAM se tiene grabaciones de las sesiones en los servidores productivos en el cual quedan registrados todas las actividades realizadas en ellos (ver anexo 1), lo que contribuye a poder prevenir y detectar posibles amenazas.
- *Mejor gestión de contraseñas.* Mediante PAM también se logró tener un mejor manejo de credenciales dentro de los servidores productivos de la organización ya que se logró aplicar políticas de seguridad en las mismas, las cuales incluyen una rotación periódica de credenciales lo cual antes de la implementación no se tenía. Este punto queda evidenciado en la cuarta de etapa del proceso de implementación (Figura 18).
- *Inicio de sesión único.* Mediante PAM se logró que el usuario cuenta con un acceso centralizado hacia los servidores. En este caso el usuario solo con ingresar al sistema PAM puede visualizar los servidores a los cuales requiere el acceso sin necesidad de volver a detallar un usuario y credencial para el acceso.
- *Cumplimiento normativo.* La implementación de PAM logró que a la organización cumpla con los diferentes requisitos normativos, así como el cumplimiento de acuerdo con los lineamientos internos, lo cual conllevó a la reducción de observaciones de auditorías.

4.2. Recomendaciones

- *Ampliar alcance.* Se puede ampliar el alcance explorando la inclusión de servidores productivos de otros dominios. Para el presente caso de uso dentro de la entidad bancaria se manejan varios dominios; así que el poder incluir los servidores de estos dominios es algo factible a nivel técnico.
- *Integrar otros activos.* PAM es una herramienta versátil que te da la posibilidad de integrar otros activos como por ejemplo bases de datos, los cuales también son considerados recursos críticos. Por lo cual se recomienda validar la integración de las bases de datos de la organización.

- *Incluir flujo de autorización PAM.* Dentro del sistema PAM hay una opción que te permite añadir una capa de control adicional a los accesos solicitados a los servidores. Se trata de un flujo de autorización en el cual el solicitante no ingresa directamente al servidor sino que previo a ello lanza una solicitud hacia un aprobador que previamente debe estar definido para su grupo, el cual debe ingresar a PAM solo para brindar su conformidad sobre el acceso solicitado (inclusive puede limitar el tiempo de acceso solicitado) o rechazar la solicitud.
- *Mantener actualizado el sistema y la infraestructura.* En este caso, la marca BeyondTrust sigue sacando actualizaciones del sistema, por lo cual se recomienda mantener el sistema con las últimas actualizaciones ya que estas pueden incluir correcciones de seguridad y nuevas funcionalidades. Así también, mantener actualizada la infraestructura sobre la cual se implementó el sistema, manteniendo actualizados los sistemas operativos y aplicaciones usadas. (para más detalle ver Anexo 2)
- *Validar la correcta ejecución de las copias de seguridad.* Las copias de seguridad o backups permiten tener un respaldo frente a fallos críticos del sistema o un incidente de seguridad. Es importante realizar las copias de seguridad y resguardarlas en un lugar seguro y que no sea en la propia infraestructura del sistema. (para más detalle ver Anexo 2)
- *Mantener actualizado la información de servidores dentro de PAM.* Se recomienda revisar periódicamente los reportes generados a través de PAM para validar la información referente a servidores como hostname o IP. Se deben eliminar dentro de la consola de PAM los servidores que se den de baja dentro de la organización. (ver detalle de Anexo 3)
- *Concientización a los usuarios.* Es importante el poder seguir concientizando a los usuarios sobre el uso de sistemas como PAM, recalcando su importancia frente al correcto uso de las cuentas privilegiadas e identidades en general.

FUENTES DE INFORMACIÓN

CyberArk. (2023). Gestión del Acceso con Privilegios (PAM). Obtenido de CyberArk: <https://www.cyberark.com/es/what-is/privileged-access-management/>

BeyondTrust. (2023). Privileged Access Management (PAM). Obtenido de <https://www.beyondtrust.com/resources/glossary/privileged-access-management-pam>

BCP. (2023). Nosotros. Obtenido de <https://www.viabcp.com/nosotros>

Ekran. (2022). 5 Steps for Building an Agile Identity and Access Management Strategy. Obtenido de <https://www.ekransystem.com/en/blog/agile-iam-strategy>

Security Intelligence. (2023). How to Use Scrum to Make an Identity Management Project More Agile. Obtenido de <https://securityintelligence.com/how-to-use-scrum-to-make-an-identity-management-project-more-agile/>

Gartner. (2019). Gartner. Take an Agile Approach to IAM Deployment. Obtenido de <https://www.gartner.com/en/documents/3942119>

Gartner. (2023). Privileged Access Management. Obtenido de <https://www.gartner.com/reviews/market/privileged-access-management>

Microsoft. (2023). What is privileged access management (PAM)?. Obtenido de <https://www.microsoft.com/en-us/security/business/security-101/what-is-privileged-access-management-pam>

Kuokkanen, A. (2020). Newcomer's introduction to Privileged Access Management. Obtenido de https://www.theseus.fi/bitstream/handle/10024/348503/Opinnaytetyo_Kuokkanen_Antti.pdf?sequence=2

Waltermire, K. (2018). Privileged Account Management for the Financial Services Sector. Obtenido de <https://www.nccoe.nist.gov/sites/default/files/legacy-files/fs-pam-nist-sp1800-18b-draft.pdf>

Amazon. (2023). ¿En qué consiste Scrum?. Obtenido de <https://aws.amazon.com/es/what-is/scrum/>

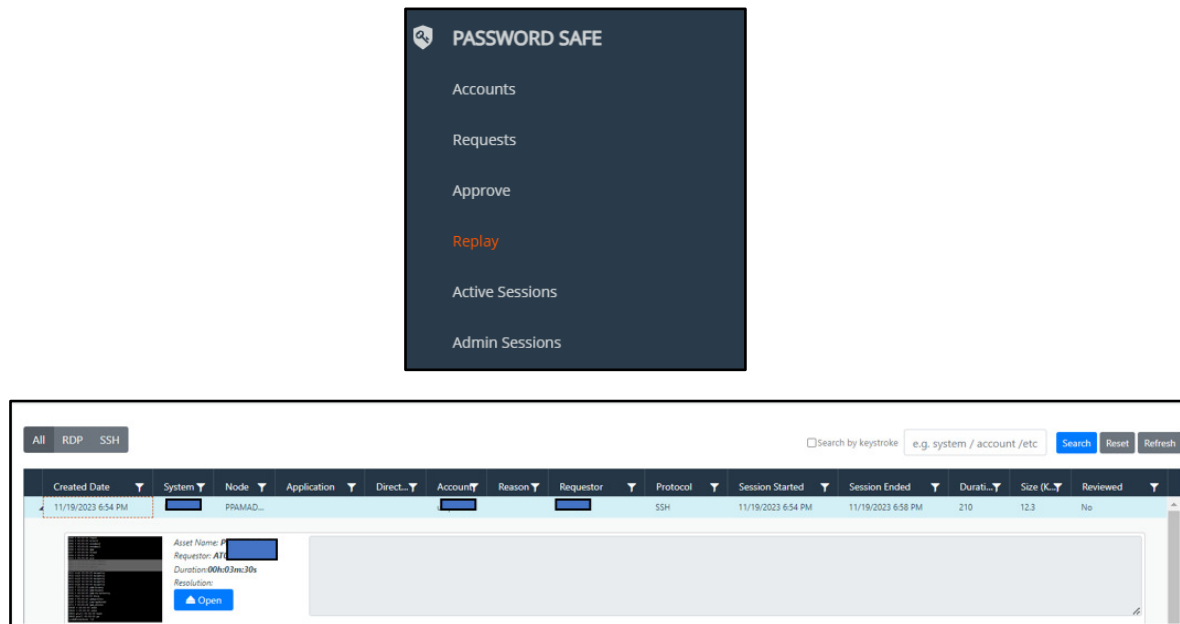
IONOS. (2023). Active Directory de Microsoft. Obtenido de <https://www.ionos.es/digitalguide/servidores/know-how/que-es-el-active-directory/>

Microsoft. (2023). Introducción a Windows Server. Obtenido de <https://learn.microsoft.com/es-es/windows-server/get-started/get-started-with-windows-server>

Red Hat. (2023). Linux. Obtenido de <https://www.redhat.com/es/topics/linux>

ANEXOS

Anexo 1



Nota: Opción dentro de PAM para ver las grabaciones generadas por cada sesión iniciada dentro de un servidor.

Anexo 2

Mejores prácticas en equipos y configuraciones brindadas por el proveedor:

- A pesar de que el software de BeyondTrust se encuentra instalado en un Windows Server, la recomendación general es no agregar estos equipos a un dominio. Esto debido a que se presentan casos en los que el despliegue de una política de grupo interfiere con el funcionamiento de la propia plataforma. Tener en cuenta que el software de BeyondTrust aplica un hardening propio al SO host. De ser necesario ingresar los equipos a un dominio, favor de solicitar apoyo para el proceso.
- Evitar la instalación de software de terceros (ej. Antivirus, EDR, etc.). De igual manera, se presentan casos en los que software instalados en los UVM interfieren o impiden ciertas funcionalidades de la plataforma e incluso producen indisponibilidad del servicio. Además, esta práctica es prohibida por BeyondTrust y puede incurrir en la garantía del producto. Se cuenta con una excepción para el software Thales usado para integraciones de HSM.
- Implementar el uso de certificados SSL para proteger la comunicación del UVM con los distintos equipos (ej. Endpoint del usuario, balanceador de cargas, etc.).
- Incluir el uso de MFA para el acceso a la plataforma web de BeyondTrust (BeyondInsight). Se recomienda que la aplicación de múltiples factores de autenticación sea sobre todos los usuarios, indistinto del rol que manejen.

- Manejar una jerarquía de usuarios y cuentas privilegiadas basado en roles (RBAC). Se recomienda implementar un sistema de aprobación para cuentas privilegiadas de mayor criticidad y privilegios. Se requiere mapear dichas cuentas y asignar rol de aprobadores a usuarios o grupo de usuarios.
- Integración con un gestor de eventos (SIEM) para tener mayor visibilidad sobre el comportamiento y uso de la herramienta. Así mismo, es posible implementar un sistema de envío de eventos por correo electrónico con la finalidad de un envío de eventos más directo

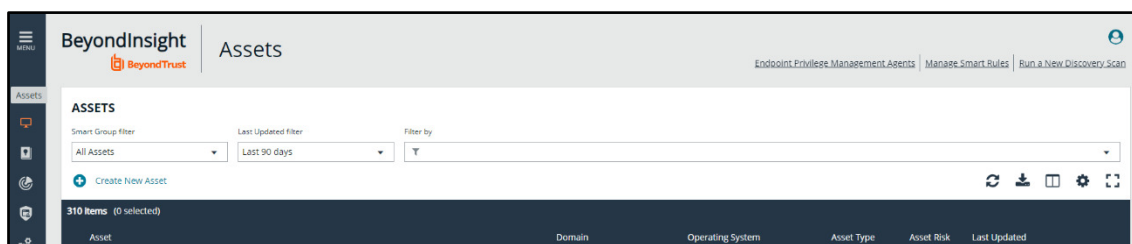
Mejores prácticas en Backups:

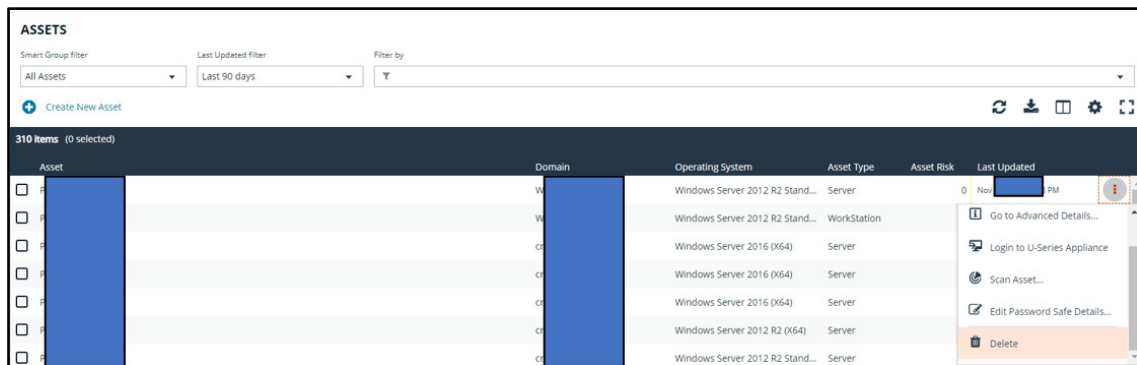
- Se recomienda configurar tareas programadas para generar backups de manera periódica, principalmente sobre la configuración del equipo.
- Destinar los backups a un repositorio externo. En el caso que el equipo se vea comprometido y no se pueda acceder, es imposible extraer la información en caso esta sea almacenada en el mismo servidor por lo que se recomienda un equipo externo.
- Verificar, de manera periódica, la ejecución de la tarea programada para la generación de backups. Desde la plataforma web se puede verificar el estado de estas tareas y sus resultados.
- Generar y almacenar una copia de las llaves de encriptación de cada uno de los UVM. En caso de desastre esta información es solicitada por el equipo de apoyo de BeyondTrust por lo que se recomienda tener una copia fuera de los UVM.

Mejores prácticas en Upgrades:

- Se recomienda deshabilitar la descarga automática de paquetes de actualización. Estos paquetes pueden ser descargados a demanda.
- Se recomienda deshabilitar la opción de reinicio automático bajo condiciones del equipo. Normalmente utilizado durante el proceso de upgrade, se desactiva para evitar el reinicio inesperado producto de una actualización.
- Planificar la instalación de parches de seguridad de Windows, aprobados por BeyondTrust (SUPI). Estos parches son liberados de manera mensual por lo que un plan para su instalación progresiva es recomendable.

Anexo 3



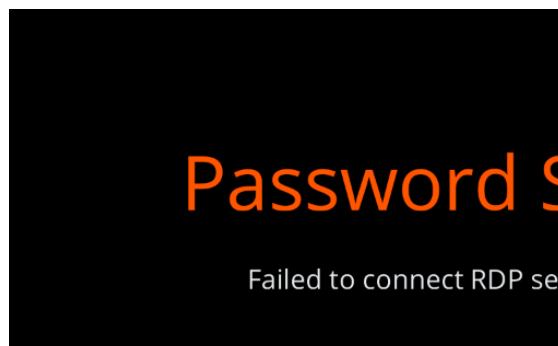


Nota: Se muestra las figuras para realizar la eliminación de un servidor dentro del sistema PAM

Anexo 4

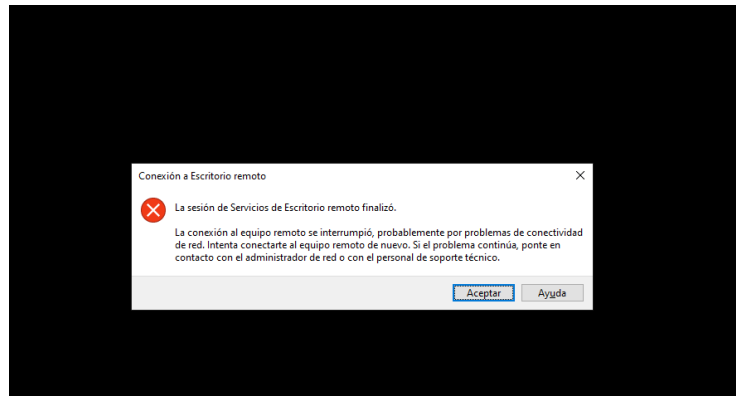
Bitácora de errores redactada

1. Aparece un error al momento de conectarse al servidor por medio de PAM.



Descartes:

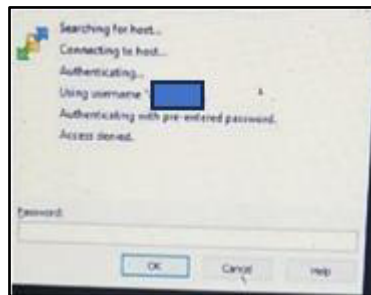
- Validar que el servidor se encuentre operativo y en red interna de la organización. Se puede hacer un ping.
 - Validar que el servidor sólo cuenta con una ip asignada a nivel de DNS.
 - Validar que el usuario funcional y el usuario manager se encuentren configurados correctamente. De ser el caso realizar la rotación de credenciales del usuario manager.
 - Validar a nivel de red si existe conectividad desde los appliance de PAM hacia el servidor al que se quiere acceder.
 - Validar que no haya bloqueos a nivel del FFW de la organización.
2. Se cierra la sesión al cabo de cierto periodo de tiempo.



Descartes:

- En este caso se debe validar la configuración del servidor al que se está intentando acceder. Se debe validar la política asignada por periodo de inactividad.

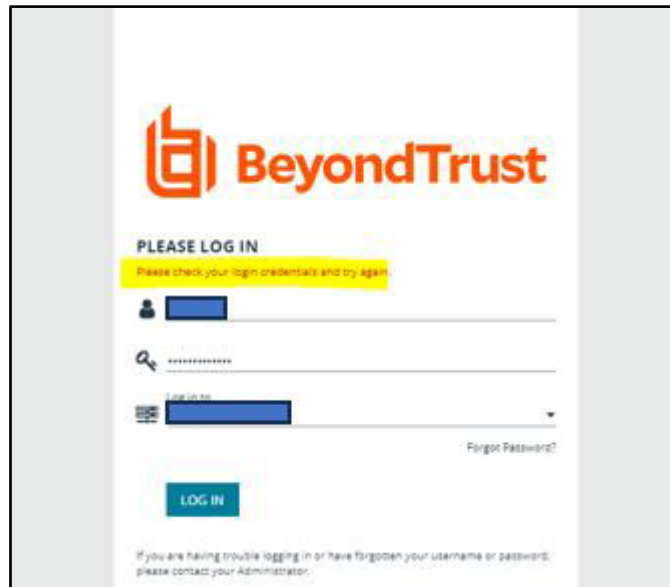
3. No ingresa sesión en servidores LINUX solicitando ingresar la credencial.



Descartes

- Para este caso se debe validar que el usuario manager no se encuentre bloqueado dentro del servidor.
- Realizar el cambio de credencial del usuario manager para volver a validar el ingreso.

4. Colaborador de la entidad no logra iniciar sesión.



Descartes:

- En este caso se debe validar si el colaborador tiene asignado el grupo de red que le brinda el acceso a PAM en el Active Directory.
- Se debe validar que la cuenta del colaborador no se encuentre bloqueada en AD.
- Se debe descartar que su credencial no haya expirado.