FACULTAD DE INGENIERÍA Y ARQUITECTURA

ESCUELA PROFESIONAL DE INGENIERÍA DE COMPUTACIÓN Y SISTEMAS

IMPLEMENTACIÓN DE UN SISTEMA DE GESTIÓN DE IDENTIDADES PRIVILEGIADAS PARA EL CONTROL DE ACCESO EN UNA EMPRESA DE RETAIL

PRESENTADA POR

LUCÍA ASTRID CONTRERAS PÉREZ

ROBERTO ANTONIO VEGA ORTEGA

ASESOR

LUZ SUSSY BAYONA ORÉ

LUIS ESTEBAN PALACIOS QUICHIZ

TESIS

PARA OPTAR EL TÍTULO PROFESIONAL DE INGENIERO DE COMPUTACIÓN Y SISTEMAS

LIMA – PERÚ

2019

USMP
UNIVERSIDAD DE SAN MARTIN DE PORRES
FACULTAD DE INGENIERÍA Y ARQUITECTURA

ESCUELA PROFESIONAL DE INGENIERÍA DE COMPUTACIÓN Y SISTEMAS

IMPLEMENTACIÓN DE UN SISTEMA DE GESTIÓN DE IDENTIDADES PRIVILEGIADAS PARA EL CONTROL DE ACCESO EN UNA EMPRESA DE RETAIL

TESIS

PARA OPTAR EL TÍTULO PROFESIONAL DE INGENIERO DE COMPUTACIÓN Y SISTEMAS

PRESENTADO POR

CONTRERAS PÉREZ, LUCÍA ASTRID
VEGA ORTEGA, ROBERTO ANTONIO

ASESORES: Dr. Bayona Oré, Luz Sussy
Mg. Palacios Quichiz, Luis Esteban

LIMA - PERÚ

2019

Dedico esta tesis a mi familia. A mis padres y hermanas, por su apoyo incondicional y ser mi motivación diaria a superarme con sacrificio y esfuerzo.

Lucía Astrid Contreras Pérez

Dedico este trabajo a mis padres por haberme enseñado a tener siempre el espíritu de lucha y nunca decaer frente a las adversidades; a mis hermanos y enamorada por su apoyo incondicional que me permite crecer como persona y profesional.

Roberto Antonio Vega Ortega

En primer lugar, agradezco a Dios, por llenarme de bendiciones y permitir la realización de esta tesis. Quiero agradecer a los asesores del taller de tesis, quienes nos han apoyado con su experiencia en terminar el presente trabajo.

Lucía Astrid Contreras Pérez

Agradezco a Dios por darme la oportunidad de haber culminado este trabajo. Así mismo, un profundo agradecimiento a mis asesores del curso de taller de tesis que me guiaron a cumplir este primer objetivo y finalmente muy agradecido con esta universidad que me abrió las puertas para ser un ingeniero y cumplir con mis metas.

Roberto Antonio Vega Ortega

ÍNDICE

ÍNDICE DE TABLAS

ÍNDICE DE FIGURAS

Página

ÍNDICE DE ANEXOS

RESUMEN

La presente tesis propone reducir los riesgos internos de seguridad informática de una empresa de retail, que carece de medidas de seguridad de información. Se tiene como objetivo la implementación de un Sistema de Gestión de Acceso Privilegiado que permitirá tener una gestión de contraseñas efectiva, con la finalidad de controlar el acceso en los activos de Tecnología de Información (TI), aplicando políticas, permitiendo evitar el *leapfrog*, teniendo control y registro de las actividades de los usuarios, además, tener la trazabilidad de los cambios realizados en los activos de TI y mejorar la operatividad de los usuarios. Durante la gestión del proyecto se acopió información sobre la empresa de retail, como procesos, infraestructura de red, sistemas que utilizan y las credenciales de los usuarios.

Con respecto a la gestión del proyecto, se basó en el método Plan-Do-Check-Act (PDCA), que es sugerida por la norma ISO/IEC 27001:2013, y también se aplicó los controles relacionados con la gestión de credenciales de la norma, con el fin de garantizar la protección de la información de la empresa de retail.

Culminada la implementación de la solución de gestión de accesos privilegiados, se logró minimizar los riesgos de amenazas y vulnerabilidades sobre los activos críticos de TI de la empresa de retail, como son: confidencialidad, disponibilidad e integridad de la información.

Palabras Claves: Seguridad informática y de la información, Gestión de credenciales, Sistema de Gestión de Acceso Privilegiado.

ABSTRACT

This thesis proposes to reduce the internal risks of informatic security of a retail company, which lacks information security measures. The objective is the implementation of a Privileged Access Management System that will allow effective password management, with the purpose of controlling the access in Information Technology (IT) assets, applying policies, allowing to avoid leapfrog, taking control and registration of user activities, also, have the traceability of changes made in IT assets and improve the operation of users. During the management of the project, information about the retail company was collected, such as processes, network infrastructure, systems they use and user's credentials.

With regard to project management, it was based on the Plan-Do-Check-Act (PDCA) method, which is suggested by the ISO / IEC 27001: 2013 standard, and the controls related to the management of credentials of the standard were also applied, in order to guarantee the protection of the information of the retail company.

Once the implementation of the privileged access management solution was completed, the risks of threats and vulnerabilities on the critical IT assets of the retail company were minimized, such as: confidentiality, availability and integrity of the information.

Key Words: Informatic and Information security, Management of credentials, Privileged Access Management System.

INTRODUCCIÓN

Hoy en día las empresas compiten y mejoran su operatividad a través del software. La tecnología juega un rol importante en la estrategia del negocio, implica cambio y extensión continúa en la infraestructura a medida que la empresa avanza en la transformación digital, y ello conlleva que el riesgo sea mayor.

Las empresas gastan millones de dólares en *firewalls*, encriptación y dispositivos de acceso seguro, invirtiendo grandes cantidades de dinero a pesar de que estas no abordan el eslabón más débil de la cadena de seguridad: las personas que utilizan administran y operan sistemas informáticos. Una de las más grandes amenazas de seguridad en el ámbito de seguridad cibernética es el uso indebido de cuentas con permisos elevados, que en la presente tesis se le denominará identidades privilegiadas (Mitnick, 2017). Para mitigar dicho riesgo se sugiere tener un plan de seguridad de acceso a dispositivos.

El sistema CA Privileged Access Management (PAM por sus siglas en inglés) permite a la organización administrar las cuentas privilegiadas con el fin de proteger sus activos críticos, cumplir con las regulaciones de cumplimiento y evitar las infracciones de datos.

Durante el año 2016 a 2017 el riesgo de ser víctima de ataques cibernéticos se incrementó en un 45%, siendo cada vez más comunes y

sofisticados; directamente ligados a la brecha de credenciales privilegiadas (IdentityForce, 2017).

CA Technologies (2017) determina que conocer sus usuarios privilegiados es conocer su riesgo y para minimizar el riesgo se requiere de herramientas de gestión de acceso privilegiado, así como ser capaces de soportar la automatización del proceso de autorización y permitir la escalabilidad mediante el apoyo a ambas operaciones dinámicas.

El tema de falta de seguridad afecta a varias organizaciones, entre ellas se encuentra la empresa de retail en la que se realizará la implementación de la solución CA Privileged Access Manager; la empresa en mención se dedica a venta directa de productos como fragancias, maquillaje, cuidado de rostro, cuidado de cuerpo y bijouterie, actualmente presente en 10 países de América y Europa, que tampoco está exenta a este tipo de problemas.

La presente tesis está compuesta por seis capítulos, donde se define el planteamiento de problema, objetivo y la justificación de la solución propuesta, nos basamos en casos exitosos nacionales e internacionales que tiene relación con la problemática planteada, para la mejor comprensión de la tesis se incluye las secciones de bases teóricas y definición de términos. Previamente a la implementación de la solución propuesta se definieron los materiales y el método a aplicar, incluyendo los entregables. Al finalizar el desarrollo de la implementación de la solución se realizaron pruebas y los resultados obtenidos fueron comparados con los objetivos planteados. Además, se incluye conclusiones, recomendaciones y anexos.

CAPÍTULO I
PLANTEAMIENTO DEL PROBLEMA

1.1 Problemática

1.1.1 Situación problemática.

La situación problemática en el contexto presentado es que sigue incrementándose la cantidad de fraudes y datos perdidos o robados, desde el año 2013 hasta el año 2017 se ha presentado más de 9.7 billones de registros perdidos o robados en Estados Unidos, debido a incumplimientos de seguridad de información por parte de las empresas (Gemalto NV, 2018).

Uno de estos robos cibernéticos reportados con mayor impacto y asociado al tema de nuestra tesis ocurrió en Bangladesh, que se encuentra situado en el sur de Asia, el Banco Central de Bangladesh sufrió un caso de robo de dinero de 81 millones de dólares en el año 2016. Luego de la investigación por varias empresas de seguridad de TI, incluyendo *Kaspersky* Lab (2016) lograron identificar que el grupo de hackers se llamaba Lazarus, siendo autor de ataques a compañías de fabricación, medios e instituciones financieras en al menos 18 países de todo el mundo desde el 2009.

El modo de operación de este grupo era romper un código vulnerable accesible remotamente como un servidor Web y plantar un malware dentro de esta página, para que una vez que se visita dicha página la computadora de la víctima (empleado de la empresa) reciba el malware lo que trae

componentes adicionales, permitiendo este estar dentro de la red y logrando expandir su control hasta obtener las credenciales privilegiadas de los sistemas y finalmente realizar su robo (*Information Security Media Group* [ISMG], 2016).

Al presenciar la gran cantidad de casos de robos informáticos reportados relacionados al uso de credenciales privilegiados para cumplir con su objetivo, se detecta que la empresa de retail puede ser víctima de este tipo de ataques, ya que administra gran cantidad de identidades al existir de 6 a 7 veces más cuentas privilegiadas que la cantidad de empleados existentes; debido a ello la gestión y actualización manual de contraseñas es un proceso costoso, repetitivo y lento, también se da otro escenario de riesgo interno al contar con credenciales privilegiadas compartidas entre diferentes administradores, lo que genera una brecha de inseguridad en el que no se tiene la trazabilidad de quién fue el autor del inicio de sesión y/o configuración de un sistema, lo que supone una considerable dificultad para su auditoría y riesgo porque impacta la continuidad operativa.

A continuación, se estará definiendo los accesos privilegiados como identidades privilegiadas.

1.1.2 Definición del Problema.

Inadecuada gestión de identidades privilegiadas de los administradores de las plataformas de TI en la empresa de retail.

Los problemas específicos son los siguientes:

- Lentitud en el proceso de autenticación.
- Riesgo de extracción de información de los activos de TI por usuarios no autorizados.
- Demora en el proceso de aprobación de acceso a dispositivos críticos y control de cambios en fase de producción de la empresa.

1.2 Objetivos

1.2.1 Objetivo General

Mejorar la gestión de identidades privilegiadas de los administradores de las plataformas de TI en la empresa de retail.

1.2.2 Objetivo Específicos

- Reducir el tiempo del proceso de autenticación en los activos de TI, mejorando la eficiencia operacional.
- Mitigar el riesgo de extracción de información de los activos de TI por usuarios no autorizados.
- Reducir el tiempo del proceso de aprobación de acceso a dispositivos críticos en producción de la empresa de retail.

1.3 Justificación

La justificación práctica es que la implementación de la solución de Gestión de Identidades Privilegiadas permitirá prevenir los accesos no autorizados, el *leapfrog* en los sistemas de la infraestructura de TI de la empresa, además, brindar acceso seguro con dichas identidades privilegiadas a los administradores de TI, permitiendo acceso a los dispositivos de forma controlada y auditada. Además, permitirá aumentar la eficiencia operacional con la funcionalidad de *Single Sign-on,* y brindar funcionalidades de monitoreo, grabación de sesión y rotación de contraseñas de dispositivos que son administrados por *Command Line Interface* (CLI).

Se podrá fortalecer el cumplimiento de las tareas de los administradores del área de TI, teniendo una autenticación centralizada, así como asegurar ambientes híbridos que posee la empresa y mitigar amenazas internas, además, esta implementación otorgará herramientas de auditoría y análisis forense en caso de producirse brechas de seguridad.

La solución de CA Technologies, *Privileged access manager* (Administración de accesos privilegiados), permitirá a la empresa de retail aumentar la eficiencia, garantizar un servicio consistente y de alta calidad, que

respaldará el crecimiento futuro de la compañía, optimizando el proceso de administración de credenciales privilegiadas y mayor visibilidad de las actividades de los usuarios privilegiados.

1.4 Alcance

Los alcances que tendrá el proyecto son los siguientes:

- La implementación del sistema de gestión de identidades privilegiadas para el control de acceso de los usuarios de la empresa de retail.
- Dentro de nuestro alcance se tendrá 150 equipos custodiados en la solución CA PAM, teniendo en cuenta que por cada dispositivo se configurará un máximo de dos cuentas.
- Para la implementación de la solución se hará la adquisición de dos licencias de CA PAM.
- Con respecto a los usuarios, se configurará 25 cuentas para los administradores de TI.
- Se realizará capacitación a los usuarios finales y administradores de la solución sobre el uso y administración de esta respectivamente (Ver Tabla 20).
- Los documentos para presentar al cliente son: Plan de implementación del proyecto, documento de diseño y arquitectura, levantamiento de observaciones, documento de configuración de equipos, plan de pruebas, resultado de la implementación de CA PAM, resultado del plan de prueba, levantamiento de observaciones de la implementación, guía de usuario, plan de recuperación del servicio y guía de proveedor.

1.5 Limitaciones

Las limitaciones que tendrá gel proyecto son los siguientes:

- No se proveerá licencia de los dispositivos que serán custodiados por CA PAM.
- No se proveerá el software y los equipos físicos requeridos para la implementación que son de responsabilidad del cliente (Ver Tabla 3 y 4).

- En base a las licencias adquiridas se tiene el límite de 25 usuarios que podrán acceder a la Solución CA PAM.
- Por cada servidor de la solución tendrá un máximo de 2 mil sesiones concurrentes.
- La implementación de la solución tendrá como duración 53 días (Ver Tabla 9).
- Cualquier cambio en la documentación de la solución, serán acordados previamente con los clientes y pueden dar lugar a cambio en el esfuerzo estimado.
- El cliente es el responsable de establecer y mantener un efectivo monitoreo de la solución y todos los controles internos.
- El cliente será responsable de la gestión de usuario del directorio activo.

1.6 Viabilidad

1.6.1 Viabilidad Técnica

Los recursos tecnológicos necesarios para el correcto funcionamiento de la solución son los virtual *appliance* en la que se aloja la solución (sistema operativo, base de datos y servicios de aplicaciones), además, se requiere de un recurso compartido para el alojamiento de las grabaciones de sesiones. El riesgo durante el desarrollo está relacionado con el acopio de la información verídica que debe proveer el cliente.

1.6.2 Viabilidad económica

Para la implementación de la solución se asumió un costo total de S/104,279.00 y el cliente asumió el costo hundido total S/13,184.00.

1.6.3 Viabilidad Social

El impacto obtenido fue satisfactorio ya que la información que gestiona la empresa de retail tiene niveles de seguridad más altos por lo que su vulnerabilidad es reducida.

1.6.4 Viabilidad Operativa

La solución es escalable y adaptable por lo que tiene proyección de operatividad sostenible, el primordial requisito es que la solución se encuentre en un *datacenter* (centro de datos) con el ambiente adecuado para mantener los servidores en óptimo estado y también tener una bóveda física de credenciales de los dispositivos custodiados por CA *Privileged Access Manager*.

CAPÍTULO II
MARCO TEÓRICO

En el presente capítulo, se muestran los antecedentes de temas similares que se han trabajado en relación con los sistemas de gestión de seguridad. Además, se detallan las bases teóricas necesarias para el desarrollo del tema de investigación. Por último, se realiza la definición de los términos más relevantes considerados en el transcurso del proyecto.

2.1 Antecedentes

Los antecedentes que se presentan a continuación son temas de investigación desarrollados en proyectos de pregrado y en maestrías de diversas universidades, entre nacionales y extranjeras que se basaron en temas similares a esta tesis.

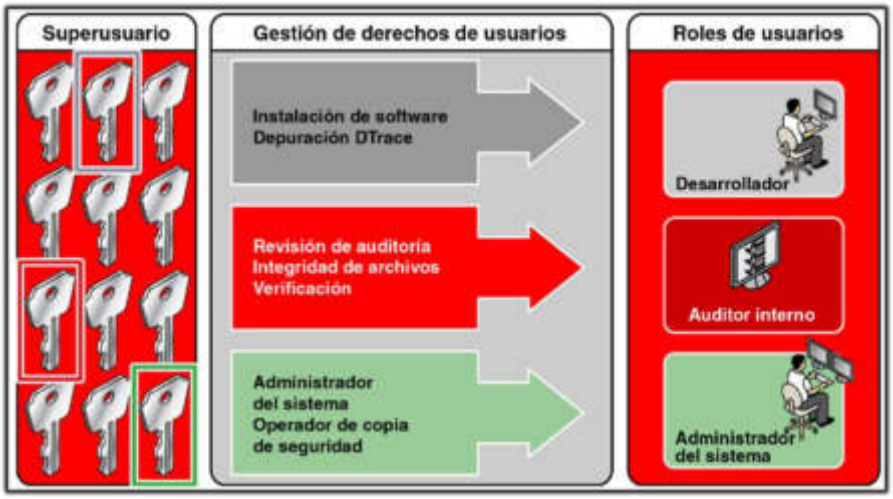
2.1.1 Amenazas de las credenciales de súper usuarios.

Sohner, M. (2014) en su tema de investigación “Gestión de usuarios privilegiados en contraseñas entornos compartidos” identificó que las amenazas surgen en un ambiente donde se utilizan credenciales con altos privilegios, esto se debe a que la mayoría de las veces estas son compartidas y utilizadas por personas que no cuentan con la autorización. De esta manera, se genera la inseguridad de los activos de información de la empresa y para evitar que estos casos se sigan suscitando, lo ideal es otorgar a cada persona una identidad individual. Con la finalidad de autenticar a un usuario y autorizar

el acceso a los recursos, para luego auditar las acciones que realicen cada una de las personas que cuentan con este tipo de privilegio (Ver Figura 1).

La importancia de aplicar esta medida es reducir el acceso incontrolable de personas no autorizadas a los sistemas privilegiados y así lograr minimizar el riesgo de que los activos de información sean extraídos ilícitamente.

Figura 1: Gestión de derechos de usuarios



Fuente: Oracle Company (2014)

2.1.2 Cuentas privilegiadas para proveedores de servicio cloud.

En la actualidad la gran mayoría de organizaciones utiliza la nube para almacenar sus activos de información y esperan que los datos almacenados sean protegidos en términos de confidencialidad, integridad y disponibilidad. Sin embargo, esto no las hace invulnerables de sufrir algún tipo de ataque ya que a medida que la infraestructura se distribuye en varias ubicaciones físicas, el acceso y el control se conceden a más personas, como consecuencia el riesgo se incrementa. La solución planteada es el manejo adecuado de autenticación que pueda ayudar a mitigar el riesgo de robo de cuentas, pérdidas y la transgresión de datos. Además, se debe aplicar la estrategia de que ningún individuo debe tener mayor control de lo que necesite

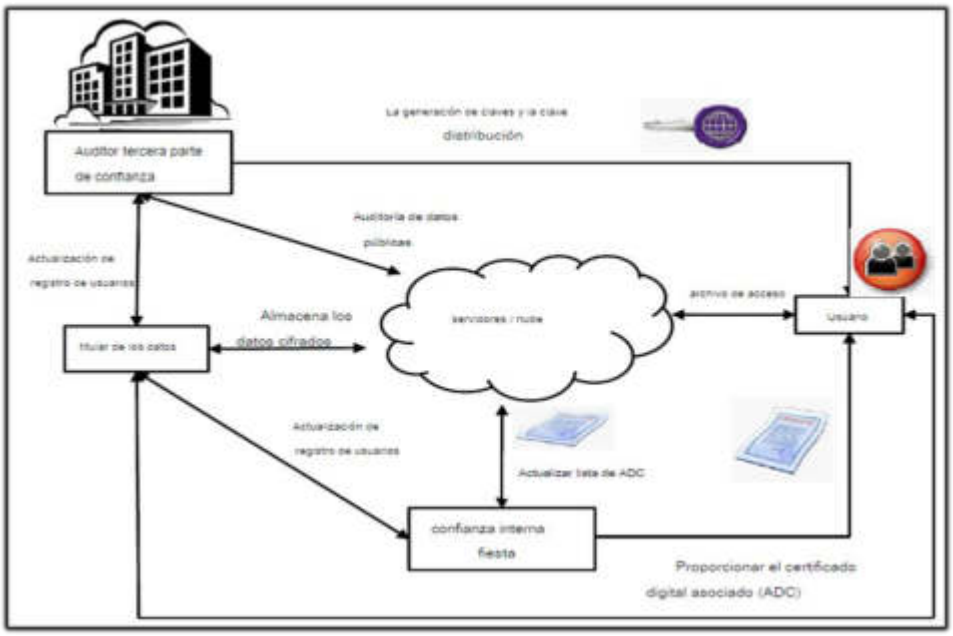
para cumplir su función. El método para asegurar que el privilegio se gestione correctamente es aplicar la administración de un acceso privilegiado (Suntana, K., Martini, B.,Hunt, R. & Raymond, K.,2015):

> La computación en la nube ayuda a la transformación de la industria de la computación tradicional, paradigma de Internet y TI. Debido a que muchos proveedores de servicios *cloud* (CSP) no son de confianza; la confidencialidad, integridad y privacidad de la información de la empresa deben ser protegidas por algún mecanismo. Es así como se propone el acceso por filtrado, que permite preservar los datos de los usuarios o intrusos desconocidos en la nube. (Manjusha, R. & Ramachandran, R. , 2015, p.220)

Hoy en día una gran cantidad de organizaciones está optando por migrar sus activos a máquinas virtuales alojadas en la nube, porque les permite tener acceso a una alta velocidad y a un costo mínimo. Sin embargo, esto no exime de la vulnerabilidad de acceso a la información que existe en este tipo de servicio. Es ahí que los derechos de acceso tienen que ser proporcionados con el fin de prevenir intrusos en la infraestructura de gestión de privilegios (PMI). El objetivo del diseño de la PMI es lograr el control de acceso a los archivos almacenados por el sistema de computación en la nube. No obstante, el titular de los datos debe activar el acceso privilegiado distintivo a cada usuario, lo que es diseñar exactamente en los ficheros de datos, que está autorizado a acceder.

Esta solución está en capacidad de lograr los objetivos de seguridad tales como la auditoría de usuario y favorecer procesos básicos tales como la modificación, inserción, eliminación, la verificación y la contribución de usuarios (Manjusha, R. & Ramachandran, R., 2015). En la siguiente figura se muestra lo descrito en este párrafo (Ver Figura 2).

Figura 2: La seguridad de la nube que utilizan certificados digitales



Fuente: Manjusha, R. y Ramachandran, R (2015)

2.1.3 Mitigar los riesgos en una cadena de suministro.

La cadena de suministro para una organización de bienes y servicios es un problema de seguridad, ya que muchos proveedores pueden tener un amplio acceso a los recursos y activos dentro del entorno de la empresa. Debido a esto los atacantes utilizan los medios más sofisticados para atacarlos porque son el blanco más fácil para un ataque inicial y son utilizados como un punto de entrada a su objetivo final. Por consiguiente, la solución tecnológica para mitigar el riesgo de la cadena de suministro, en la empresa, debe incluir la gestión de privilegios, implementar un control de acceso, monitoreo de los usuarios privilegiados y aplicar mecanismos para prevenir el abuso de información privilegiado Shackleford, D. (2015) (Ver Figura 3).

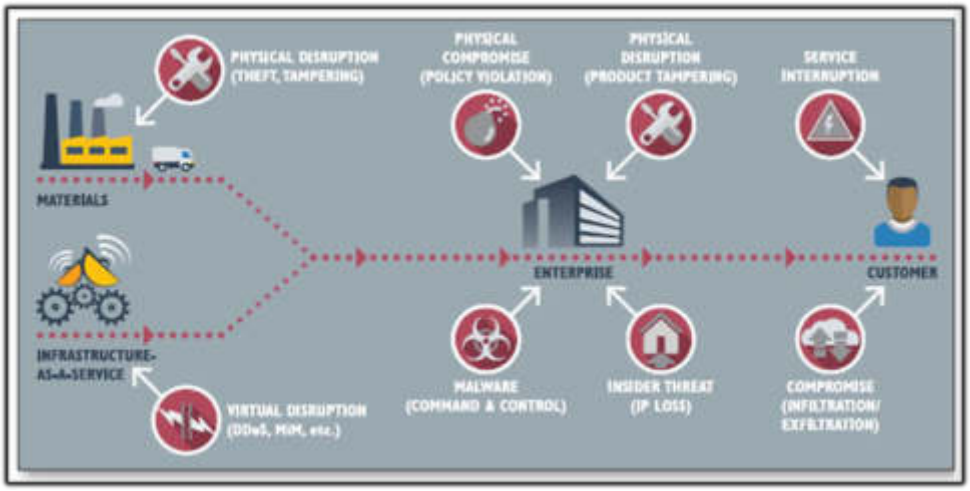
Por tal motivo se debe incluir lo siguiente:

- Ejecutar la separación de funciones y privilegios mínimos: consiste en que nadie puede realizar todas las funciones, para ello se debe conceder los privilegios necesarios a cada una (Shackleford, D., 2015).
- Implementar una estricta y robusta contraseña y aplicar políticas de gestión de cuentas: esto se debe efectuar tanto al personal como al

administrador de las cuentas privilegiadas para que sea más complicado al hacking expropiar las credenciales del personal (Shackleford, D. , 2015).

- Registro y monitoreo de las acciones de los empleados: se debe estar alerta a las funciones que realice el personal y realizar el seguimiento de las acciones (Shackleford, D., 2015).
- Tener cuidado que los administradores de sistemas y usuarios privilegiados estén compartiendo las credenciales a otros usuarios (Shackleford, D., 2015).

Figura 3: Brechas en la cadena de suministro



Fuente: Shackleford, D. (2015)

2.1.4 Sistemas de gestión de seguridad de información.

Cruz, M & Fukusaki, L. (2017) en su tesis “Diseño e implementación de un sistema de gestión de seguridad de la información para proteger los activos de información de la clínica Medcam Perú S.A.C” identificaron que la clínica Medcam Perú S.A.C presentaba una alta vulnerabilidad en los activos de información por falta de gestión de seguridad de información. Por tal motivo, es que los autores determinaron implementar un SGSI como una solución, para detectar, proteger y mitigar los riesgos a los que están expuestos los activos de información. Como resultado la empresa se encuentra en la capacidad de responder ante los riesgos a los que está expuesta. Además, la empresa con este SGSI garantiza el cumplimiento de la

ley 29733 que es la protección de datos personales de los clientes. Para cumplir con los objetivos propuestos los autores utilizaron como herramienta de apoyo la metodología PDCA.

Giraldo, L. (2016) en su tesis “Análisis para la Implementación de un Sistema de Gestión de la Seguridad de la Información según la Norma ISO 27001 en la empresa SERVIDOC S.A” identificó que la empresa Servidoc S.A no contaba con ningún método, control o política de seguridad que le permitiese identificar las vulnerabilidades, riesgos y ataques a los activos de la organización. Por tal motivo realizó un análisis para determinar el SGSI que le permita determinar y proponer una solución de seguridad de informática para las distintas áreas de las que está compuesta la empresa. Dentro de ello las principales y las que manejan información más sensible son contabilidad, facturación e historias clínicas de los pacientes. Para el tema de investigación Giraldo utilizó como herramienta de desarrollo la metodología Magerit, según la ISO 27001 tiene como propósito mitigar los riesgos de una organización.

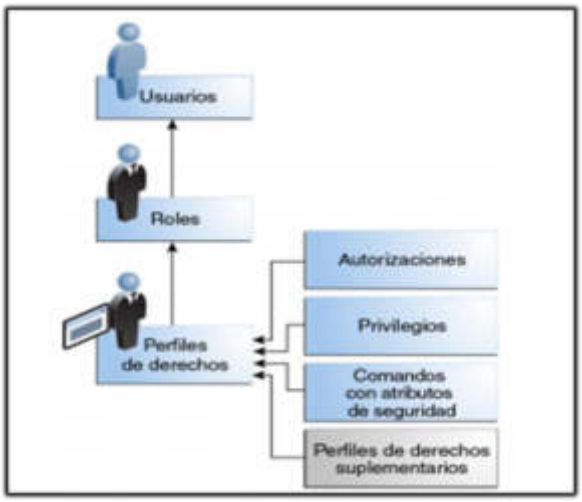
Villena, M. (2014) en su tesis “Diseño de un sistema de gestión de seguridad de información para servicios postales del Perú S.A” identificó que la empresa Perú S.A. se encontraba en la necesidad de implementar un SGSI. Debido a que la nueva resolución ministerial con N°129-2012-PCM solicita que toda empresa dedicada al servicio de Serpost debe tener implementado un sistema de seguridad. El cual garantice los servicios postales en todas sus modalidades con ámbito de acción a nivel nacional e internacional ya que para ese entonces la empresa no contaba con ningún SGSI. No obstante, luego de la implementación la empresa obtuvo como resultado la aprobación ministerial. Además, garantizó la protección de la información digital independientemente del área que la contenía. Esta implementación se realizó mediante la metodología COBIT 5.0.

2.1.5 Mitigación de los riesgos a través de políticas de seguridad.

Guarnizo, J, & Prieto, E. (2014) en su tema de investigación “Diseño de un sistema de gestión de seguridad de la información (SGSI) para la empresa Agility S.A” identificaron que la empresa Agility S.A. fue vulnerada y experimentó un alto grado de pérdida y alteración de su información. Debido a que no contaba con controles, políticas y sistemas de filtrado que detecten y garanticen la integridad, confidencialidad y disponibilidad de los datos. Por tal motivo, Los Autores diseñaron un SGSI para asegurar y proteger la información, y a su vez tener un ambiente suficiente y seguro para proteger los activos de información. Con la finalidad de asegurar la credibilidad de la organización y generar la confianza de los clientes. No obstante, para cumplir con el objetivo del proyecto Los Autores se basaron en la herramienta metodológica PDCA, la cual proporciona una solución sistemática a los problemas y mejora de procesos. Finalmente, asegurar la reducción de costes de la no calidad manteniendo la eficacia y eficiencia de la organización (Ver Figura 4).

Talavera, V. (2015) en su tesis “Diseño de un sistema de gestión de Seguridad de la información para una entidad estatal de salud de acuerdo con la ISO/IEC 27001:2013”, detectó que no cuenta con un SGSI que le permita identificar los riesgos a los cuales se encuentran expuestos los activos de información del Instituto Nacional Materno Perinatal. Por tal motivo se propone como objetivo diseñar el SGSI de acuerdo con lo que indica la ISO/IEC 27001:2013. Obteniéndose como resultado el diseño e implementación de controles y políticas de seguridad de la información. Es así que concluye que se debería crear un comité de seguridad de la información, órgano que se encarga de gestionar e implementar el SGSI. Además, debe tener soporte de la dirección general para que facilite el acceso y el análisis del riesgo que acecha a cada área de la entidad de salud.

Figura 4: Gestión de seguridad de Información



Fuente: Oracle Company (2014)

2.2 Bases teóricas

2.2.1 Administración de acceso privilegiado (PAM).

El sistema de PAM según Rouse, M. (2016) es un marco para los procesos de negocios que facilita la gestión de las identidades electrónicas. El cual puede ser utilizado para iniciar, capturar, gestionar identidades de los usuarios y sus permisos de acceso correspondiente de forma automatizada. Esto asegura que los privilegios de acceso se concedan con una interpretación de políticas y reglas establecidas. De modo que todos los individuos al momento de conectarse a sus máquinas, estas están debidamente autenticadas, autorizadas y auditadas. (p.1)

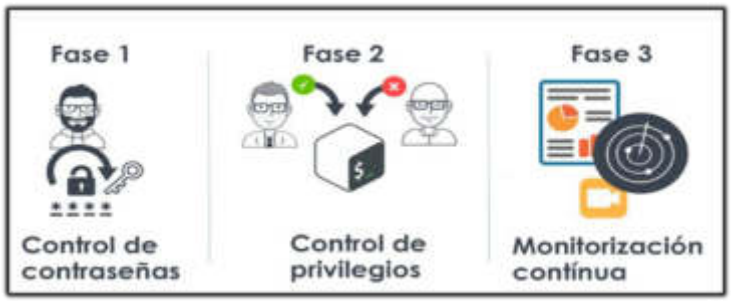
Gilart, I. (2016) afirma: La gestión y seguridad de las cuentas privilegiadas necesitan procedimientos y soluciones que difundan las medidas de control habituales y requieren una adecuación entre el nivel de riesgo y la operativa llevada a cabo por los usuarios. Y tiene como objetivo unificar la identidad en todas las plataformas para reducir la complejidad de la gestión de estas. (p.1)

Fadida, I., Balzam, G., Jerbi, A. & Barak, N. (2014) en su artículo "*Privileged shared account password sanitation*" afirman que las cuentas con

privilegios son utilizadas para tener acceso a datos y procesos críticos. Los administradores de sistemas suelen utilizar este tipo de cuentas para realizar tareas administrativas, en puntos finales, también para colocarlos en archivos de servicio de scripts y archivos de configuración para facilitar el procesamiento sin vigilancia. El riesgo de usar estas cuentas es que no se tiene un control de las actividades que se realizan ya que no se asigna a cada usuario una identificación personal. Para minimizar el riesgo surgió CA PAM (Gestión de acceso privilegiado) es un software que a través de su proceso integrado permite a una organización asegurar, administrar y dar seguimiento de todas las actividades asociadas con las cuentas más poderosas dentro de la organización. PAM proporciona gestión de acceso basado en roles para cuentas privilegiadas en puntos finales de destino de una locación central.

Representa el acceso a un espacio compartido donde varios usuarios pueden acceder con sus credenciales (Ver Figura 5).

Figura 5: Fases del despliegue de cuentas privilegiadas



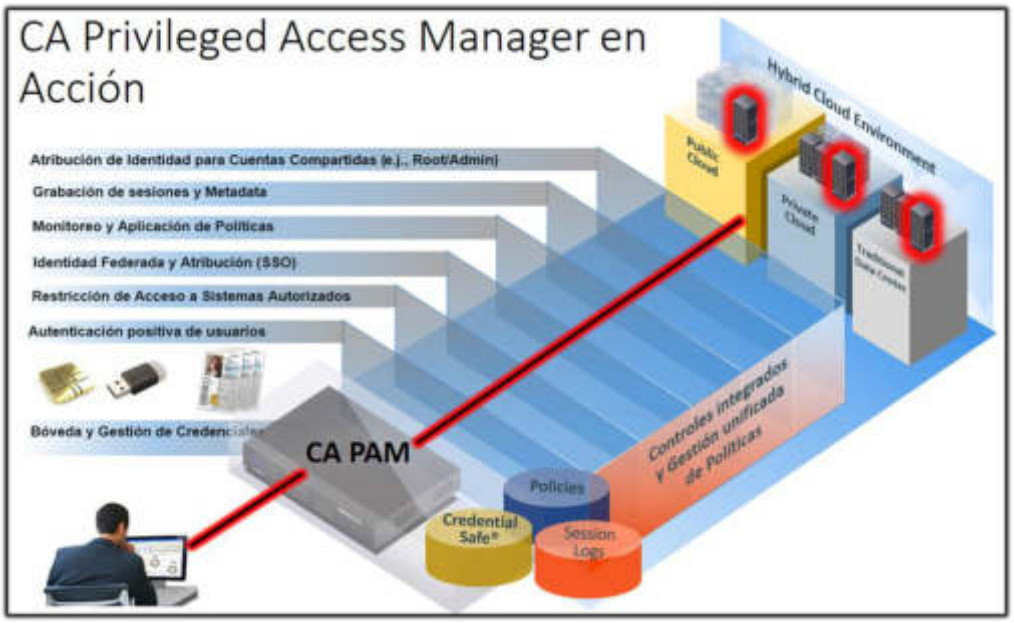
Fuente: Rubén Ramiro (2017)

2.2.2 Gestión de contraseñas PAM.

Administración de accesos privilegiados (PAM) es un mecanismo flexible para la autenticación de usuarios. Gracias a PAM, los administradores de sistemas pueden modelar e implementar diferentes políticas de autenticación para los distintos usuarios de forma individualizada para cada servicio. Pero hay que manejar estas facilidades con mucho cuidado ya que se debe conocer correctamente el funcionamiento o estar muy atentos. Debido a que un descuido puede comprometer gravemente la seguridad del sistema (González, I & Padrón, M., 2014) (Ver Figura 6).

Las ventajas que brinda CA PAM según CA Technologies (2018) son: “(1). Ofrece un esquema de autenticación común y centralizado. (2) Permite a los desarrolladores abstraerse de las labores de autenticación. (3) Facilita el mantenimiento de las aplicaciones. (4) Ofrece flexibilidad y control tanto para el desarrollador como para el administrador de sistema.” (p.3).

Figura 6: Diagrama PAM



Fuente: CA Technologies (2018)

2.2.3 Amenaza Cibernética.

Las amenazas pueden darse de forma externa o interna en la organización, pueden ser oportunistas o bien planificadas y selectivas. También pueden ser perpetradas por individuos o por grupos de individuos (Hibbert, B. & Haber, M., 2018).

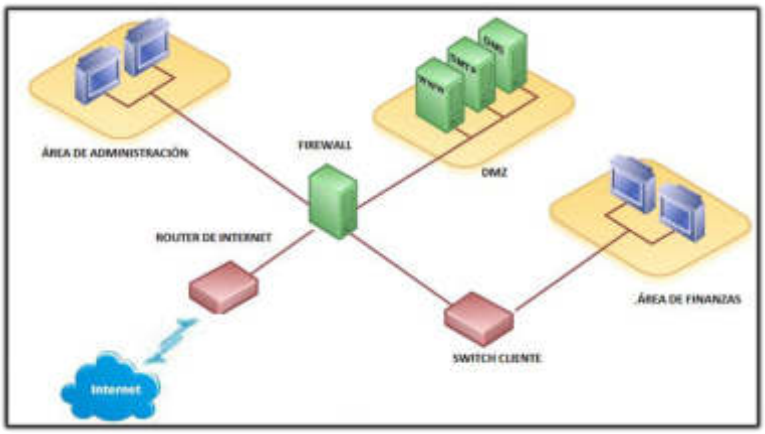
Las tecnologías de información y la comunicación se han desarrollado enormemente. Lo que empezó como una herramienta para ayudar a optimizar los procesos administrativos, es ahora un instrumento estratégico en la industria, la administración y la defensa. Con ello también las amenazas cibernéticas fueron apareciendo según la evolución de la

tecnología, un ejemplo de ello es la crisis de Kosovo, en donde la OTAN se vio afectada con estos primeros *malware* (programas malignos) que afectaron los sistemas informáticos críticos que administran suministros de energía. En ese entonces los ciberataques se vieron solo como un riesgo, limitado en su alcance y daño potencial (Caro, J., 2013).

Los ataques cibernéticos son eventos que se inician a través del Internet contra un objetivo con la intención de negar, interrumpir, destruir o explorar un entorno operativo habilitado para la computadora. Muchos ataques de este tipo están destinados a comprometerse con fines de explotación, extracción, manipulación o destruir la integridad de datos específicos (Hudson, 2017).

Todos los ciberataques tienen como fin apoderarse de información de suma importancia de una o varias organizaciones y/o empresas, para posteriormente lucrar a través de ello. Por ejemplo, vender esta información a la propia empresa o en otros casos distribuirla en los mercados negros, lugar en donde está muy cotizado este tipo de información. Por tal motivo, es de suma importancia que las organizaciones diseñen y estructuren bien su red interna, como se logra observar en la siguiente imagen (Ver Figura 7).

Figura 7: Estructura de red para mitigar amenazas



Fuente: Elaboración de autores

2.2.4 Amenazas Internas.

Una amenaza interna está relacionada con las malas intenciones, descuido del empleado, socios o terceros como contratistas que pongan en riesgo la confidencialidad y bienestar general de la información vital para una empresa (Hibbert, B. & Haber, M., 2018).

El control interno es un sistema estructural y organizacional conformado por un conjunto de procedimientos que puede ayudar a una empresa a reducir la extracción ilegal de información, la pérdida de recursos y evitar los ataques internos. Esto permite conseguir sus metas de desempeño y rentabilidad, evitando peligros no reconocidos y sorpresas a lo largo del trayecto operativo de la organización (Centro Integral de Educación Continua, CIEC, 2009).

Para evitar amenazas internas y reducir el riesgo de ser vulnerada la información de la organización, el personal debe cumplir con las políticas, procedimientos, prácticas y estructuras organizacionales. Estas son definidas por la alta gerencia, esto debe formar parte de la cultura organizacional del control interno, lo que implica un proceso de capacitación para dejar en claro el papel que debe cumplir el empleado ya que esto también determina la continuidad del negocio (ISO/IEC 27001, 2013).

2.2.5 Seguridad de Información.

La seguridad de la Información tiene como fin la protección de la confidencialidad, la integridad, la disponibilidad y que no se lleve a cabo la interrupción o destrucción no autorizada de la información y/o datos. Independientemente del formato en que se encuentre, ya sean electrónicos, impresos, audio u otros. Cabe aclarar que la seguridad absoluta no es posible, no existe un sistema 100% seguro, de forma que el elemento de riesgo está siempre presente (Hibbert, B. & Haber, M., 2018) (Ver Figura 8).

El sistema de gestión de seguridad de la información preserva la confidencialidad, integridad y disponibilidad de la información mediante la

aplicación de un proceso de gestión de riesgos y otorga a las partes interesadas confianza sobre la adecuada gestión de los riesgos. (ISO/IEC 27001, 2013, p.5)

Los activos están sujetos tanto a amenazas deliberadas como accidentales, mientras que los procesos relacionados, los sistemas, las redes y las personas tienen vulnerabilidades inherentes. Los cambios en los procesos y sistemas de negocio u otros cambios externos pueden crear nuevos riesgos de seguridad de la información. Por lo tanto, dada la variedad de formas en que las amenazas podrían aprovecharse de las vulnerabilidades para dañar a la organización, los riesgos de seguridad de la información están siempre presentes. Una seguridad de la información eficaz reduce estos riesgos protegiendo a la organización frente a las amenazas y vulnerabilidades, y en consecuencia reduce el impacto en sus activos. (ISO/IEC 27002, 2013, p.6)

No obstante, las grandes empresas están en continuo seguimiento sobre la seguridad de su información, es por tal motivo, que también renuevan constantemente sus herramientas tecnológicas para velar por la seguridad y evitar que intrusos vulneren el acceso a su data.

Figura 8: Los tres pilares que garantizan la seguridad de la información

Fuente: Eloisa Calixto Marquez (2017)

2.2.6 Norma ISO/IEC 27000.

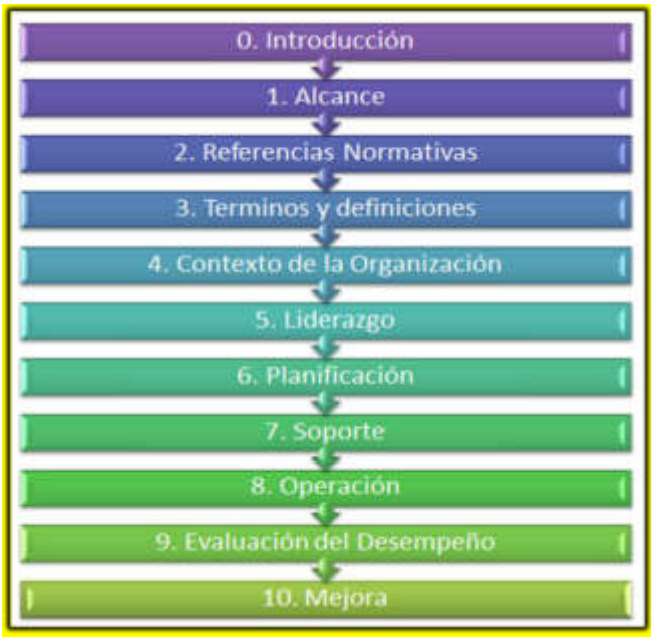
- **Norma ISO/IEC 27001:2013**

La ISO/IEC 27001 (2013) es un estándar internacional desarrollado como una guía para el análisis, implementación, control y mantenimiento de un Sistema de Gestión de Seguridad de la Información. Con un enfoque orientado a los procesos de negocio, es una norma general aplicable a cualquier giro de negocio y activos de información que las empresas puedan tener. (p.5)

La ISO se adapta a las necesidades exactas de la organización, a través de los controles de seguridad de la información que se identifiquen, facilitando la integración y trabajo conjunto entre los diferentes estándares de gestión publicados por dicha entidad (ISO/IEC 27001, 2013).

En la siguiente imagen se muestra la estructura de la ISO 27001:2013, sin embargo, para el desarrollo del proyecto se considera desde la fase seis “planeación” hasta la última fase de “mejora” (Ver Figura 9).

Figura 9: Estructura de la ISO/IEC 27001:2013



Fuente: ISO/IEC 27001(2013)

Según la estructura de la ISO 27001:2013 está dividida en 11 fases de las cuales, para el análisis, implementación, control y mantenimiento del sistema de gestión de seguridad de información de nuestro proyecto, se consideró las fases de planificación, soporte, operación, evaluación de desempeño y mejora. De las cuales se procede a detallar cada una de ellas, y así mismo se hace referencia de los entregables que se tiene en cada fase.

- **Fase 1: Planificación**

Consiste en asegurar que el SGSI consiga los resultados previstos, reducir los efectos indeseados, analizar los riesgos de la seguridad de información, determinar los recursos requeridos y determinar la responsabilidad de controlar el sistema luego de su implementación (ISO/IEC 27001, 2013).

Entregable

- Plan de implementación del proyecto.

- **Fase 2: Soporte**

Consiste en identificar los recursos a utilizar para la implementación, mantenimiento y mejora continua del SGSI, y para ello la empresa debe estar disponible en otorgar facilidades de adquisición de estos (ISO/IEC 27001, 2013).

Entregable

- Documento de diseño y arquitectura.

- **Fase 3: Operación**

Según la ISO/IEC 27001 (2013) Consiste en “Implementar, planificar y controlar los procesos para cumplir con los requisitos propuestos” (p.12).

Entregables

- Levantamiento de información.

- Documento de resumen de configuración.
- Plan de prueba.

- **Fase 4: Evaluación del desempeño**

Consiste en evaluar el desempeño y la eficacia del SGSI, a través del monitoreo del comportamiento de la solución implementada

Entregables

- Resultado de la implementación de CA PAM.
- Resultado de plan de prueba.

- **Fase 5: Mejora**

Consiste en aplicar las soluciones de mejoras a las fallas detectadas en la etapa anterior, con el propósito de cumplir con los objetivos propuestos en el plan de proyecto (ISO/IEC 27001, 2013).

Entregables

- Levantamiento de observaciones de la implementación.
- Guía de usuario.
- Plan de recuperación del servicio.
- Guía de proveedor.

- **Norma ISO/IEC 27002:2013**

La norma de seguridad de la información ISO / IEC 27002 (2013) es un “Código de prácticas para los controles de seguridad de la información" (p.1). El documento ofrece recomendaciones de buenas prácticas y orientación para que las organizaciones puedan seleccionar e implementar controles de seguridad de la información en el proceso de iniciar, implementar y mantener un SGSI (ISO / IEC 27002, 2013).

En la siguiente imagen se muestra la estructura que conforman la ISO 27002:2013 (Ver Figura 10).

Figura 10: Fases de la norma ISO 27002:2013

Fuente: Ana Rojo (2016)

En la siguiente tabla se describen las 14 fases de la ISO 27002:2013, sin embargo, para el desarrollo de proyecto nos apoyamos desde la fase de políticas de seguridad de información hasta la fase de criptografía, fases que también son descritas por la ISO 27001:2013, pero con menor detalle (Ver Tabla 1).

Tabla 1: Fases de la ISO 27002:2013

Norma ISO 27002:2013	
Fases	**Descripción**
Política de seguridad de información	Consiste en proporcionar orientación y apoyo a la gestión de seguridad de la información de acuerdo con los requisitos del negocio y normas pertinentes.
Organización de seguridad de la información	Se basa en establecer un marco de gestión para iniciar y controlar la implementación y operación de la seguridad de la información dentro de la organización.
Seguridad relativa a los recursos humanos	Consiste en establecer políticas para asegurar la responsabilidad de los empleados y los contratistas.

Fases	Descripción
Gestión de activos	Se basa en identificar los activos de la organización y definir las responsabilidades de protección adecuadas.
Control de acceso	Permite limitar el acceso a los recursos de tratamiento de información y a la información.
Criptografía	Consiste en garantizar un uso adecuado y eficaz de la criptografía para proteger la confidencialidad, autenticidad y/o integridad de la información.
Seguridad física y del entorno	Se basa en prevenir el acceso físico no autorizado, los daños e interferencia a la información de la organización y a los recursos de tratamiento de la información.
Seguridad de las operaciones	Consiste en asegurar el funcionamiento correcto y seguro de las instalaciones de tratamiento de la información.
Seguridad de las comunicaciones	Permite asegurar la protección de la información en las redes y los recursos de tratamiento de la información.
Adquisición, desarrollo y mantenimiento de los sistemas de información	Consiste en garantizar que la seguridad de la información sea parte integral de los sistemas de información a través de todo el ciclo de vida. Esto también incluye los requisitos para los sistemas de información que proporcionan los servicios a través de redes públicas.
Relación con proveedores	Consiste en asegurar la protección de los activos de la organización que sean accesibles a los proveedores.
Gestión de incidentes de seguridad de la información	Se basa en asegurar un enfoque coherente y eficaz para la gestión de incidentes de seguridad de la información, incluida la comunicación de eventos de seguridad y debilidades.
Aspectos de seguridad de la información para la gestión de la continuidad del negocio	La continuidad de la seguridad de la información debería formar parte de los sistemas de gestión de continuidad del negocio de la organización.
Cumplimiento	Consiste en evitar incumplimientos de las obligaciones legales, estatutarias, reglamentarias o contractuales relativas a la seguridad de la información o de los requisitos de seguridad.

Fuente: ISO/IEC 27002 (2013)

Las sesiones de las fases establecidas por la ISO/IEC 27002 son 14, de las cuales para el desarrollo e implementación del sistema de gestión de seguridad de información de este proyecto se consideraron las 6 primeras, que son las siguientes.

- **Fase 1: Política de seguridad de información**

Se define el “Conjunto de políticas de seguridad de información al máximo nivel que sea aprobado por la dirección y comunicado a los empleados” (ISO/IEC 27002, 2013, p.9).

- Control de acceso.
- Uso adecuado de activos.
- Controles criptográficos.
- Privacidad y protección de la información identificativa de personas.

- **Fase 2: Organización de seguridad de la información**

Consiste en asignar responsabilidades relativas a seguridad de la información para proteger los activos de la empresa. Aquellos individuos a los que se les han asignado responsabilidades de seguridad pueden delegar estas tareas de seguridad a otros. Sin embargo, se debe comprobar que las tareas que se asignaron sean realizadas correctamente. (ISO/IEC 27002, 2013, p.12)

- Asignar roles y cargos de trabajo.
- Segregar tareas para reducir el riesgo de uso incorrecto de los activos de la organización.

- **Fase 3: Seguridad relativa a los recursos humanos**

Consiste en elegir a la persona idónea que pueda hacerse cargo de los activos y de la información sensible que maneja la empresa (ISO/IEC 27002, 2013).

- Cuando un empleado se retira de la empresa se debe eliminar las credenciales que estuvo utilizando.

- **Fase 4: Gestión de activos**

Se basa en que la organización debe identificar los activos

relevantes para el ciclo de vida de la información, también debe documentar su importancia y conservarla en inventario (ISO/IEC 27002, 2013).

- Inventarios de los activos de la organización.
- Relacionar los activos con sus propietarios.

- **Fase 5: Control de acceso.**

Consiste en establecer, documentar y revisar una política de control de acceso basada en los requisitos de negocio y de seguridad de la información (ISO/IEC 27002, 2013).

- Acceso a las redes y a los servicios de red solo por personal autorizado.
- Registro y baja de usuarios.
- Aprovisionamiento de acceso de usuario a los sistemas de información.
- Restringir y controlar el uso de usuarios con privilegios.
- Retirar o reasignar los derechos de acceso.
- Advertir del uso y confidencialidad de la autenticación.
- Restricción del acceso a la información en base a las políticas de control de acceso.
- Seguir el proceso seguro de autenticación.
- Asignar Contraseñas robustas.
- Monitorear el acceso donde se encuentran los principales activos de la organización.

- **Fase 6: Criptografía.**

En la norma ISO/IEC 27002 (2013) la criptografía consiste en "Desarrollar e implementar una política sobre el uso de los controles criptográficos para proteger la información" (p.40).

- Implementar políticas de gestión de claves.
- Determinar la dimensión y la complejidad de las claves.

- Determinar cada que tiempo se debe cambiar la clave.
- Destruir las claves en caso de que el empleado se retire de la empresa.

2.2.7 Método PDCA.

La ISO 27001:2005 es la norma que brinda un modelo robusto para implementar los principios en aquellas directrices que controlan la evaluación de riesgos, diseño e implementación de la seguridad, gestión y reevaluación de la seguridad (ISO/IEC 27001, 2005).

Para implementar un SGSI en base a los controles, la norma ISO recomienda utilizar el método *Plan-Do-Check-Act* (PDCA), que en español es Planificar-Hacer-Verificar-Actuar. Es un método cíclico (Ver Figura 11).

- **Etapa 1: Planificar**

  Se establecen las políticas, los objetivos, procesos y procedimientos de seguridad pertinentes para gestionar el riesgo y mejorar la seguridad de la información. Con el fin de entregar resultados acordes con las políticas y objetivos globales de una organización (ISO/IEC 27001, 2005).

- **Etapa 2: Hacer**

  Se lleva a cabo la implementación del SGSI aplicando las políticas, los controles, procesos y procedimientos establecidos en la primera etapa (ISO/IEC 27001, 2005).

- **Etapa 3: Verificar**

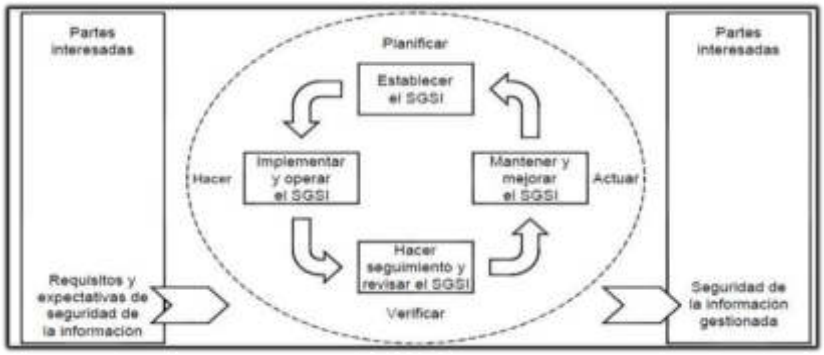
  Se evalúa y se mide el desempeño del proceso contra las políticas, los objetivos de seguridad y la experiencia práctica, para reportar los resultados fallidos, con la finalidad de identificar y plantear acciones correctivas (ISO/IEC 27001, 2005).

- **Etapa 4: Actuar**

  Consiste en emprender acciones correctivas y preventivas en

base a los resultados de la auditoría interna del SGSI y la revisión por la dirección, para lograr la mejora continua del SGSI (ISO/IEC 27001, 2005).

Figura 11: Modelo PDCA aplicado a los procesos de SGSI



Fuente: Proyecto de Norma Técnica Colombiana (2012)

2.3 Términos Básicos

- **Appliance:** Sistema integrado que contiene conjunto de funciones y herramientas en un mismo espacio.
- ***Single sign-on*:** "Es un procedimiento de autenticación que habilita al usuario para acceder a varios sistemas con una sola instancia de identificación" (Apress.Telefónica, T., 2009, p.199).
- **Riesgo:** "Efecto de la incertidumbre sobre la consecución de los objetivos" (ISO/IEC 27000, 2014, p.13).
- **Amenaza:** "Causa potencial de un incidente no deseado, el cual puede ocasionar daño a un sistema o a una organización" (ISO/IEC 27000, 2014, p.16).
- **Análisis de riesgo:** "Criterios de riesgo para determinar si el riesgo y/o su magnitud son aceptables o tolerables" (ISO/IEC 27000, 2014, p.15).
- **Vulnerabilidad:** "Debilidad de un activo o de un control que puede ser explotada por una o más amenazas" (ISO/IEC 27000, 2014, p.17).
- **Confidencialidad:** "Propiedad de la información por la que se mantiene inaccesible y no se revela a individuos, entidades o procesos no autorizados" (ISO/IEC 27000, 2014, p.7).
- **Integridad:** "Propiedad de exactitud y completitud" (ISO/IEC 27000, 2014, p.10).

- **Ataque:** Acto de aplicar la fuerza para ingresar a un acceso sin tener la autorización (Hibbert, B. & Haber, M. ,2018).
- **Ataque *Leapfrog*:** Son ataques que se llevan a cabo a través de saltos por puertos abiertos, empiezan con la obtención de información menos riesgoso, para luego ser utilizados y perpetrar otros ataques de mayor riesgo.
- **Ciberataque:** Difusión de programas maliciosos (virus) para extraer información ilícita a través de la Internet (Hibbert, B. & Haber, M., 2018).
- **Sistema de Gestión:** "Conjunto de elementos de una organización, interrelacionados o que interactúan para establecer políticas, objetivos y procesos para lograr estos objetivos" (ISO/IEC 27000, 2014, p.11).
- **Seguridad de información:** "Protección adecuada de la información contra la pérdida de su disponibilidad, confidencialidad e integridad" (ISO/IEC 27000, 2014, p.17).
- **Respuesta a los ciberataques:** Aplicación de barreras para contra restar los ataques que se dan a través de la Internet.
- **Disponibilidad:** "Propiedad de ser accesible y estar listo para su uso a demanda de una entidad autorizada" (ISO/IEC 27000, 2014, p.7).
- **Privilegios:** "Es un derecho especial o una ventaja. Es una elevación por encima de la normal y no un ajuste o un permiso dado a las masas" (Hibbert, B. & Haber, M., 2018, p.26).
- **Identidades Privilegiadas:** Credenciales con privilegios.
- **Trazabilidad:** Es el registro de todas las acciones en un ciclo de producción antes de llegar al final del resultado.
- **Sistema de Información:** "Aplicaciones, servicios, activos de tecnologías de la información y otros componentes para manejar información" (ISO/IEC 27000, 2014, p.10).
- **Identidad:** "Es un ser humano, o usuario, que interactúa con los recursos de las aplicaciones de los sistemas operativos" (Hibbert, B. & Haber, M. 2018, p.10).
- **Políticas:** Conjunto de reglas y directrices que se establecen para un procedimiento.
- **Cuentas:** "Es una representación electrónica de una identidad o de referencia para un conjunto de permisos y privilegios necesarios para una

aplicación o recurso de conectar o utilizar dentro de los confines de sistema" (Hibbert, B. & Haber, M., 2018, p.10).

- **Tecnología de Información (TI):** "Conjunto de herramientas, procesos, metodologías y equipos que ayuda a facilitar la creación, transformación, almacenamiento, transmisión, protección y destrucción de información" (Hibbert, B. & Haber, M., 2018, p.18).
- ***Firewall*:** Software o Hardware que tiene como funcionamiento permitir el acceso de un dispositivo de TI a internet y/o a otro dispositivo de la misma red.

En el siguiente capítulo se dará a conocer de manera más granular los materiales y método utilizado para realizar la implementación de la solución.

CAPÍTULO III
METODOLOGÍA

En el presente trabajo se lleva a la práctica la investigación aplicada, ya que se emplean los conocimientos adquiridos durante la formación profesional. Lo cual permite identificar y evaluar alternativas de mejora del proceso de investigación.

Se dará a conocer los materiales, el método y la norma ISO 27001:2013 a utilizar, que nos permitirá cumplir con los objetivos planteados.

3.1 Materiales

A continuación, se mencionará los materiales que se requerirán durante la implementación del proyecto, teniendo en cuenta que los materiales que son responsabilidad del cliente no incurrirán un costo para el proyecto, ya que son recursos que proveerá el cliente coordinado previamente a iniciar el proyecto.

3.1.1 Recursos Humanos.

Seguidamente, los recursos humanos que se requerirán para el desarrollo del proyecto (Ver Tabla 2). Por acuerdo de confidencialidad no será posible la divulgación de los nombres de los clientes, por ello se denominarán Cliente 1 y Cliente 2.

Tabla 2: Recursos humanos utilizados en el proyecto

Rol	Responsable	Descripción
Gestor del proyecto	Lucía Contreras	Encargado de gestionar las coordinaciones con los interesados y dar seguimiento a las actividades del proyecto.
Consultor Security Information	Lucía Contreras	Encargado de levantar requerimientos funcionales y no funcionales, además, realizar el desarrollo de la implementación.
Analista de TI	Roberto Vega	Encargado de realizar el desarrollo de la implementación.
Líder del proyecto	Cliente 1	Jefe de departamento de redes, telecomunicaciones y base de datos (DRTBD) de la empresa de retail, es encargado de aprobar el inicio y cierre del proyecto.
Líder técnico del proyecto	Cliente 2	Especialista en el área DRTBD de la empresa de retail, es responsable de administrar la solución de gestión de credenciales y brindar datos requeridos de la empresa.

Fuente: Elaboración de autores

3.1.2 Software.

A continuación, se describen los recursos de software que se requerirán para el desarrollo del presente proyecto, que permitirán desplegar y dar soporte a la solución propuesta (Ver Tabla 3). La empresa de retail se deberá de encargar de la adquisición e implementación del software indicado como su responsabilidad, según lo establecido en el contrato previamente a iniciar el proyecto.

Tabla 3: Software utilizado en el proyecto

Nombre de recurso	Cantidad	Responsable	Descripción
CA Privileged Access Manager (Contiene sistema operativo, base de datos y servidor de aplicaciones)	2	CA Technologies	Virtual Appliance versión 3.2.

Nombre de recurso	Cantidad	Responsable	Descripción
Repositorio para grabación de sesiones.	2	Cliente	*Capacidad 512 GB. *Usuario / Contraseña. *Ruta del recurso compartido.
Ofimática, MS Office 2013	2	Cliente	MS Word / MS Excel / MS Visio / Onedrive.
Plataforma de virtualización.	1	Cliente	VMware Esxi versión 6 mínimo.
VMware Workstation	2	Autores	Versión 12
Alta Disponibilidad	1	Cliente	* Virtual IP * FQDN del VIP
Dispositivos para configurar	150	Cliente	Los dispositivos que serán custodiados por CA PAM.
Microsoft Active Directory	1	Cliente	Directiva de grupo

Fuente: Elaboración de autores

3.1.3 Hardware.

A continuación, se describen los recursos de hardware que se requerirán para el desarrollo del presente proyecto, que permitirán desplegar y dar soporte a la solución propuesta (Ver Tabla 4). La empresa de retail se deberá de encargar de la adquisición e implementación del hardware indicado como su responsabilidad, según lo establecido en el contrato previamente a iniciar el proyecto.

Tabla 4: Hardware utilizado en el proyecto

Nombre de recurso	Cantidad	Responsable	Descripción
Jump Server (Servidor de salto)	1	Cliente	* Windows Server 2012 R2 * Disco duro: 1 TB * 8 GB de memoria RAM
Servidor para CA PAM	2	Cliente	Virtual (VMWARE) * 01 Quad Core Intel Xeon > 3.5 GHz o Equivalente * 16 GB de memoria RAM * Disco duro: 80GB

Nombre de recurso	Cantidad	Responsable	Descripción
Laptop Personal	2	Autores	*RAM: 8 gb *Disco duro: 1 Tb
Impresora	1	Autores	HP
Comunicación	2	Autores	Cable de red

Fuente: Elaboración de autores

3.1.4 Costos del proyecto.

A continuación, se detallarán los costos que se requiere en el presente proyecto con respecto a los recursos humanos, software y hardware.

Los costos asumidos por el cliente no son considerados como parte del costo total de nuestro proyecto, ya que son considerados como costo hundido.

a. Costos de recursos humanos

Los costos de recursos humanos asumidos por la empresa consultora a su equipo de proyecto (Ver tabla 5).

Tabla 5: Costos de recursos humanos de la empresa consultora

Equipo de proyecto	Días laborales	Cantidad horas / día	Cantidad horas laboradas	Costo hora - hombre	Costo total
Gestor del proyecto	50	8	400	S/20.00	S/8,000.00
Consultor *Security Information*	36	8	288	S/18.00	S/5,184.00
Analista de TI (*)	36	6	216	S/0.00	S/0.00
Subtotal					S/13,184.00

Fuente: Elaboración de autores

(*) La empresa consultora no realizó remuneración alguna al Analista de TI, debido que es considerado como apoyo al no pertenecer a

esta. Sin embargo, el costo de un Analista de TI según el mercado es de S/.15.00 por hora y para el presente proyecto sería un costo total de su sueldo S/. 3,240.00.

Los costos de recursos humanos asumidos por la empresa de retail (Ver tabla 6). El rol del cliente 1 es líder del proyecto y el cliente 2 es líder técnico del proyecto.

Tabla 6: Costos de recursos humanos de la empresa de retail

Equipo de proyecto	Días laborales	Cantidad horas / día	Cantidad horas laboradas	Costo hora - hombre	Costo total
Líder del proyecto	50	8	400	S/85.00	S/34,000.00
Líder técnico del proyecto	50	8	400	S/56.00	S/22,400.00
Subtotal					S/56,400.00

Fuente: Elaboración de autores

b. Costos de software

Se da a conocer los costos de software requeridos para la culminación del proyecto, que son asumidos por la empresa consultora (Ver tabla 7).

Tabla 7: Costos de software de la empresa consultora

Software	Cantidad	Costo unitario (S/.)	Costo total (S/.)
CA Privileged Access Manager	2	S/44,744.00	S/89,488.00
Ofimática, MS Office 2013	2	S/50.00	S/100.00
Vmware Workstation	2	S/35.00	S/70.00
Subtotal			S/89,658.00

Fuente: Elaboración de autores

Se da a conocer los costos de software requeridos para la culminación del proyecto en base a precios del mercado, que son asumidos por la empresa de retail (Ver tabla 8).

Tabla 8: Costos de software de la empresa de retail

Software	Cantidad	Costo unitario (S/.)	Costo total (S/.)
Repositorio para grabación de sesiones (*)	2	S/0.00	S/0.00
Plataforma de virtualización	1	S/6,127.94	S/6,127.94
Cuentas privilegiadas (*)	300	S/0.00	S/0.00
Microsoft Active Directory (Directorio activo)	1	S/3,285.36	S/3,285.36
Subtotal			S/9,413.30

Fuente: Elaboración de autores

(*) El repositorio para grabación de sesiones utilizará recursos del servidor *jump server* y las cuentas privilegiadas serán 2 por cada dispositivo custodiado.

c. Costos de hardware

Se da a conocer los costos de hardware requeridos para la culminación del proyecto, que son asumidos por la empresa consultora (Ver tabla 9).

Tabla 9: Costos de hardware de la empresa consultora

Hardware	Cantidad	Costo unitario	Costo total
Laptop Personal (*)	2	S/ 550.00	S/1100.00
Comunicación (Cable de red)	2	S/ 3.50	S/.7.00
Impresora (*)	1	S/ 330.00	S/330.00
Subtotal			S/1,437.00

Fuente: Elaboración de autores

(*) los precios que se muestran son el resultado de haber aplicado la depreciación lineal, la laptop tiene 3 años de uso, su costo real es S/ 2,200.00 soles c/u, mientras que la impresora tiene 2 años de uso y su costo es de S/ 660.00 soles, la depreciación según ley le corresponde el 25 % por año.

Se da a conocer el costo de hardware requerido para la culminación del proyecto en base a precios del mercado, que son asumidos por la empresa de retail (Ver tabla 10).

Tabla 10: Costos de hardware de la empresa de retail

Hardware	Cantidad	Costo unitario	Costo total
Servidores (*)	2	S/.9,500.00	S/19,000.00
Subtotal			S/19,000.00

Fuente: Elaboración de autores

(*) El servidor en mención por la virtualización contiene el servidor de *jump server* y los dos servidores para CA PAM.

d. Costo total

A continuación, se da a conocer el costo total del proyecto, que es asumido por la empresa consultora para el desarrollo del mismo (Ver tabla 11).

Tabla 11: Costo total de la empresa consultora

Recurso	Costo
Recursos humanos	S/13,184.00
Software	S/89,658.00
Hardware	S/1,437.00
Total	S/104,279.00

Fuente: Elaboración de autores

A continuación, se da a conocer el total del costo hundido y el costo de los recursos humanos (cliente 1 y cliente 2) que es asumido por la empresa de retail (Ver tabla 12).

Tabla 12: Costo total de la empresa de retail

Recurso	Costo
Recursos humanos	S/56,400.00
Software	S/9,413.30
Hardware	S/19,000.00
Total	S/84,813.30

Fuente: Elaboración de autores

3.1.5 Cronograma.

A continuación, se describirá las actividades principales de cada etapa y se dará a conocer el responsable de cada actividad, teniendo en cuenta que se definió como LC a Lucía Contreras y RV a Roberto Vega (Ver Tabla 13).

Se anexa el diagrama de Gantt para tener una mejor facilidad y cómoda visualización de las actividades establecidas en el proyecto (Ver Anexo 1).

Tabla 13: Cronograma del proyecto

Nombre de tarea	Duración	Comienzo	Fin	Nombres de los recursos
IMPLEMENTACIÓN DE UN SIST. DE GEST. DE IDENT. PARA EL CONTROL DE ACCESO PRIV. EN UNA EMPRESA DE RETAIL	**52.25 días**	**mar 7/08/18**	**jue 18/10/18**	
ETAPA PLANIFICAR	**9 días**	**mar 7/08/18**	**lun 20/08/18**	
FASE PLANIFICACIÓN	**6 días**	**mar 7/08/18**	**mié 15/08/18**	
Definición de Prerrequisitos	1 día	mar 7/08/18	mié 8/08/18	LC
Validación de objetivos y requerimientos	0.5 días	mié 8/08/18	mié 8/08/18	LC
Definición del cronograma de actividades	1 día	jue 9/08/18	jue 9/08/18	LC
Kick-Off / WorkShop	1 día	vie 10/08/18	vie 10/08/18	LC;MS Office[1]
Elaboración del Plan de Implementación del proyecto	2 días	lun 13/08/18	mar 14/08/18	LC;MS Office[1]
Hito: Plan de implementación entregado	0 días	mar 14/08/18	mar 14/08/18	
Revisión del Plan de Implementación	0.5 días	mié 15/08/18	mié 15/08/18	Cliente 1;Cliente 2; LC
Hito: Plan de implementación aprobado	0 días	mié 15/08/18	mié 15/08/18	
FASE SOPORTE	**3 días**	**mié 15/08/18**	**lun 20/08/18**	
Documento de Diseño y Arquitecutra (Draft)	1 día	mié 15/08/18	jue 16/08/18	LC;RV
Revisión de Documento de Diseño y Arquitectura (Draft) y afinaciones	1 día	jue 16/08/18	vie 17/08/18	LC;Cliente 2

Hito: Documento de diseño y arquitectura de solución CA PAM	0 días	vie 17/08/18	vie 17/08/18	
Levantamiento y análisis de información	**1 día**	**vie 17/08/18**	**lun 20/08/18**	
Definición y revisión de Endpoints y cuentas privilegiadas	0.5 días	vie 17/08/18	vie 17/08/18	Cliente 2;LC; Ova CA PAM[0]
Revisión de información del flujo de trabajo de procesos asociados a la Gestión de accesos de usuarios privilegiados	0.5 días	lun 20/08/18	lun 20/08/18	LC;RV

Nombre de tarea	Duración	Comienzo	Fin	Nombres de los recursos
ETAPA HACER	**34.5 días**	**lun 20/08/18**	**vie 5/10/18**	
FASE OPERACIÓN	**34.5 días**	**lun 20/08/18**	**vie 5/10/18**	
Elaboración del documento de levantamiento de información	1 día	lun 20/08/18	mar 21/08/18	RV
Implementación: Módulo de Usuarios Privilegiados: CA PAM	**33.5 días**	**mar 21/08/18**	**vie 5/10/18**	
Instalación y configuración de los componentes de la solución CA Privileged Access Manager	**3 días**	**mar 21/08/18**	**vie 24/08/18**	
Revisión de entrega de requerimientos de HW/SW y accesos	0.5 días	mar 21/08/18	mar 21/08/18	LC;MS Office[1]
Instalación de 02 CA PAM Virtual Appliance en modo de Alta disponibilidad	2 días	mié 22/08/18	jue 23/08/18	FQDN Virtual IP[1]; LC; Ova CA PAM[1]; Vmware ESXI[1]
Integración con AD, Integración con Correo (Notificaciones)	0.5 días	vie 24/08/18	vie 24/08/18	LC;Ova CA PAM[1]
Despliegue Ambiente CERTIFICACÍON	**11 días**	**vie 24/08/18**	**lun 10/09/18**	
Definición y configuración de (min 01 Endpoints de win, Unix, Linux, y 02 dispositivos de comunicación, 02 bd)	2 días	vie 24/08/18	mar 28/08/18	Ova CA PAM[1];RV
Definición de Cuentas Privilegiadas (hasta 02 cuentas privilegiadas por endpoint)	1 día	mar 28/08/18	mié 29/08/18	MS Office[1];RV
Desarrollo de hasta 10 RDP Applications (TOAD for Oracle, Cliente CheckPoint, Equipos de Seguridad)	3 días	mié 29/08/18	lun 3/09/18	LC;Ova CA PAM[1]
Configuración de Flujos Básicos de Aprobación (hasta 03)	2 días	lun 3/09/18	mié 5/09/18	Ova CA PAM[1];RV
Configuración de Políticas de Grabación de Sesiones y Filtrado de Comandos	0.5 días	mié 5/09/18	mié 5/09/18	RV;Ova CA PAM[1]
Configuración de Roles Administrativos (hasta 02)	0.5 días	jue 6/09/18	jue 6/09/18	Ova CA PAM[1]; Repositorio de grabaciones[1]
Configuración de Políticas de Acceso a Cuentas Privilegiadas (hasta 04	1 día	jue 6/09/18	vie 7/09/18	Ova CA PAM[1];RV
Pruebas funcionales internas	1 día	vie 7/09/18	lun 10/09/18	LC;Ova CA PAM[1]; RV
Despliegue Ambiente PRODUCCIÓN	**19.5 días**	**lun 10/09/18**	**vie 5/10/18**	
Definición y despliegue de PAM sobre 150 endpoints (Tipos de endpoints que fueron probados en Ambiente Certificación)	4 días	lun 10/09/18	vie 14/09/18	Ova CA PAM[1];RV
Definición de gestión de cuentas privilegiadas (hasta 02 cuentas privilegiadas por endpoint)	2 días	vie 14/09/18	mar 18/09/18	LC;Ova CA PAM[1]
Afinar 10 RDP Application	2 días	mar 18/09/18	jue 20/09/18	LC;Ova CA PAM[1]
Configuración de Flujos Básicos de Aprobación (hasta 03)	1 día	jue 20/09/18	vie 21/09/18	LC;Ova CA PAM[1]
Configuración de políticas de grabación de sesiones y filtrado de comandos	1 día	vie 21/09/18	lun 24/09/18	LC; Repositorio de
Configuración de perfiles de acceso a cuentas privilegiadas (hasta 04)	4 días	lun 24/09/18	vie 28/09/18	LC;Ova CA PAM[1]
Configuración de polítcas de acceso a cuentas privilegiadas (hasta 04)	3 días	vie 28/09/18	mié 3/10/18	LC;Ova CA PAM[1]
Elaboración entregable Documento de configuración de equipos	1 día	mié 3/10/18	jue 4/10/18	MS Office[1];RV
Entrega y revisión del Plan de prueba	0.5 días	jue 4/10/18	jue 4/10/18	Cliente 1;LC;RV
Correcciones y ajustes acordes a los hallazgos de las pruebas	1 día	vie 5/10/18	vie 5/10/18	LC;Ova CA PAM[1]
Hito: Plan de pruebas de CA PAM aprobado	0 días	vie 5/10/18	vie 5/10/18	

ETAPA VERIFICAR	**4 días**	**lun 8/10/18**	**jue 11/10/18**	
FASE EVALUACIÓN DEL DESEMPEÑO	**4 días**	**lun 8/10/18**	**jue 11/10/18**	
Pruebas Funcionales	1 día	lun 8/10/18	lun 8/10/18	LC;Ova CA PAM[1]; RV
Checklist funcional de la solución implementada	1 día	mar 9/10/18	mar 9/10/18	LC;MS Office[1];RV
Elaboración entregable Resultado de la implementación de CA PAM	1 día	mié 10/10/18	mié 10/10/18	MS Office[1];RV
Ejecución del plan de de pruebas	1 día	jue 11/10/18	jue 11/10/18	Cliente 1;LC; Ova CA PAM[1]
Hito: solución CA PAM implementada en Amb. Producción	0 días	jue 11/10/18	jue 11/10/18	
ETAPA ACTUAR	**4.75 días**	**vie 12/10/18**	**jue 18/10/18**	
FASE MEJORA	**4.75 días**	**vie 12/10/18**	**jue 18/10/18**	
Elaboración entregable Levantamiento de observaciones de la implementación	1 día	vie 12/10/18	vie 12/10/18	MS Office[1];RV
Elaboración entregable Guía de usuario	1 día	lun 15/10/18	lun 15/10/18	MS Office[1];RV
Elaboración entregable Plan de recuperación de servicio	1 día	mar 16/10/18	mar 16/10/18	LC;MS Office[1]
Elaboración entregable Guía de proveedor	1 día	mié 17/10/18	mié 17/10/18	MS Office[1];RV
Evaluación post-proyecto	0.5 días	jue 18/10/18	jue 18/10/18	Cliente 1;Cliente 2; LC
Presentación del servicio	0.25 días	jue 18/10/18	jue 18/10/18	Cliente 1;Cliente 2; LC
Cierre de proyecto	0 días	jue 18/10/18	jue 18/10/18	

Fuente: Elaboración de autores

3.2 Método

Para la presente tesis se ha empleado el método “Plan-Do-Check-Act” (PDCA) recomendado por la ISO/IEC 27001, el cual es un Sistema de Gestión de Seguridad de Información.

El método (PDCA) también conocido como Ciclo de Mejora Continua o Circulo Deming describe las cuatro etapas importantes que se deben llevar a cabo de forma sistemática, para así lograr un progreso continuo, aumentar la calidad, tener una gestión más segura, mitigar fallas en la gestión e incrementar la eficiencia y la eficacia de la organización (ISO 27001, 2005).

En la siguiente tabla se muestran las fases de la ISO/IEC 27001:2013 que son incluidas en cada una de las etapas del ciclo PDCA. Además, se realiza un listado de los documentos a presentar en cada una ellas (Ver Tabla 14).

Tabla 14: El ciclo PDCA

Etapa	Fases	Entregables
PLANIFICAR	• Planificación • Soporte	• Plan de implementación del proyecto • Documento de diseño y arquitectura
HACER	• Operación	• Levantamiento de Información • Documento de configuración de equipos • Plan de pruebas
VERIFICAR	• Evaluación del desempeño.	• Resultado de la implementación de CA PAM • Resultado de plan de prueba
ACTUAR	• Mejora|	• Levantamiento de observaciones de la implementación • Guía de usuario • Plan de recuperación del servicio • Guía de proveedor

Fuente: Elaboración de autores

Se procede a realizar la descripción del método PDCA de cada una de las etapas y las fases de la ISO/IEC 27001:2013.

- **Etapa 1: Planificar**

Primero se debe analizar y estudiar el proceso de control de seguridad que tiene implementado la organización, para determinar qué cambios se pueden mejorar y en qué forma se debe realizar. En esta etapa se definen 2 fases que serán descritas a continuación para tener un mejor entendimiento en lo que consisten (ISO/IEC 27001, 2005).

- **Fase a. Planificación**

El objetivo de esta primera fase es realizar el planteamiento del problema bien definido, además de comprender el alcance del proyecto de la implementación de la solución CA PAM y las tareas asignadas a los miembros del equipo (ISO/IEC 27001, 2013).

El plan de implementación del proyecto es el documento que se tiene como entregable de esta primera fase, el desarrollo de este está compuesto por los siguientes temas:

- Problemática de la empresa de retail.
- Situación actual de la seguridad en la administración de acceso privilegiado.
- Solución propuesta para la administración de acceso privilegiado.
- Alcance de la solución propuesta.
- Estrategia de la implementación.
- Requerimientos del personal.
- Capacitación al personal.
- Impacto de la implementación.
- Gestión del riesgo del proyecto.
- Suposiciones y restricciones.

- **Fase b. Soporte**

El objetivo que se describe en esta fase es definir el diseño y la arquitectura de la empresa de retail y tener como entregable el documento de diseño y arquitectura (ISO/IEC 27001, 2013).

El documento mencionado está compuesto por los siguientes temas:

- Diseño de la solución.
- Requerimiento técnico.
- Equipos custodiados.
- Estrategia de Transición.
- Puertos de los componentes de la solución.
- Casos de uso de la solución.
- Impacto de la solución.

- **Etapa 2: Hacer**

Se realiza el levantamiento de información para continuar con la implementación del SGSI. Esta etapa es la más larga considerada en tiempo y complejidad que las demás, ya que antes de implementar el sistema en producción y generar los cambios a gran escala, se trabaja en un ambiente de certificación para comprobar el funcionamiento. Con el fin de evitar que los errores sucedan cuando el sistema se encuentre en un ambiente de producción (ISO/IEC 27001, 2005).

- **Fase c. Operación**

En esta fase se procede a realizar la implementación del SGSI, teniendo como precedente los requerimientos establecidos en la primera etapa del ciclo PDCA.

En el desarrollo de esta fase se tiene como entregable el levantamiento de información y documento de configuración de equipos (ISO/IEC 27001, 2013).

El documento de levantamiento de información abarca las siguientes áreas.

- Área de Base de Datos.
- Área de seguridad de la información.
- Área de redes.

El documento de configuración de equipos está compuesto por los siguientes temas:

- La preparación de la solución CA PAM.
- Gestión de identidades privilegiadas en dispositivos Web.

- **Etapa 3: Verificar**

Luego de haber culminado con la implementación del SGSI, se deja un período de tiempo para verificar su correcto funcionamiento. Si el resultado de la implementación no cumple las expectativas iniciales, deben ser modificadas

con el fin de cumplir con los objetivos propuestos, se tendrán que identificar las fallas y errores que hayan ocurrido durante este período (ISO/IEC 27001, 2005).

- **Fase d. Evaluación de desempeño**

Se tiene como objetivo evaluar el desempeño del funcionamiento del SGSI implementado, el cual consiste en determinar las fallas y errores que estos puedan presentar luego de la implementación de la solución (ISO/IEC 27001, 2013).

En el desarrollo de esta fase se tiene como entregable el resultado de la implementación de CA PAM en las áreas ya antes mencionadas.

- **Etapa 4: Actuar**

La última etapa del método PDCA es donde se miden los resultados esperados en base a los objetivos propuestos. En caso de no llegar a ejecutar esta etapa no se tendrá garantía de que el SGSI implementado obtenga buenos resultados. Asimismo, aquí es donde se abordará la acción de establecer acciones correctivas que mitiguen el riesgo de un desempeño no satisfactorio de la solución afectando a la empresa (ISO/IEC 27001, 2005).

La implementación no siempre es satisfactoria ya que para cumplir con el objetivo propuesto es necesario realizar correcciones en paralelo a la etapa anterior.

- **Fase e. Mejora**

Consiste en realizar acciones para controlar y corregir los errores que se presenten luego de la implementación. Con la finalidad de que se cumplan los objetivos propuestos (ISO/IEC 27001, 2013). En el desarrollo de esta fase se tiene como entregables el levantamiento de observaciones de la implementación, guía de usuario, guía de proveedor y plan de recuperación del servicio.

El documento levantamiento de observaciones de la implementación fue realizada en las 3 áreas ya mencionado en la primera fase.

- Levantamiento de observaciones en el área de base de datos.
- Levantamiento de información en el área de Seguridad de redes.
- Levantamiento de información en el área de redes.

En el siguiente capítulo se describe el desarrollo de la propuesta establecida como solución bajo el enfoque del método PDCA y la ISO/IEC 27001:2013.

CAPÍTULO IV
DESARROLLO DEL PROYECTO

En el presente capítulo se desarrolla la implementación del sistema de gestión de identidades privilegiadas en una empresa de retail, en base a las etapas de la metodología PDCA teniendo en consideración las fases del ISO/IEC 27001:2013 e incluido los entregables que abarca cada fase.

Por acuerdo de confidencialidad no será posible hacer mención los nombres de los clientes de la empresa de retail, por lo que se le llamará al jefe del departamento de departamento de redes, telecomunicaciones y base de datos (DRTBD) como cliente 1, y al especialista de DRTBD como cliente 2.

4.1 Etapa Planificar

A continuación, se da a conocer la situación actual de la empresa y los componentes de la solución para determinar el impacto que tendrá la empresa luego de la implementación.

4.1.1 Fase de planificación.

A continuación, el entregable de la fase de planificación “Plan de implementación del proyecto” y el entregable de la fase de soporte “Documento de diseño y arquitectura” de la solución CA PAM.

- **ENTREGABLE: Plan De Implementación del Proyecto**

El entregable Plan de Implementación del Proyecto deberá ser firmado por el cliente 1 y el cliente 2 como demostración del compromiso con el proyecto, así como la aceptación y comprensión de los objetivos.

a. Situación de la empresa de retail

La empresa de retail en la actualidad tiene una inadecuada gestión de identidades privilegiadas de los administradores de las plataformas de TI, trayendo como consecuencia el descontrol de las actividades realizadas por los usuarios administradores de los activos de TI. La ejecución de procesos con privilegios en el sistema está dentro de los errores más peligrosos y que no se tiene la trazabilidad de lo que realizan los administradores. Las cuentas de súper usuario manejados en el área de base de datos, seguridad de la información y de redes, como en el caso de sistemas operativos (*root* y *administrador*), base de datos, aplicaciones e infraestructura, ha generado una ardua tarea de manejo de la gestión de estas cuentas dado el número creciente de dispositivos y complejidad tecnológica, lo que implica un alto riesgo a la manipulación de la información confidencial. Debido a la gran cantidad de cuentas privilegiadas que maneja cada empleado, muchos de ellos registran sus cuentas en una hoja de cálculo, bloc de notas, post-it, entre otros medios, por lo que genera un alto riesgo de que esas credenciales lo obtenga un usuario no autorizado, pudiendo este extraer información de los activos de TI sin ser autorizado.

Por otro lado, la empresa de retail no cuenta con un proceso eficiente de aprobación de acceso a dispositivos críticos, ya que la comunicación es mediante correo o de forma verbal con el jefe de área, y además puede ocurrir el caso que el administrador realice la configuración en los ambientes de producción sin informar ya que este tiene control de las credenciales con privilegios, este escenario aduce a que no se tenga control de cambios realizados en los dispositivos de producción.

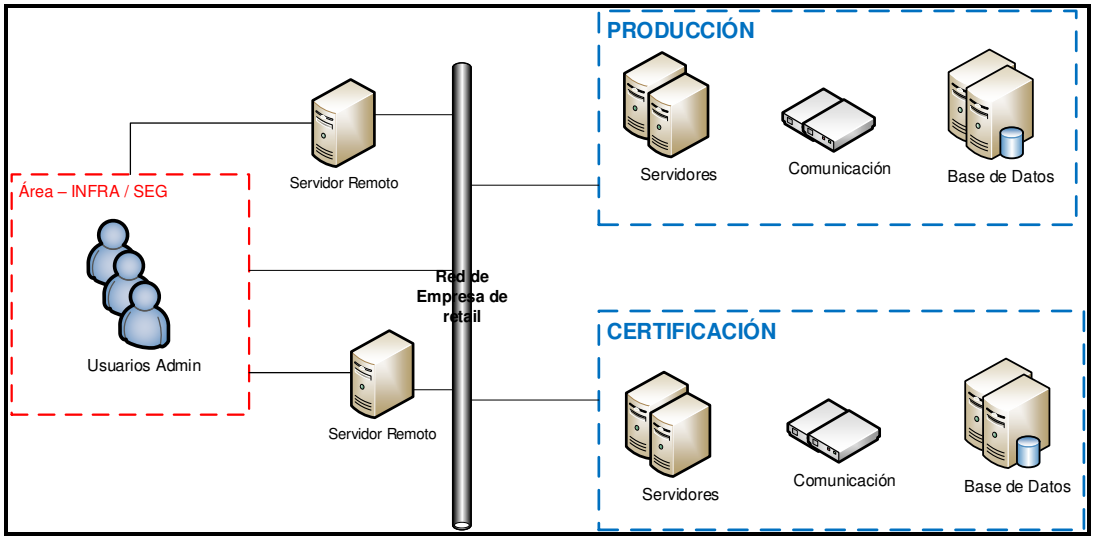
b. Situación Actual

En la actualidad, ocurren muchos casos de robo de información y de gran impacto en las empresas, tanto en prestigio como económicamente, y muchos de estos casos ocurridos fueron en base al robo de credenciales, por lo que la empresa de retail requiere de una solución que permita gestionar cuentas privilegiadas y así mismo aplicar auditorías.

La empresa de retail administra gran cantidad de cuentas privilegiadas, la cual el cliente lo denomina identidades privilegiadas, la empresa cuenta con dispositivos muy críticos por lo que tiene la necesidad de contar con una solución que permita mitigar el riesgo de robo de información y/o alteración de información sin tener trazabilidad.

El siguiente diagrama explica cómo es la conexión actualmente en la empresa de retail, en la que se logra visualizar que no hay una autenticación centralizada (Ver Figura 12)

Figura 12: Situación actual de la estructura de red



Fuente: Elaboración de autores

En la siguiente tabla se da a conocer las brechas de inseguridad identificadas en la empresa de retail (Ver tabla 15).

La empresa de retail está conformada por distintos departamentos, con respecto a la especialidad de informática se llama departamento de redes, telecomunicaciones y base de datos (DRTBD), dicho departamento está conformado por las áreas de base de datos, seguridad de la información y redes. A continuación, se muestra el diagrama de la distribución de dichas áreas (Ver figura 13).

Figura 13: Diagrama de distribución de áreas del DRTBD

Fuente: Elaboración de autores

Tabla 15: Requerimientos del cliente

Referencia – Requerimiento de la Solución	Brecha / Issue
RS – 01 – Mejora Seguridad y Cumplimiento	**UNIX:** - Usuarios con acceso privilegiados podrían crear backdoor (en español puerta trasera, secuencia especial que es utilizado para evitar sistemas de seguridad) en los sistemas para obtener acceso privilegiado. - Cuando el usuario es terminado, los backdoors permanecen y cualquiera podría explotarlos. - Ejecución de comandos sin filtrado. **WINDOWS:** - Individuos maliciosos quienes comprometen cuentas privilegiadas, obtendrían acceso administrativo a controladores de dominio y vulnerar la seguridad de la red. - Estos individuos podrían ser usuarios no autorizados quienes obtuvieron contraseñas administrativas, o ellos podrían ser legítimos administradores quienes están coaccionados. - Usuarios con acceso administrativos local podrían descargar-instalar software como necesiten. Esto podría introducir malware-virus en la red.

Referencia – Requerimiento de la Solución	Brecha / Issue
	ORACLE - Sin registro de sesiones - Cuentas personales con acceso administrativo, sin restricciones. - Permitiendo realizar alteraciones sobre la BD no autorizadas o sensibles, en caso las cuentas privilegiadas cayeran sobre personas mal intencionadas. **WEB PORTAL:** - Usuarios con acceso privilegiado en portales web podrían corromper configuraciones dentro de la aplicación web. - Obtener datos sensibles de la organización y estos compartirlos o comerciarlos.
RS – 02 – Facilidad de Gestión de Cuentas Privilegiadas	**Situación Actual:** - La empresa de retail no cuenta con herramientas de administración de cuentas privilegiadas de sus diferentes plataformas. - No cuenta con gestión centralizada de cuentas privilegiadas.
RS – 03 - Gestión Centralizada	**Situación Actual:** - No hay solución para realizar gestión centralizada de las cuentas privilegiadas a través de la empresa de retail y sus administradores. - No hay portal de autoservicio de cuentas privilegiadas para check in/out. - No hay flujos de trabajo automatizados para otorgar acceso a cuentas privilegiadas.
RS – 04 – Rendición de Cuentas	**Situación Actual:** - No hay registro de quién, por qué y cómo usan los accesos privilegiados. - Ausencia de rendición de cuentas es identificada como un problema de cumplimientos.
RS – 05 – Reportes	**Situación Actual:** - No hay reportes disponibles que puedan consolidar todas las cuentas privilegiadas y su uso dentro del ambiente de la empresa de retail. - Ausencia de reporte de accesos privilegiados.

Fuentes: Elaboración de autores

c. Solución propuesta

Privileged Access Manager

CA PAM es una plataforma de Administración de Acceso e Identidad Privilegiada que permite proteger y administrar los sistemas donde sea que residan, de data centers tradicionales a plataformas de nube pública y privada virtualizados.

CA PAM permite a los clientes reforzar con un exhaustivo e integrado conjunto de controles a través de un sistema de administración de políticas unificadas que hace esto fácil para la configuración inicial y durante el desarrollo de las tareas de administración de políticas.

El servicio de implementación de CA PAM está diseñado para ser desplegado en el ambiente de Tecnología de Información (TI) de la empresa para ayudar a asegurar el acceso a identidades privilegiadas basado en roles y responsabilidad a través de múltiples plataformas (Unix, Windows, BD, Portales Web, Dispositivos de red), consolidar la gestión de identidades privilegiadas con una única interfaz de usuario y administrar las solicitudes de acceso privilegiado y contraseñas.

Esta solución también provee la habilidad para automatizar el balanceo de carga y escuchar las consultas “https” a través de un VIP configurado.

Tras el análisis de la situación de la empresa, se le recomendó optar por la licencia que cuenta con un máximo de 25 usuarios privilegiados como base limitada, y dispositivos con identidades privilegiadas ilimitadas.

Arquitectura de la solución

A continuación, se describirá de manera resumida la estructura de la solución de Gestión de Identidades Privilegiadas, así también, los componentes esenciales para su implementación.

La solución por implementar es un *virtual appliance* (vApp) en la versión 3.2 y está embebido con los siguientes sistemas y/o aplicaciones:

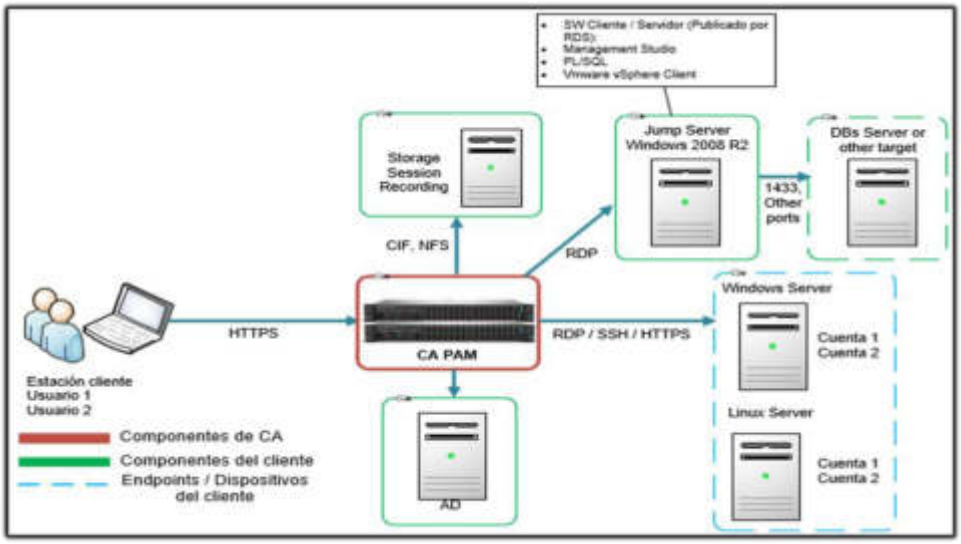
- Sistema Operativo
- Servidor de Aplicaciones
- Base de Datos

Se tiene la función de *single sign-on,* que permite ocultar las credenciales a los usuarios mientras se provee acceso. Esto significa que no es necesario que los usuarios privilegiados sepan las credenciales de los sistemas de utiliza sino solo es necesario que sepa su credencial del CA PAM.

Se describe a continuación el diagrama de despliegue de la solución de CA PAM; así también la descripción de sus componentes y el protocolo de comunicación (Ver figura 14).

Nota: La Arquitectura de solución propuesta se detallará en el documento de Diseño y Arquitectura.

Figura 14: Diagrama de despliegue de la solución



Fuente: Elaboración de autores

A continuación, se detalla los componentes planteados en el diagrama de despliegue de la solución (Ver tabla 16).

Tabla 16: Componentes del despliegue de la solución

Gestión de Identidades Privilegiadas		
CA Privileged Access Manager	CA Technologies	• 02 virtual *appliance* que trabajarán en Alta Disponibilidad. • Versión: CA PAM 3.2
Recurso Compartido	Infraestructura Cliente	• Recurso con 512 Gb de almacenamiento para las grabaciones de sesión.
Jump Server	Infraestructura Cliente	• Terminal *Services* Windows que permitirá acceder a sistemas Cliente/Servidor.
Dispositivos	Infraestructura Cliente	• Las cuentas privilegiadas de los dispositivos serán custodiadas por CA PAM.
Microsoft Active Directory	Infraestructura Cliente	• Repositorio de usuarios que accederán a CA PAM.

Fuente: Elaboración de autores

A continuación, la solución planteada ante el requerimiento del cliente es la siguiente (Ver tabla 17).

Tabla 17: Solución propuesta

Resultado de Solución Cruce de Referencia	Estado planeado "A ser"
RS-01 – Mejora de Seguridad y Cumplimiento	• La solución estará configurada para almacenar credenciales de cuentas privilegiadas gestionadas. • CA PAM encriptará las credenciales de cuentas privilegiadas antes de almacenarlas. La solución usará un robusto kernel de criptografía de 256-bit para seguridad máxima. • La solución administrará rotación de credenciales de cuentas privilegiadas acorde las políticas configuradas. • Solución puede proveer credenciales para cuentas privilegiadas con o sin aprobaciones. • Cuando un usuario inicia sesión en CA PAM, usuario verá las cuentas privilegiadas acorde sus funciones. • Los accesos privilegiados pueden ser proveído basado en "*Need to Know*" sin revelar las credenciales al usuario final, así limita el reusó de las credenciales.
RS-02 – Facilidad de Gestión de Cuentas Privilegiada	• La solución puede definir que grupos (AD) estarán capaces de acceder a las credenciales almacenada dentro de la solución. • La solución puede enviar notificaciones vía correo a propietarios de cuentas configuradas para aprobar/denegar la solicitud para acceder a las cuentas privilegiadas. Solo después de la aprobación de la solicitud, la solución proveerá al usuario el acceso a la cuenta autorizada. • Para acceso de usuarios a cuentas críticas, solución puede proveer la capacidad de iniciar sesión directamente al dispositivo o aplicación objetivo como la cuenta privilegiada. Esto evitará la necesidad de compartir contraseñas con los usuarios o accesos privilegiados permanentes. • Las contraseñas de las cuentas privilegiadas serán cambiadas cada 60 días.

RS-03 – Gestión Centralizada	La solución puede proveer un portal centralizado para: ✓ Importar LDAP/AD grupos ✓ Configurar dispositivos Windows ✓ Configurar dispositivos Unix ✓ Configurar dispositivos Web Portal ✓ Configurar dispositivos de red ✓ Configurar cuentas privilegiadas ✓ Configurar "*Password Composition Policies*" ✓ Configurar "*Password View Policies*" ✓ Configurar políticas de acceso ✓ Generar reportes ✓ rotación de contraseñas a dispositivos administrador a dispositivos CLI ✓ Reproducir sesiones grabadas
RS-04 - Rendición de Cuentas	CA PAM auditará quién, cuándo y cómo se usa el acceso privilegiado. Toda la información de auditoría será registrada y asegurado dentro del appliance.
RS-05 – Reportes	Reportes de uso de cuentas privilegiadas puede ser generado de la consola central de gestión (interfaz web CA PAM y cliente).

Fuente: Elaboración de autores

Infraestructura del cliente

A continuación, se detalla la infraestructura requerida para la implementación de la solución de CA PAM.

Hardware y software

Los recursos de hardware y software que permitirán desplegar y soportar la solución propuesta son los siguientes (Ver tabla 3 y 4).

Instalaciones

A continuación, se describe algunos puntos referentes a las facilidades de las instalaciones físicas necesarias para la implementación de la solución de Gestión de Identidades Privilegiadas en la empresa de retail (Ver tabla 18).

Tabla 18: Requerimientos de instalaciones

Ítem	Observaciones
Espacio de Trabajo	Espacio de trabajo para 3 personas con disponibilidad en el siguiente horario: • Lunes a viernes (09:00 – 19:00).
Internet	Conexión a internet para: • Consultas en la web del fabricante. • Apertura de issues en la web del fabricante. • Comunidad de expertos del fabricante e investigación.
Red interna	Conexión de laptops a la red interna de la empresa de retail para: • Conexión a la infraestructura CA PAM. • Conexión a Dispositivos de Ambiente CERTIFICACIÓN. • Conexión a Dispositivos de Ambiente PRODUCCIÓN. • Ejecutar pruebas. • Documentación.
Sala de Reunión	Para: • Establecer reuniones requeridas durante ejecución del proyecto. • Transferencia de conocimiento. • Capacitación a usuarios.

Ítem	Observaciones
Acceso Remoto	Para: • Continuar con actividades del proyecto ante problemas de disponibilidad de las instalaciones o del proveedor de manera presencial. • Poder dar seguimiento a casos activos con el fabricante fuera de horario.

Fuente: Elaboración de autores

Actores de la solución

A continuación, los actores involucrados que interactuarán con la solución CA PAM (Ver tabla 19).

Tabla 19: Actores de la solución

Actor (Rol)	Descripción	Departamento	Uso de Sistemas	Expectativa de Uso con Nueva Solución
Usuario (Con Acceso Privilegiado)	Este actor requiere el uso de una cuenta privilegiada.	DRTBD	Este individuo utiliza la cuenta privilegiada en los dispositivos: Windows, Unix, BD, Web Portal.	Este individuo iniciará sesión en la consola administrativa de CA PAM. Basado en su rol, el tendrá acceso a dispositivos o deberá solicitar acceso. Las políticas de acceso serán aplicadas al individuo o grupo del individuo.
Operador de acceso de cuenta privilegiada	Este actor es responsable de provisionar y configurar las cuentas privilegiadas.	DRTBD	Este actor provisiona acceso privilegiados a nivel de OS.	Serán responsables para configurar las cuentas privilegiadas.
Administrador de Solución	Individuo responsable de configurar controles de seguridad usando PAM.	LOS AUTORES	Este actor configuraría y gestionaría los controles de seguridad dentro del ambiente.	Los autores se encargarán de administrar CA PAM.
Dispositivo Objetivo	Dispositivos de Unix, Windows, Web Portal y Cliente/Servidor.	DRTBD	Estos son los dispositivos que los usuarios acceden para realizar sus tareas según roles y responsabilidades.	Estos dispositivos continuarán dando servicios en el ambiente de la empresa de retail, la diferencia es que la solución proveerá un mecanismo centralizado para facilitar el acceso, y así proveer un único lugar para gestionar cuentas privilegiadas a través del ambiente.
Solución de Seguridad – CA PAM	Esta solución permite gestionar y controlar los accesos privilegiados.	DRTBD	Actualmente no existe.	Usuarios autorizados accederán a los dispositivos a través de la solución PAM. Administradores de seguridad iniciarán sesión en la consola central para configurar acceso privilegiado.

Fuente: Elaboración de autores

d. Alcance

Los recursos identificados por la empresa de retail son 150 dispositivos que se tiene que configurar en la solución de *Privileged Access Manager* para la gestión de cuentas privilegiadas son el siguiente (Ver tabla 20).

Tabla 20: Alcance de aplicativos a incorporar a CA PAM

Aplicación	Método de Acceso	Cantidad
Dispositivos de redes	SSH	44
Dispositivos de seguridad	SSH	24
Linux	SSH	5
Windows Server	RDP	36
BD – ORACLE	App C/S	25
WEB	HTTPS	16
TOTAL		150

Fuente: Elaboración de autores

Nota: Los recursos de Base de Datos residen en los servidores Windows y Linux ya listados.

e. Documentación

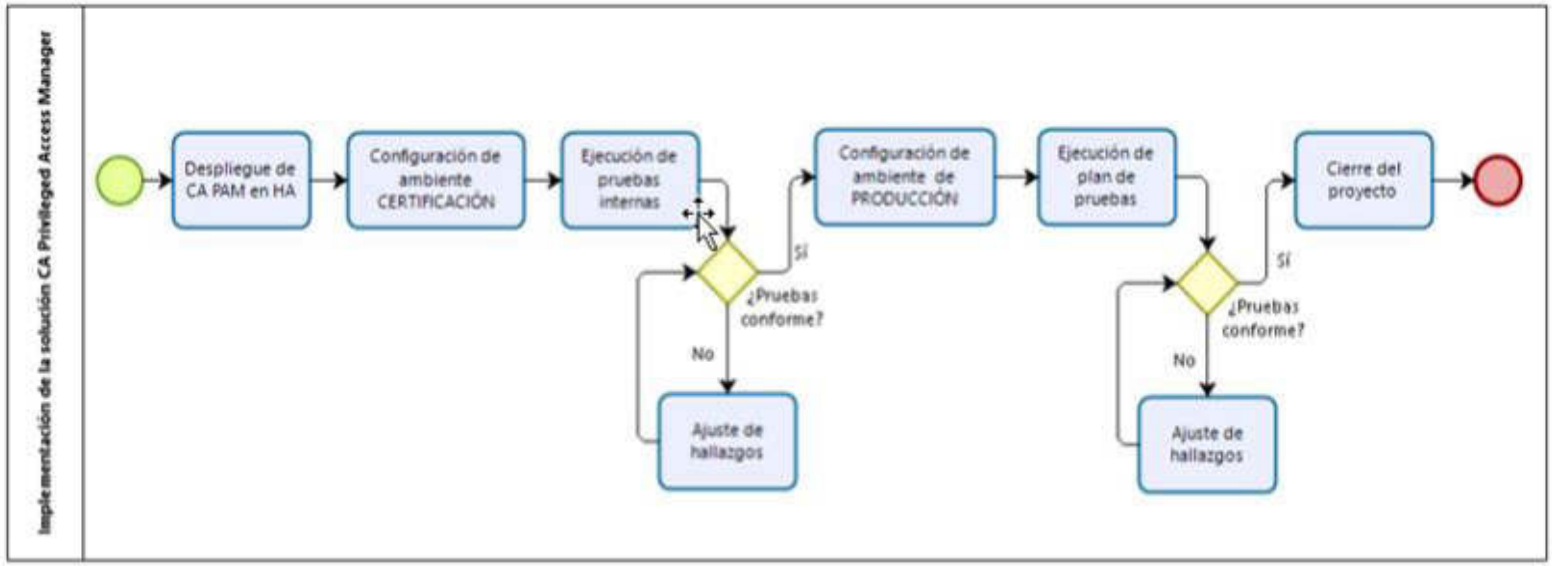
En el cuadro se describe los documentos que serán desarrollados o consultados durante la ejecución del proyecto **(Ver tabla 10).**

f. Estrategia de implementación

Estrategia de transición

A continuación, se muestra las actividades a realizar para la implementación de la solución *Privileged Access Manager* (Ver Figura 15).

Figura 15: Estrategia del despliegue



Fuente: Elaboración de autores

Los dispositivos serán distribuidos de la siguiente forma de las cuales se configurará 2 cuentas por cada dispositivo (Ver tabla 21).

Tabla 21: Dispositivos a configurar en la solución

Ambiente	*Endpoints* a Proteger
Certificación	• 2 dispositivo Windows. • 2 dispositivo Unix. • 2 dispositivo BD – Oracle.
Producción	• RDP: 36 dispositivos Windows. • SSH: 73 dispositivos Linux. • HTTPS: 16 páginas web. • App C/S: 25 BD – Oracle.

Fuente: Elaboración de autores

Estrategia de Pruebas

Se propondrá una estrategia de pruebas que permita validar la correcta operación de las funcionalidades habilitadas en la solución de Gestión de Identidades Privilegiadas. A continuación, descripción de las actividades o tareas a realizar dentro del Plan de Pruebas (Ver tabla 22).

Tabla 22: Plan de prueba

Actividades	Descripción
Plan de Pruebas	Se elaborará documento de Plan de Pruebas con los casos de uso con aprobación de la empresa de retail para su ejecución.
	Ambiente de CERTIFICACIÓN
Pruebas Internas	El equipo de implementación validará las funcionalidades de la solución post implementación del ambiente de CERTIFICACIÓN.
	Ambiente de PRODUCCIÓN
Lista de Verificación	Revisión de funcionalidades operativas en ambiente de PRODUCCIÓN antes de ejecutar el plan de pruebas.
Ejecución de Plan de Pruebas	Post implementación de ambiente PRODUCCIÓN y aprobación de Plan de Pruebas, se procede a ejecutar los casos de uso en conjunto con la empresa de retail.

Fuente: Elaboración de autores

Nota: Las pruebas a ejecutar de la solución propuesta se detallará en el documento de Plan de Pruebas.

Adicionalmente, durante la ejecución del proyecto se consultará documentación del fabricante.

g. Requerimiento del personal

A continuación, descripción del personal requerido por parte de la empresa de retail para la implementación e integración del sistema de PAM con las plataformas de la empresa de retail (Ver tabla 23).

Tabla 23: Requerimiento del personal

Rol	Descripción
Administrador de Plataforma Windows	Personal con pericia en tecnologías Windows para cumplir con los requerimientos que se necesiten en la integración de CA PAM con plataformas Windows.
Administrador de Plataforma Linux/Unix	Personal con pericia en tecnologías Unix/Linux para cumplir con los requerimientos que se necesiten en la integración de CA PAM con plataformas Unix/Linux.
Administrador de Dispositivos de Red	Personal con conocimiento sobre los dispositivos de red que conforme la red de la empresa de retail.
Administrador de Equipos de Seguridad	Personal con conocimiento sobre los equipos de seguridad de la empresa de retail que se integraran con CA PAM.
Administrador de aplicación dentro de alcance	Personal con conocimiento sobre la aplicación a integrar con CA PAM.

Fuente: Elaboración de autores

h. Capacitación al personal

A continuación, se describirá el alcance del entrenamiento que será dirigido tanto a los usuarios que consumirán la solución propuesta como los administradores de la solución (Ver Tabla 24).

Tabla 24: Capacitación al personal

Objetivos	Descripción	Tiempo
Usuarios Finales	La capacitación se basará en la solución de CA PAM: - Acceso a las cuentas privilegiadas/dispositivos vía CA PAM.	2 sesiones de 4 horas cada una.
Administradores de la solución	La capacitación se basará en la administración de la solución CA PAM: - Arquitectura de CA PAM. - Administración de Cuentas Privilegiadas. - Aprovisionamiento de Dispositivos. - Generación de Reportes. - Visualización de Grabación de Sesiones y Logs. - Operación del Clúster.	1 sesión (4 horas).

Fuente: Elaboración de autores

i. Impacto de la implementación

La implementación de la solución CA PAM tendrá impacto sobre los usuarios administradores y sus accesos. A continuación, se describe los posibles impactos que se podrían dar post implementación (Ver Tabla 25).

Tabla 25: Impacto de la implementación

Objetivos	Impacto
Administradores de Plataformas	• No tendrán ninguna credencial privilegiada de las plataformas (Por Ejm: Windows, Linux, switch) y será gestionado por CA PAM. • Único canal de acceso a los dispositivos de la empresa de retail y será vía CA PAM. • Toda actividad realizada en los dispositivos será grabada y, además, se tendrá trazabilidad de los accesos aun utilizando cuentas compartidas. • No se podrá ejecutar comandos vía SSH que por políticas de la empresa de retail no estarán permitidos. • Cierto acceso requerirá de previa aprobación por el propietario de la aplicación o equipo de seguridad.

Objetivos	Impacto
Administradores del Sistema	• Generar respaldos periódicos de la configuración y base de datos de CA PAM. • Validar cambios de contraseña en la consola de CA PAM. • Validar notificaciones de correo de intento de transgresión de políticas que podrían llegar de CA PAM.

Fuente: Elaboración de autores

j. Gestión de riesgo del proyecto

Se detecta anticipadamente los riesgos que puedan ocurrir durante el desarrollo de la implementación de CA PAM en la empresa de retail.

Para la medición de la probabilidad que ocurra algún riesgo identificado durante la implementación de la solución, se estableció los siguientes indicadores (Ver tabla 26).

Tabla 26: Indicadores de probabilidad del suceso del riesgo

Probabilidad del riesgo	Valor del riesgo
< 10%	Muy bajo
10 – 25 %	Bajo
25 – 50 %	Moderado
50 – 75 %	Alto
> 75%	Muy alto

Fuente: Elaboración de autores

Para la medición del impacto que tendría en la implementación de la solución ante la ocurrencia de un riesgo identificado para así establecer la prioridad, se estableció los siguientes indicadores (Ver tabla 27).

Tabla 27: Indicadores de impacto del riesgo

Valor de impacto	Efecto o impacto	Prioridad
1	Catastrófico	Alta
2	Crítico	Media
3	Marginal	Baja

Fuente: Elaboración de autores

Se muestra los riesgos detectados que podría acontecerse durante la implementación de la solución CA PAM, logrando establecer la probabilidad que ocurra dicho riesgo y el impacto que este tendría (Ver tabla 28).

Tabla 28: Riesgos detectados

Riesgo	Probabilidad	Impacto	Valor de impacto	Acción	Planes de Acción	Responsable
Empleados presenten problemas de salud	7%	Demora en la ejecución del proyecto. Entrega de este fuera de tiempo.	3	Mitigar	Reorganizar al equipo de manera que exista traslado temporal de responsabilidades.	Gestor del proyecto
Falta de compromiso de los trabajadores con el proyecto	5%	Demoras en la ejecución del proyecto. Baja calidad en los resultados del proyecto.	2	Prevenir	Programar las reuniones con días anticipadas y en un horario apto para todos. Tener comunicación constante con los miembros del equipo, a su vez revisar su avance con el cronograma de trabajo.	Miembro de equipo
Algún miembro del equipo renuncie	8%	Demora en la ejecución del proyecto. Entrega de este a destiempo.	2	Mitigar	Ajustar el plan de proyecto para cualquier cambio.	Gestor del proyecto
Personal no especializado	10%	Demora en el avance de la ejecución del proyecto. Baja calidad en los resultados del proyecto.	2	Mitigar	Realizar capacitaciones, de esta manera el que conoce oriente al que le falta.	Miembro de equipo
Modificaciones en el alcance en el transcurso del proyecto.	45%	Tome mayor tiempo en el desarrollo del proyecto. El presupuesto Incremente. Se necesite más recurso humano.	1	Mitigar	Informar al cliente de los próximos pasos y de las tareas pendientes para gestionar expectativas y anticiparse. Mantener una comunicación constante con los responsables del proyecto teniendo reuniones de seguimiento.	Cliente

Riesgo	Probabilidad	Impacto	Valor de impacto	Acción	Planes de Acción	Responsable
Falta de comunicación por parte de los integrantes del grupo.	5%	Una mala implementación. Se pierde la calidad en el producto final.	2	Mitigar	Reuniones periódicas del equipo de trabajo.	Miembros del equipo
Falta de compromiso del cliente para el proyecto	30%	Se extienda el tiempo de desarrollo del proyecto. Amenaza con la continuidad del proyecto.	1	Mitigar	Validar el plan de trabajo con el cliente. Establecer el compromiso del cliente para el proyecto. Definir su participación dentro del proyecto.	Cliente

Fuente: Elaboración de autores

k. Suposiciones y restricciones

A continuación, se describirá algunas suposiciones y restricciones del plan de implementación que nos ayudarán respecto al desarrollo y ejecución del documento.

- Las actividades y fechas del plan de implementación se ajustarán al cronograma de actividades que se describirá en puntos posteriores dentro del documento (Ver Tabla 9).
- La solución CA PAM debe tener conectividad con todos los dispositivos custodiados.
- Es de importancia contar con la disponibilidad de los usuarios claves en los procesos que se describieron anteriormente.
- Es de importancia contar con los recursos necesarios para la elaboración del ambiente de Certificación y la ejecución del Plan de Pruebas.
- Es de importancia cumplir con los requerimientos de HW/SW que se proveyeron en su momento.
- Se gestionará cuentas privilegiadas que sean administrativas y que no se encuentren definidas en: texto plano, dentro de codificación, dentro de un proceso o dependiente del algún aparte de su store principal.

4.1.2 Fase de soporte.

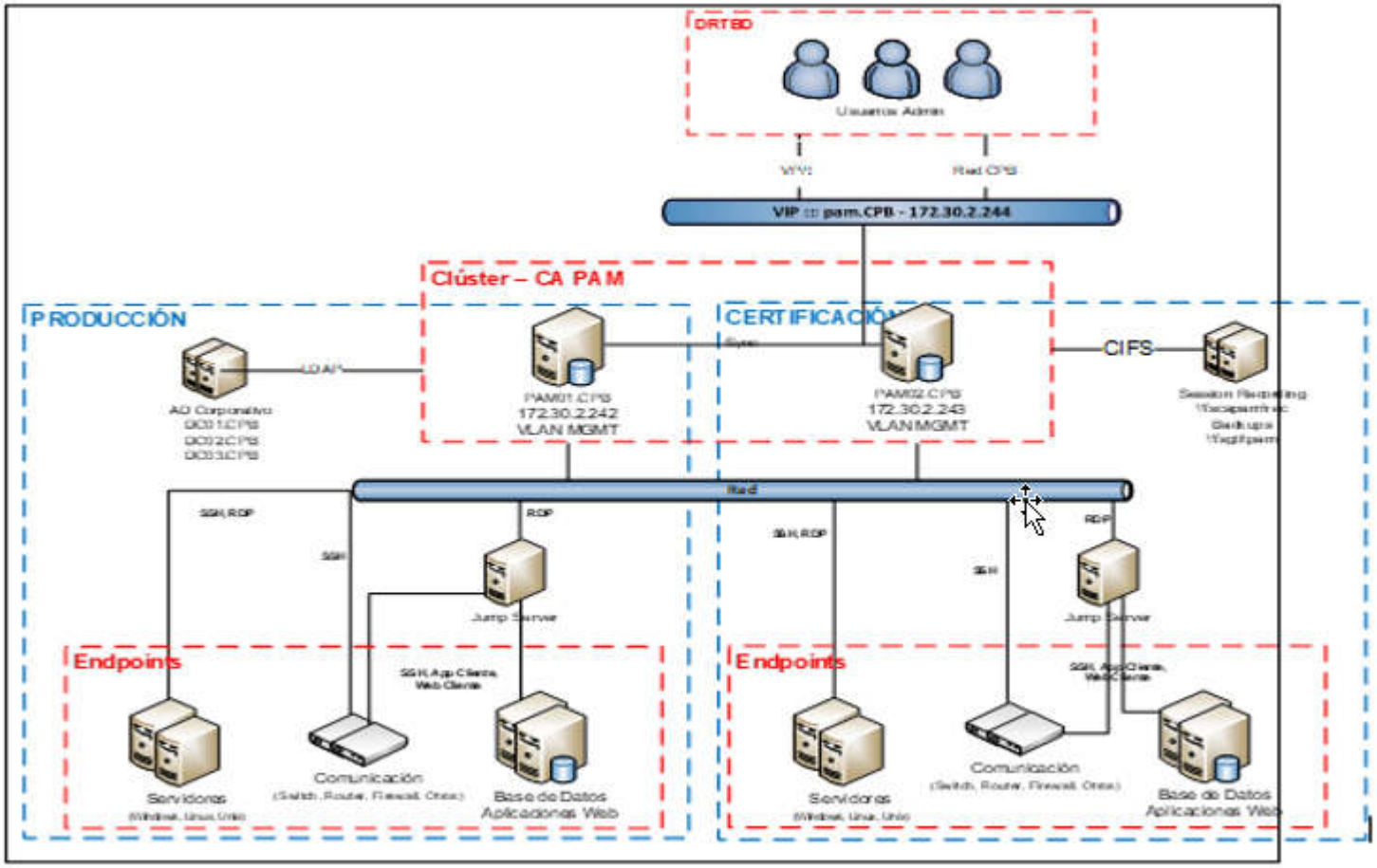
A continuación, se muestra el entregable de la fase de soporte "Documento de diseño y arquitectura".

- **ENTREGABLE: Documento de diseño y arquitectura**

a. Diseño de la solución

El acceso privilegiado a los dispositivos de la empresa de retail será administrado por el cliente 2 en conjunto con los autores de la tesis, el cual permitirá asegurar y controlar las sesiones a diversos sistemas (Ver Figura 16).

Figura 16: Diseño de la solución



Fuente: Elaboración de autores

El gráfico anterior permite describir puntos importantes, a partir de la implementación de la solución CA PAM:

- Los usuarios administradores tendrán un único canal de acceso a los dispositivos vía cliente de CA PAM y Web.
- Los usuarios accederán a la consola de CA PAM con Usuario/Contraseña de AD.
- Los usuarios tendrán acceso directo a los dispositivos sin requerir conocer las credenciales de las cuentas privilegiadas.
- Todas las grabaciones de sesión serán almacenadas en el repositorio externo.

b. Requerimientos técnicos

A continuación, se describe los requerimientos técnicos requeridos para culminar la implementación de la solución CA PAM.

Especificaciones de Hardware - Software

Los requerimientos de software y hardware que se necesitan para la implementación de la solución de CA PAM son los siguientes (Ver tabla 3 y 4).

Balanceo de carga

Para la habilitación del clúster de CA PAM y mantener la alta disponibilidad, se requiere de la siguiente IP virtual (Ver tabla 25).

- **FQDN:** https://pam.cpb
- **Virtual IP:** https:// 172.30.2.244
- **Tipo Balanceo:** Activo – Activo
- **Plataforma:** CA PAM

c. Dispositivos custodiados

A continuación, se da a conocer los dispositivos a configurar en la solución con sus credenciales privilegiados según el alcance brindado por el cliente.

- **Área de Base de datos (BD)**

En el levantamiento de información del área de BD se obtiene 25 base de datos Oracle que serán registrado en la solución *Privileged Access Manager* (Ver tabla 29).

Tabla 29: Dispositivos custodiados del área de BD

N°	Base de Datos	Tipo Aplicativo	Servidor
1	cpbbd	Oracle	zsrv01
2	cpbbtd	Oracle	csrv0101
3	cpbtth	Oracle	zsrv01
4	cpbtrth	Oracle	csrv0107
5	cpbthru	Oracle	zsrv54
6	Cpbthru2	Oracle	172.30.1.90
7	cpblbtr	Oracle	zsrv01
8	cpblbr	Oracle	csrv0103
9	cpbdwd	Oracle	zsrv01
10	Cpbdwd2	Oracle	csrv0105
11	cpbdeal	Oracle	zsrv01
12	Cpbdeal2	Oracle	csrv0104
13	XE	Oracle	dbpam (172.30.1.16)
14	cpbsicap	Oracle	zsrv01
15	Cpbsicap2	Oracle	csrv0106
16	oradmz	Oracle	srvoracle
17	Oradmz2	Oracle	192.168.72.17
18	cpbolap	Oracle	zsrv52
19	Cpbolap2	Oracle	172.30.1.32
20	cpbmeta	Oracle	zsrv52
21	Cpbmeta2	Oracle	172.30.1.32
22	rmancat	Oracle	zsrv01a
23	Rmancat2	Oracle	172.30.1.52
24	ovmmeta	Oracle	zsrv52
25	Ovmmeta2	Oracle	172.30.1.32

Fuente: Elaboración de autores

- **Área de Seguridad de la Información**

En el levantamiento de información del área de seguridad de la información se obtiene 29 dispositivos SSH entre dispositivos de redes y servidor linux, 16 páginas web y 36 servidores Windows con método de acceso RDP (Ver tabla 30), estos sistemas serán registrado en la solución *Privileged Access Manager*.

Tabla 30: Dispositivos custodiados del área de seguridad

N°	Nombre de dispositivo	URL Consola Administrativa / Nombre Servidor	Método de acceso
1	Firewall Aplicaciones Web	https://192.168.224.10:8083/SecureSphere/secsphLogin.jsp	SSH/WEB
2	Email Security (Antispam)	https://192.168.224.14/login	SSH/WEB
3	Email Security (Antispam)	https://192.168.224.15/login	SSH/WEB
4	DNS Externo, DHCP	CPBNET	SSH
5	Firewall (Nodo Principal - Sucursales)	https://192.168.224.26:9443/p/login/	SSH/WEB
6	Firewall (Sucursales)	https://172.29.2.132:9443/login	SSH/WEB
7	Firewall (Sucursales)	https://172.29.3.132:9443/login	SSH/WEB
8	Firewall (Sucursales)	https://172.29.4.132:9443/login	SSH/WEB
9	Firewall (Sucursales)	https://172.29.5.132:9443/login	SSH/WEB
10	Firewall (Sucursales)	https://172.29.6.132:9443/login	SSH/WEB
11	Firewall (Sucursales)	https://172.29.7.132:9443/login	SSH/WEB
12	Firewall (Sucursales)	https://172.29.8.132:9443/login	SSH/WEB
13	Web Security (Proxy)	https://CPBroxy.CPB:4712/Konfigurator/request	SSH/WEB

N°	Nombre de dispositivo	URL Consola Administrativa / Nombre Servidor	Método de acceso
14	SSL/VPN	https://xnet.CPB.pe/dana-na/auth/url_admin/welcome.cgi	WEB
15	Balanceador de enlaces	https://200.37.165.29/	WEB
16	SIEM	https://192.168.224.31/Application.html	SSH/WEB
17	Antivirus	https://SC01/login.html	WEB
18	Servidor Proxy	Squid Proxy	SSH
19	Consola Exchange	https://exch.CPB..pe/ecp	WEB
20	Mailbox01	exchmb01	SSH/RDP-Windows
21	Mailbox02	exchmb02	SSH/RDP-Windows
22	Mailbox03	exchmb03	SSH/RDP-Windows
23	Mailbox04	exchmb04	SSH/RDP-Windows
24	Mailbox05	exchmb05	SSH/RDP-Windows
25	Mailbox06	exchmb06	SSH/RDP-Windows
26	CAS01	exchca01	RDP-Windows
27	CAS02	exchca02	RDP-Windows
28	Qlikview publisher	qlikviewpub	RDP-Windows
29	Qlikview Prod	qlikviewprod	RDP-Windows
30	Workflow	workflowprd1	RDP-Windows
31	Laserfiche AXON	laserfichetra1	RDP-Windows
32	Laserfiche Producción	laserficheprd1	RDP-Windows
33	DATATEC	dapidataec	RDP-Windows
34	Servicios Axon	serviciosprod	RDP-Windows

N°	Nombre de dispositivo	URL Consola Administrativa / Nombre Servidor	Método de acceso
35	plataforma Axon	plataformaprod	SSH
36	Frontal AXON	frontalprod	SSH
37	Sede AXON	sedeprod	SSH
38	Reporteador Exchange	exchreporter	RDP-Windows
39	Auditoria File Server / Exchange	changeaud	RDP-Windows
40	Lotus Notes	CPBnt14	RDP-Windows
41	FS EE.EE	fsest	RDP-Windows
42	FS Opint	fsint	RDP-Windows
43	FS Comunicaciones	fscom	RDP-Windows
44	FS Auditoria	fsaud	RDP-Windows
45	FS Fondo empleados	fsfe	RDP-Windows
46	FS Riesgos	fsrsg	RDP-Windows
47	FS CONTAB	fscon	RDP-Windows
48	FS Teso	fscir	RDP-Windows
49	FS GTI	fsgti	RDP-Windows
50	FS Juridica	fsjur	RDP-Windows
51	FS SOFT	fs1	RDP-Windows
52	Portal CPB	CPBortal	SSH
53	Intranet	lnx001	SSH
54	Domain Controler 1	dc01	RDP-Windows
55	Domain Controler 2	dc02	RDP-Windows
56	Domain Controler 3	dc03	RDP-Windows
57	SPIJ	srv60	RDP-Windows
58	SICAP	srv76	RDP-Windows
59	Incentage	srv95	RDP-Windows
60	NTP	srvsca	RDP-Windows

N°	Nombre de dispositivo	URL Consola Administrativa / Nombre Servidor	Método de acceso
61	Cisco Telepresence Conductor	srv-op-con00	SSH
62	Cisco Telepresence Conductor	srv-op-conad00	SSH
63	Cisco Telepresence Conductor	srv-op-conre00	SSH

Fuente: Elaboración de autores

- **Área de redes**

En el levantamiento de información del área de redes se obtiene 44 dispositivos de redes (ver tabla 31) que serán registrado en la solución CA PAM.

Tabla 31: Dispositivos custodiados del área de redes

N°	Plataforma	Nombre de dispositivo	Puerto	Dirección IP
1	Cisco IOS	OP-SW-S3	22	172.30.4.37
2	Cisco IOS	OP-SW-S1A	22	172.30.4.38
3	Cisco IOS	OP-SW-S1C	22	172.30.4.39
4	Cisco IOS	OP-SW-S1C1	22	172.30.4.40
5	Cisco IOS	OP-SW-P1A	22	172.30.4.41
6	Cisco IOS	OP-SW-P1C	22	172.30.4.42
7	Cisco IOS	OP-SW-P1C1	22	172.30.4.43
8	Cisco IOS	OP-SW-P2A	22	172.30.4.44
9	Cisco IOS	OP-SW-P2C	22	172.30.4.45
10	Cisco IOS	OP-SW-P3	22	172.30.4.46
11	Cisco IOS	OP-SW-P3A	22	172.30.4.47
12	Cisco IOS	OP-SW-P3C	22	172.30.4.48
13	Cisco IOS	OP-SW-P5	22	172.30.4.49
14	Cisco IOS	OP-SW-P6	22	172.30.4.50
15	Cisco IOS	OP-SW-P7	22	172.30.4.51
16	Cisco IOS	MUSEO-SW-P4	22	172.30.4.52
17	Cisco IOS	CNM-SW-2A	22	172.30.4.53

N°	Plataforma	Nombre de dispositivo	Puerto	Dirección IP
18	Cisco IOS	CNM-SW-2B	22	172.30.4.54
19	Cisco IOS	CNM-SW-OCN	22	172.30.4.55
20	Cisco IOS	CNM-SW-2C	22	172.30.4.56
21	Cisco IOS	CID-SW-P1	22	172.30.4.57
22	Cisco IOS	CID-SW-P4	22	172.30.4.58
23	Cisco IOS	CID-SW-P4A1	22	172.30.4.59
24	Cisco IOS	CID-SW-P4A2	22	172.30.4.100
25	Cisco IOS	Switch LAB CU	22	172.30.4.62
26	Huawei	OP-SW-S3-huawei	22	172.30.4.102
27	Huawei	OP-SW-S1C-huawei	22	172.30.4.103
28	Huawei	OP-SW-S3-1-huawei (sala de capacitación)	22	172.30.4.104
29	Cisco Nexus Operating System (NX-OS)	CPB1	22	172.30.2.146
30	Cisco Nexus Operating System (NX-OS)	CPB1-CORE1	22	172.30.2.121
31	Cisco Nexus Operating System (NX-OS)	CPB1-ENTERPRISE1	22	172.30.2.251
32	Cisco Nexus Operating System (NX-OS)	CPB2	22	172.30.2.147
33	Cisco Nexus Operating System (NX-OS)	CPB2-CORE2	22	172.30.2.122
34	Cisco Nexus Operating System (NX-OS)	CPB2-ENTERPRISE2	22	172.30.2.252
35	Cisco Nexus Operating System (NX-OS)	CPB3	22	172.30.2.148
36	Cisco Nexus Operating System (NX-OS)	CPB3-CORE3	22	172.30.2.123
37	Cisco Nexus Operating System (NX-OS)	CPB3-ENTERPRISE3	22	172.30.2.253
38	Cisco IOS	Brocade SAN0-OP	22	172.30.2.25

N°	Plataforma	Nombre de dispositivo	Puerto	Dirección IP
39	Cisco IOS	Brocade SAN1-OP	22	172.30.2.26
40	Cisco IOS	Brocade SAN0-CER	22	172.30.2.27
41	Cisco IOS	Brocade SAN1-CER	22	172.30.2.28
42	Expressway Core PUB	srv-op-xpc00	22	172.30.5.27
43	Expressway Edge PUB	srv-op-xpe01	22	192.168.79.4
44	Telepresence Server	srv-op-ts00	22	172.30.5.26

Fuente: Elaboración de autores

d. Estrategia de transición

Para la implementación se realiza las actividades principales ya identificadas (Ver Figura 14) para la culminación satisfactoria.

Los dispositivos y cuentas privilegiadas a proteger serán distribuidos de la siguiente forma (Ver Tabla 32).

Tabla 32: Estrategia de transición

Ambiente	Dispositivos por proteger	Comentarios
CERTIFICACIÓN	• Switch CISCO - 172.30.4.39/ 172.30.4.40 • Huawei OP-SW-S3-huawei – 172.30.4.102 • Auditoria File Server/ Exchange - changeaud • Jump Server - 172.30.2.246 • Oracle cpbbd – zsrv01 • Oracle cpbdwd – zsrv01	En total serán **6 dispositivos** para el ambiente de certificación, **cada dispositivo con hasta 2 cuentas privilegiadas.** **Nota:** Se requerirá de Jump Server, para que los usuarios puedan acceder a aplicaciones de tipo cliente-servidor.
PRODUCCIÓN	• Ver tabla 26 • Ver tabla 27 • Ver tabla 28	En total son 150 **dispositivos** para el ambiente de producción, **cada dispositivo con máximo 2 cuentas privilegiadas.**

Fuente: Elaboración de autores

Se manejará flujos de aprobaciones para acceder a los dispositivos, siendo el aprobador el jefe del departamento RTBD.

Se definió que los administradores de la solución serán: Cliente 1 y Cliente 2.

- **Cliente 1:** jefe del departamento de redes, telecomunicaciones y base de datos.

- **Cliente 2:** Especialista del departamento de redes, telecomunicaciones y base de datos.

Ningún usuario definido como Auditor dentro de CA PAM por el momento, esto podría ser configurado por el administrador de CA PAM en cualquier momento.

e. Puertos de los componentes de la solución

Los puertos usados por los componentes de la solución están resumidos en la siguiente tabla (Ver tabla 33).

Tabla 33: Puertos de los componentes de la solución

Puerto	Origen	Destino
22	CA PAM server	SSH
123	CA PAM server	Servidor NTP
389	CA PAM server	Servidor LDAP, Controlador de Dominio
1521	CA PAM server	Servidor Oracle
443	Client workstations	CA PAM server
	CA PAM server: cluster node	CA PAM server: cluster node
445	CA PAM server	CIFS server
636	CA PAM server	Controlador de Dominio
2049	CA PAM server	NFS server
3306	CA PAM server: cluster member	Otros CA PAM server: Cluster member
3389	CA PAM server	RDP
5900	CA PAM server: cluster member	Otros CA PAM server: Cluster member

Puerto	Origen	Destino
7900	CA PAM server: cluster member	Otros CA PAM server: cluster member
7901	CA PAM server: cluster member	Otros CA PAM server: cluster member
7902	CA PAM server: cluster member	Otros CA PAM server: cluster member

Fuente: Elaboración de autores

f. Casos de uso de la solución

Los casos de uso definidos para realizar las pruebas funcionales luego de la implementación de la solución son los siguientes (Ver tabla 34).

Tabla 34: Casos de uso de la solución

Identificador de Caso de Uso	Objetivo de Caso de Uso
CU-01: Generación de Políticas de Acceso	Otorgar acceso a un usuario a un dispositivo.
CU-02: Acceso a Dispositivo Windows	Acceder a dispositivo de tipo Windows.
CU-03: Acceso a Dispositivo Web	Acceder a dispositivo de tipo Web
CU-04: Acceso a Dispositivo C/S	Acceder a dispositivo de tipo Cliente-Servidor.
CU-05: Revisión de Pistas de Auditoria	Revisar registros de Auditoria.
CU-06: Reproducir Grabación de Sesiones	Reproducir sesiones.
CU-07: Generación de Reportes Personalizados	Realizar reportes personalizados en CA PAM.
CU-08: Ejecución de Reportes predefinidos	Ejecutar reportes de CA PAM.
CU-09: *Administración CA Privileged Access Manager*	Ver respuesta de acceso a administración de *CA Privileged Access Manager*

Fuente: Elaboración de autores

g. Impacto de la solución

- **Impacto en procesos**

Resumen de como la solución mejora, asegura y simplifica el proceso de identidades privilegiadas en la siguiente tabla (Ver tabla 35). Cabe recalcar que los procesos internos oficiales de la empresa de retail lo actualizarán posteriormente a la implementación de la solución.

Tabla 35: Impacto en procesos

Objetivo	Proceso	Descripción
Administración de Acceso Privilegiado	Acceso seguro a Cuentas Privilegiadas	Solo los usuarios definidos por la empresa de retail tendrán acceso a la consola de CA PAM.
Administración de Acceso Privilegiado	Administración de Cuentas Privilegiadas	La solución almacenará credenciales de los dispositivos. La solución también administrará la rotación de contraseña de las credenciales. Con la solución en marcha, los usuarios iniciarán sesión en la consola central de administración de CA PAM para acceder a las cuentas privilegiadas gestionadas por la solución. Acceso a las credenciales de los dispositivos serán otorgados en base al rol dentro de CA PAM que la empresa de retail proveerá. El acceso a los dispositivos será con previa aprobación.

Fuente: Elaboración de autores

- **Impacto en los usuarios**

El impacto en los usuarios con la solución implementada esta resumido a continuación (Ver tabla 36).

Tabla 36: Impacto en los usuarios

Actor	Impacto
Administrador de Solución	Necesitará familiarizarse con la solución y todas sus funcionalidades para estar capacitado de sugerir/recomendar controles de seguridad dentro del ambiente de la empresa de retail.
Usuarios	Usuarios necesitarán acceso privilegiado para acceder a la interfaz web o cliente de CA PAM. No manejarán o conocerán las credenciales de las cuentas privilegiadas y, será monitoreado y alertado sus accesos.
Aprobador	Encargado de aprobar las solicitudes que los usuarios generarán para acceder a los dispositivos.

Fuente: Elaboración de autores

- **Impacto en tecnología**

Impacto de red

La solución generaría tráfico de red adicional de los siguientes componentes:

- CA PAM Appliance – Usuarios accederán a CA PAM y este se comunicará internamente al AD corporativo de la empresa de retail.
- CA PAM Appliance – Sesión de acceso privilegiado será iniciado de CA PAM a los dispositivos objetivos.
- CA PAM Appliance – Grabación de sesión será almacenada en recurso compartido externo.

Basado en esta configuración, es necesario que los puertos de red mencionados en la tabla 33 necesiten estar abiertos, para permitir la comunicación entre el usuario y los servidores que conforman la solución de Gestión de Identidades Privilegiadas.

Impacto de servidor

CA PAM es una instalación sin agentes y sin componentes instalados en los dispositivos.

Impacto en usuarios

Solo usuarios autorizados con previa aprobación estarán permitidos de adquirir acceso privilegiado en los dispositivos protegidos. Solo los usuarios autorizados estarán permitidos de instalar cliente de CA PAM.

4.2 Etapa Hacer

Se lleva a cabo la implementación del sistema de gestión de seguridad de información como respuesta al riesgo identificado, para ello se aplican políticas basadas en controles.

4.2.1 Fase de operación.

A continuación, el entregable levantamiento de información que contiene los equipos, sistemas y aplicativos a configurar

- **ENTREGABLE: Levantamiento de Información**

Se realiza la identificación y valoración de los activos de información identificados como proceso de los equipos más críticos y que demandan tener una cuenta privilegiada para cualquier cambio que implique dentro de sí misma.

La identificación de los activos consiste en determinar el área, el nombre de la base de datos o de los equipos, el tipo de servicio que brinda, el nombre del servidor, el direccionamiento IP para su gestión, el medio de gestión tanto privado como público, el protocolo, puerto de comunicación y las políticas de las contraseñas a aplicar. Con el objetivo de tener rastreados todos los activos que serán integrados dentro del sistema CA PAM algunos datos fueron cambiados y ocultados por seguridad y discreción de la empresa.

a. Levantamiento de información en el área de Base de Datos

En la siguiente tabla, se describe la información necesaria para realizar la integración de los servidores de bases de datos al CA PAM (Ver Tabla 37).

Tabla 37: Levantamiento de información del área de bases de datos

Área	Base de Datos	Tipo Aplicativo	Credencial	Servidor	Dirección IP	Tipo de Cuenta	Puerto	Políticas de Contraseña
Bases de Datos	cpbbd	Oracle	sys	zsrv01	172.30.1.220	LOCAL	1524/ 1525	- Rotación de contraseña. - No repetir la contraseña de las últimas 10 veces. - El tamaño de la credencial debe ser mayor a 8 caracteres. - La contraseña debe ser una combinación entre letras, números y caracteres especiales. - Tiempo máximo de Conexión 8 horas al día.
	cpbbtd	Oracle	sys	csrv0101	172.30.1.221	LOCAL	1531	
	cpbtth	Oracle	sys	zsrv01	172.30.1.222	LOCAL	1580	
	cpbtrth	Oracle	sys	csrv0107	172.30.1.223	LOCAL	2093	
	cpbthru	Oracle	sys	zsrv54	172.30.1.224	LOCAL	1580	
	cpbthru2	Oracle	sys	172.30.1.90	172.30.1.90	LOCAL	2093	
	cpblbtr	Oracle	sys	zsrv01	172.30.1.226	LOCAL	1531	
	cpblbr	Oracle	sys	csrv0103	172.30.1.227	LOCAL	1521	
	cpbdwd	Oracle	sys	zsrv01	172.30.1.228	LOCAL	1526	
	cpbdwd2	Oracle	sys	csrv0105	172.30.1.229	LOCAL	1531	
	cpbdeal	Oracle	sys	zsrv01	172.30.1.230	LOCAL	2093	
	cpbdeal2	Oracle	sys	csrv0104	172.30.1.231	LOCAL	1524/ 1525	
	XE	Oracle	sys	dbpam (172.30.1.16)	172.30.1.16	LOCAL	1522	
	cpbsicap	Oracle	sys	zsrv01	172.30.1.17	LOCAL	1526	
	cpbsicap2	Oracle	sys	csrv0106	172.30.1.233	LOCAL	1521	
	oradmz	Oracle	sys	srvoracle	172.30.1.16	LOCAL	1521	

Área	Base de Datos	Tipo Aplicativo	Credencial	Servidor	Dirección IP	Tipo de Cuenta	Puerto	Políticas de Contraseña
Bases de Datos	oradmz2	Oracle	sys	192.168.72.17	192.168.72.17	LOCAL	1521	- Rotación de contraseña. - No repetir la contraseña de las últimas 10 veces. - El tamaño de la credencial debe ser mayor a 8 caracteres. - La contraseña debe ser una combinación entre letras, números y caracteres especiales. - Tiempo máximo de Conexión 8 horas al día.
	cpbolap	Oracle	sys	zsrv52	172.30.1.235	LOCAL	1524/ 1525	
	cpbolap2	Oracle	sys	172.30.1.32	172.30.1.32	LOCAL	2093	
	cpbmeta	Oracle	sys	zsrv52	172.30.1.212	LOCAL	1526	
	cpbmeta2	Oracle	sys	172.30.1.32	172.30.1.32	LOCAL	1524/ 1525	
	rmancat	Oracle	sys	zsrv01a	172.30.1.221	LOCAL	1521	
	rmancat2	Oracle	sys	172.30.1.52	172.30.1.52	LOCAL	1580	
	ovmmeta	Oracle	sys	zsrv52	172.30.1.223	LOCAL	1526	
	ovmmeta2	Oracle	sys	172.30.1.32	172.30.1.32	LOCAL	1580	

Fuente: Elaboración de autores

La administración y asignación de las credenciales están a cargo de dos personas, que por criterios de seguridad son considerados como cliente 1 y cliente 2 en el presente documento. La primera persona es el jefe del departamento de redes, telecomunicaciones y base de datos (DRTBD) y la segunda persona es el especialista del DRTBD. La cantidad de cuentas privilegiadas creadas y asignadas a los encargados de la administración de la base de datos son en total 8 personas, de los cuales algunos tienen acceso a todas las Bases de datos y otros solo a algunas.

b. Levantamiento de información en el área de seguridad de la información

En la siguiente tabla, se describe la información necesaria para realizar la integración de los equipos de enrutamiento a nivel de red LAN y WAN al CA PAM, estos equipos tienen la función de brindar seguridad en la red. Además, permiten monitorear el tráfico de red entrante y saliente y decide si permite o bloquea el tráfico específico en función de un conjunto definido de reglas de seguridad (Ver Tabla 38).

Tabla 38: Levantamiento de información de equipos de seguridad

Área	Nombre de dispositivo	Método de acceso	Credencial	URL Consola Administrativa / Nombre Servidor	Dirección IP Privada	Tipo de Cuenta	Puerto	Politicas de Contraseña
Seguridad de la Información	Firewall Aplicaciones Web	SSH/WEB	Admin	https://192.168.224.10:8083/Secure Sphere/secsphLogin.jsp	192.168.224.10	LOCAL	22/9443	- Rotación de contraseña. - No repetir la contraseña de las últimas 10 veces. - El tamaño de la credencial debe ser mayor a 8 caracteres. - La contraseña debe ser una combinación entre letras, números y caracteres especiales. - Tiempo máximo de Conexión 8 horas al día.
	Email Security (Antispam)	SSH/WEB	Admin	https://192.168.224.14/login	192.168.224.14	LOCAL	22/9443	
	Email Security (Antispam)	SSH/WEB	Admin	https://192.168.224.15/login	192.168.224.15	LOCAL	22/9443	
	DNS Externo, DHCP	SSH	Admin	CPBNET	192.188.224.38	LOCAL	22	
	Firewall (Nodo Principal - Sucursales)	SSH/WEB	Admin	https://192.168.224.26:9443/p/login/	192.168.224.26	LOCAL	22/9443	
	Firewall (Sucursales)	SSH/WEB	Admin	https://172.29.2.132:9443/login	172.29.2.132	LOCAL	22/9443	
	Firewall (Sucursales)	SSH/WEB	Admin	https://172.29.3.132:9443/login	172.29.3.132	LOCAL	22/9443	
	Firewall (Sucursales)	SSH/WEB	Admin	https://172.29.4.132:9443/login	172.29.4.132	LOCAL	22/9443	
	Firewall (Sucursales)	SSH/WEB	Admin	https://172.29.5.132:9443/login	172.29.5.132	LOCAL	22/9443	
	Firewall (Sucursales)	SSH/WEB	Admin	https://172.29.6.132:9443/login	172.29.6.132	LOCAL	22/9443	
	Firewall (Sucursales)	SSH/WEB	Admin	https://172.29.7.132:9443/login	172.29.7.132	LOCAL	22/9443	
	Firewall (Sucursales)	SSH/WEB	Admin	https://172.29.8.132:9443/login	172.29.8.132	LOCAL	22/9443	
	Web Security (Proxy)	SSH/WEB	Admin	https://CPBroxy.CPB:4712/Konfigurator/request	192.188.224.39	LOCAL	22/8000	

Área	Nombre de dispositivo	Método de acceso	Credencial	URL Consola Administrativa / Nombre Servidor	Dirección IP Privada	Tipo de Cuenta	Puerto	Políticas de Contraseña
	SSL/VPN	WEB	Admin	https://xnet.CPB.pe/dana-na/auth/url_admin/welcome.cgi	192.188.224.40	LOCAL	8080	
	Balanceador de enlaces	WEB	Admin	https://200.37.165.29/	200.37.165.29	LOCAL	22/9443	
	SIEM	SSH/WEB	Admin	https://192.168.224.31/Application.html	192.168.224.31	LOCAL	22/9443	
	Antivirus	WEB	Admin	https://SC01/login.html	192.188.224.41	LOCAL	8080	- Rotación de contraseña. - No repetir la contraseña de las últimas 10 veces. - El tamaño de la credencial debe ser mayor a 8 caracteres. - La contraseña debe ser una combinación entre letras, números y caracteres especiales. - Tiempo máximo de Conexión 8 horas al día.
	Servidor Proxy	SSH	Admin	Squid Proxy	192.188.224.42	LOCAL	22	
	Consola Exchange	WEB	Admin	https://exch.CPB.pe/ecp	192.188.224.43	LOCAL	8080	
Seguridad de la Información	Mailbox01	SSH/RDP-indows	Admin	exchmb01.cpb	192.188.224.45	LOCAL	--	
	Mailbox02	SSH/RDP-Windows	Admin	exchmb02.cpb	192.188.224.46	LOCAL	--	
	Mailbox03	SSH/RDP-Windows	Admin	exchmb03.cpb	192.188.224.47	LOCAL	--	
	Mailbox04	SSH/RDP-Windows	Admin	exchmb04.cpb	192.188.224.48	LOCAL	--	
	Mailbox06	SSH/RDP-Windows	Admin	exchmb06.cpb	192.188.224.49	LOCAL	--	
	Mailbox05	SSH/RDP-Windows	Admin	exchmb05.cpb	192.188.224.50	LOCAL	--	

Área	Nombre de dispositivo	Método de acceso	Credencial	URL Consola Administrativa / Nombre Servidor	Dirección IP Privada	Tipo de Cuenta	Puerto	Políticas de Contraseña
	CAS01	RDP-Windows	Admin	exchca01.cpb	192.188.224.51	LOCAL	--	
	CAS02	RDP-Windows	Admin	exchca02.cpb	192.188.224.52	LOCAL	--	
	Qlikview publisher	RDP-Windows	Admin	qlikviewpub.cpb	192.188.224.53	LOCAL	--	
	Qlikview Prod	RDP-Windows	Admin	qlikviewprod.cpb	192.188.224.54	LOCAL	--	- Rotación de contraseña. - No repetir la contraseña de las últimas 10 veces. - El tamaño de la credencial debe ser mayor a 8 caracteres. - La contraseña debe ser una combinación entre letras, números y caracteres especiales. - Tiempo máximo de Conexión 8 horas al día.
	Workflow	RDP-Windows	Admin	workflowprd1.cpb	192.188.224.55	LOCAL	--	
	Laserfiche AXON	RDP-Windows	Admin	laserfichetra1.cpb	192.188.224.56	LOCAL	--	
Seguridad de la Información	Laserfiche Producción	RDP-Windows	Admin	laserficheprd1.cpb	192.188.224.57	LOCAL	--	
	DATATEC	RDP-Windows	Admin	dapidataec.cpb	192.188.224.58	LOCAL	--	
	Servicios Axon	RDP-Windows	Admin	serviciosprod.cpb	192.188.224.59	LOCAL	--	
	plataforma Axon	SSH	Admin	plataformaprod.cpb	192.188.224.60	LOCAL	--	
	Frontal AXON	SSH	Admin	frontalprod.cpb	192.188.224.61	LOCAL	--	
	Sede AXON	SSH	Admin	sedeprod.cpb	192.188.224.62	LOCAL	--	
	Reporteador Exchange	RDP-Windows	Admin	exchreporter.cpb	192.188.224.63	LOCAL	--	

Área	Nombre de dispositivo	Método de acceso	Credencial	URL Consola Administrativa / Nombre Servidor	Dirección IP Privada	Tipo de Cuenta	Puerto	Políticas de Contraseña
	Auditoria File Server / Exchange	RDP-Windows	Admin	changeaud.cpb	192.188.224.64	LOCAL	--	
	Lotus Notes	RDP-Windows	Admin	CPBnt14.cpb	192.188.224.65	LOCAL	--	
	FS EE.EE	RDP-Windows	Admin	fsest.cpb	192.188.224.66	LOCAL	--	- Rotación de contraseña. - No repetir la contraseña de las últimas 10 veces. - El tamaño de la credencial debe ser mayor a 8 caracteres. - La contraseña debe ser una combinación entre letras, números y caracteres especiales. - Tiempo máximo de Conexión 8 horas al día.
	FS Opint	RDP-Windows	Admin	fsint.cpb	192.188.224.67	LOCAL	--	
	FS Comunicaciones	RDP-Windows	Admin	fscom.cpb	192.188.224.68	LOCAL	--	
Seguridad de la Información	FS Auditoria	RDP-Windows	Admin	fsaud.cpb	192.188.224.69	LOCAL	--	
	FS Fondo empleados	RDP-Windows	Admin	fsfe.cpb	192.188.224.70	LOCAL	--	
	FS Riesgos	RDP-Windows	Admin	fsrsg.cpb	192.188.224.71	LOCAL	--	
	FS CONTAB	RDP-Windows	Admin	fscon.cpb	192.188.224.72	LOCAL	--	
	FS Teso	RDP-Windows	Admin	fscir.cpb	192.188.224.73	LOCAL	--	
	FS GTI	RDP-Windows	Admin	fsgti.cpb	192.188.224.74	LOCAL	--	

Área	Nombre de dispositivo	Método de acceso	Credencial	URL Consola Administrativa / Nombre Servidor	Dirección IP Privada	Tipo de Cuenta	Puerto	Políticas de Contraseña
Seguridad de la Información	FS Juridica	RDP-Windows	Admin	fsjur.cpb	192.188.224.75	LOCAL	--	- Rotación de contraseña. - No repetir la contraseña de las últimas 10 veces. - El tamaño de la credencial debe ser mayor a 8 caracteres. - La contraseña debe ser una combinación entre letras, números y caracteres especiales. - Tiempo máximo de Conexión 8 horas al día.
	FS SOFT	RDP-Windows	Admin	fs1.cpb	192.188.224.76	LOCAL	--	
	Portal CPB	SSH	Admin	CPBortal.cpb	192.188.224.77	LOCAL	--	
	Intranet	SSH	Admin	lnx001.cpb	192.188.224.78	LOCAL	--	
	Domain Controler 1	RDP-Windows	Admin	dc01.cpb	192.188.224.79	LOCAL	--	
	Domain Controler 2	RDP-Windows	Admin	dc02.cpb	192.188.224.80	LOCAL	--	
	Domain Controler 3	RDP-Windows	Admin	dc03.cpb	192.188.224.81	LOCAL	--	
	SPIJ	RDP-Windows	Admin	srv60.cpb	192.188.224.82	LOCAL	--	
	Incentage	RDP-Windows	Admin	srv95.cpb	192.188.224.83	LOCAL	--	
	NTP	RDP-Windows	Admin	srvsca.cpb	192.188.224.84	LOCAL	--	
	Cisco Telepresence Conductor	SSH	Admin	srv-op-con00.cpb	192.188.224.85	LOCAL	--	
	Cisco Telepresence Conductor	SSH	Admin	srv-op-conre00.cpb	192.188.224.86	LOCAL	--	

Fuente: Elaboración de autores

Grupo equipos de seguridad de red:

Son considerados los firewalls convencionales, los *antispam*, los servidores proxy, servidor de antivirus, entre otros. La administración de estos equipos está a cargo de 9 personas.

Credenciales privilegiadas que fueron asignadas:

- Para los firewalls se asignaron 4 credenciales debido a que se tiene esa cantidad de asistentes.

- Para los servidores proxys fueron 2 y los otros 3 restantes son para los asistentes del encargado de antivirus, y de los demás equipos de seguridad.

c. Levantamiento de información en el área de redes

En la siguiente tabla se describe la información necesaria para realizar la integración de los equipos de red LAN a CA PAM, estos equipos cumplen la función de interconectar los dispositivos finales (PCs, impresora, móvil) dentro de una misma red (Ver Tabla 39).

Para la administración de estos equipos de distribución y segmentación de red son reservadas 8 credenciales que tendrán acceso privilegiado. Con ello se cumple con el objetivo determinado en la primera etapa, donde se menciona que la cantidad de cuentas configuradas en este servicio en total son 25. De este modo, se completan credenciales indicadas en el alcance del presente trabajo.

Tabla 39: Levantamiento de información equipos de red LAN

Área	Tipo de Equipo	Modo de acceso	Credencial	Nombre del Equipo	Plataforma	Dirección IP Privada	Tipo de Conexión	Política Acceso - Super	Puerto	Políticas de Contraseña
Área de Redes	Switch	SSH /Telnet	Netadmin	OP-SW-S3	Cisco IOS	172.30.4.37	Local	Si	21/22/23	- Rotación de contraseña. - No repetir la contraseña de las últimas 10 veces. - El tamaño de la credencial debe ser mayor a 8 caracteres. - La contraseña debe ser una combinación entre letras, números y caracteres especiales. - Tiempo máximo de Conexión 8 horas al día.
	Switch	SSH /Telnet	Netadmin	OP-SW-S1A	Cisco IOS	172.30.4.38	Local	Si	21/22/23	
	Switch	SSH /Telnet	Netadmin	OP-SW-S1C1	Cisco IOS	172.30.4.39	Local	Si	21/22/23	
	Switch	SSH /Telnet	Netadmin	OP-SW-S1C1	Cisco IOS	172.30.4.40	Local	Si	21/22/23	
	Switch	SSH /Telnet	Netadmin	OP-SW-P1A	Cisco IOS	172.30.4.41	Local	Si	21/22/23	
	Switch	SSH /Telnet	Netadmin	OP-SW-P1C	Cisco IOS	172.30.4.42	Local	Si	21/22/23	
	Switch	SSH /Telnet	Netadmin	OP-SW-P1C1	Cisco IOS	172.30.4.43	Local	Si	21/22/23	
	Switch	SSH /Telnet	Netadmin	OP-SW-P2A	Cisco IOS	172.30.4.44	Local	Si	21/22/23	
	Switch	SSH /Telnet	Netadmin	OP-SW-P2C	Cisco IOS	172.30.4.45	Local	Si	21/22/23	
	Switch	SSH /Telnet	Netadmin	OP-SW-P3	Cisco IOS	172.30.4.46	Local	Si	21/22/23	
	Switch	SSH /Telnet	Netadmin	OP-SW-P3A	Cisco IOS	172.30.4.47	Local	Si	21/22/23	
	Switch	SSH /Telnet	Netadmin	OP-SW-P3C	Cisco IOS	172.30.4.48	Local	Si	21/22/23	
	Switch	SSH /Telnet	Netadmin	OP-SW-P6	Cisco IOS	172.30.4.50	Local	Si	21/22/23	
	Switch	SSH /Telnet	Netadmin	OP-SW-P7	Cisco IOS	172.30.4.51	Local	Si	21/22/23	
	Switch	SSH /Telnet	Netadmin	MUSEO-SW-P4	Cisco IOS	172.30.4.52	Local	Si	21/22/23	
	Switch	SSH /Telnet	Netadmin	CNM-SW-2A	Cisco IOS	172.30.4.53	Local	Si	21/22/23	
	Switch	SSH /Telnet	Netadmin	CNM-SW-2B	Cisco IOS	172.30.4.54	Local	Si	21/22/23	
	Switch	SSH /Telnet	Netadmin	CNM-SW-OCN	Cisco IOS	172.30.4.55	Local	Si	21/22/23	
	Switch	SSH /Telnet	Netadmin	CNM-SW-2C	Cisco IOS	172.30.4.56	Local	Si	21/22/23	
	Switch	SSH /Telnet	Netadmin	CID-SW-P1	Cisco IOS	172.30.4.57	Local	Si	21/22/23	
	Switch	SSH /Telnet	Netadmin	CID-SW-P4	Cisco IOS	172.30.4.58	Local	Si	21/22/23	
	Switch	SSH /Telnet	Netadmin	CID-SW-P4A1	Cisco	172.30.4.59	Local	Si	21/22/23	
	Switch	SSH /Telnet	Netadmin	CID-SW-P4A2	Cisco	172.30.4.100	Local	Si	21/22/23	
	Switch	SSH /Telnet	Netadmin	Switch LAB CU	Cisco	172.30.4.62	Local	Si	21/22/23	

Área	Tipo de Equipo	Modo de acceso	Credencial	Nombre del Equipo	Plataforma	Dirección IP Privada	Tipo de Conexión	Política Acceso - Super	Puerto	Políticas de Contraseña
Área de Redes	controlador wifi	SSH /Telnet/Web	Netadmin	OP-SW-S3-Huawei	Huawei	172.30.4.102	Local	Si	21/22/23/7000	- Rotación de contraseña. - No repetir la contraseña de las últimas 10 veces. - El tamaño de la credencial debe ser mayor a 8 caracteres. - La contraseña debe ser una combinación entre letras, números y caracteres especiales. - Tiempo máximo de Conexión 8 horas al día.
	controlador wifi	SSH /Telnet/Web	Netadmin	OP-SW-S1C-huawei	Huawei	172.30.4.103	Local	Si	21/22/23/7000	
	controlador wifi	SSH /Telnet/Web	Netadmin	OP-SW-S3-1-huawei sala de capacitacion	Huawei	172.30.4.104	Local	Si	21/22/23/7000	
	Aruba AirWave	SSH /Telnet/Web	Netadmin	CPB1	Cisco Nexus Operating System (NX-OS)	172.30.2.146	Local	Si	21/22/23	
	Router	SSH /Telnet/Web	Netadmin	CPB1-CORE1	Cisco Nexus Operating System (NX-OS)	172.30.2.121	Local	Si	21/22/23	
	Router	SSH /Telnet/Web	Netadmin	CPB1-ENTERPRISE1	Cisco Nexus Operating System (NX-OS)	172.30.2.251	Local	Si	21/22/23	
	Router	SSH /Telnet/Web	Netadmin	CPB2	Cisco Nexus Operating System (NX-OS)	172.30.2.147	Local	Si	21/22/23	
	Router	SSH /Telnet	Netadmin	CPB2-CORE2	Cisco Nexus Operating System (NX-OS)	172.30.2.122	Local	Si	21/22/23	
	Router	SSH /Telnet	Netadmin	CPB2-ENTERPRISE2	Cisco Nexus Operating System (NX-OS)	172.30.2.252	Local	Si	21/22/23	

Área	Tipo de Equipo	Modo de acceso	Credencial	Nombre del Equipo	Plataforma	Dirección IP Privada	Tipo de Conexión	Política Acceso - Super	Puerto	Políticas de Contraseña
Área de Redes	Router	SSH /Telnet	Netadmin	CPB3	Cisco Nexus Operating System (NX-OS)	172.30.2.148	Local	Si	21/22/23	- Rotación de contraseña. - No repetir la contraseña de las últimas 10 veces. - El tamaño de la credencial debe ser mayor a 8 caracteres. - La contraseña debe ser una combinación entre letras, números y caracteres especiales. - Tiempo máximo de Conexión 8 horas al día.
		SSH /Telnet	Netadmin	CPB3-ENTERPRISE3	Cisco Nexus Operating System (NX-OS)	172.30.2.253	Local	Si	21/22/23	
	Administrador ancho de banda Equipos Core	SSH /Telnet	Netadmin	Brocade SAN0-OP	Cisco IOS	172.30.2.25	Local	Si	21/22/23	
		SSH /Telnet	Netadmin	Brocade SAN0-CER	Cisco IOS	172.30.2.27	Local	Si	21/22/23	
		SSH /Telnet	Netadmin	Brocade SAN1-CER	Cisco IOS	172.30.2.28	Local	Si	21/22/23	
		SSH /Telnet	Netadmin	srv-op-xpc00	Expressway Core PUB	172.30.5.27	Local	Si	21/22/23	
		SSH /Telnet	Netadmin	srv-op-xpe01	Expressway Edge PUB	192.168.79.4	Local	Si	21/22/23	
		SSH /Telnet	Netadmin	srv-op-ts00	Telepresence Server	172.30.5.26	Local	Si	21/22/23	

Fuente: Elaboración de autores

- **ENTREGABLE: documento de configuración de equipos**

Se realiza la implementación del sistema de gestión de seguridad de información para la gestión de las identidades privilegiadas, el sistema a utilizar es CA PAM. Este sistema permite crear políticas, registros, monitoreo, notificaciones y restricciones de accesos de todos los usuarios que cuentan con algún tipo de cuentas privilegiadas.

La preparación empieza desde el desarrollo de los 2 servidores virtuales, que luego pasaron a contener el sistema CA PAM. Este SGSI es implementado en dos ambientes virtuales con la finalidad de tener un equipo de Backup, a su vez formar un clúster creando una dirección lógica. Y así brindar un servicio de alta disponibilidad y garantizar el respaldo de toda la información.

a. La preparación de CA PAM será descrita en los siguientes pasos

Paso1: Integración de los servidores CA PAM al dominio de la red

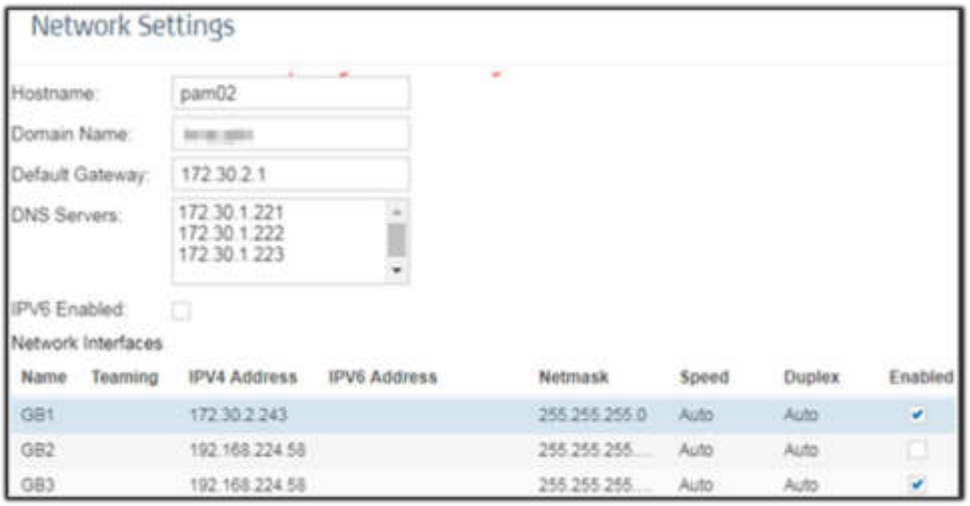
En la siguiente imagen se muestra los pasos para realizar la integración de los servidores CA PAM a la red de la empresa. Por consiguiente, para la configuración se ingresa el nombre del dispositivo, el dominio de la red, la puerta de enlace y por último las DNS (Ver Figura 17 y 18).

Figura 17: Servidor CA PAM 1

Fuente: Elaboración de autores

Nota: Se aplica la misma configuración realizada en el servidor 1.

Figura 18: Servidor CA PAM 2

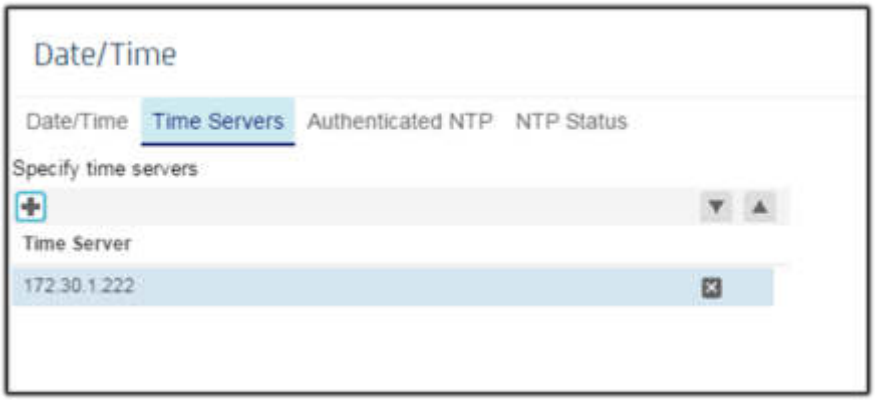


Fuente: Elaboración de autores

Paso 2: Integración del servidor NTP con CA PAM

Se realiza la integración del servidor NTP con CA PAM con el objetivo de que CA PAM registre todas las actividades de los usuarios en base a la fecha y hora que indica el servidor NTP (Ver Figura 19).

Figura 19: Integración del servidor NTP con CA PAM



Fuente: Elaboración de autores

Paso 3: Activación de Clúster (pam01.cpb.pe principal)

Se crea el Clúster con los dos servidores que contienen el CA PAM. En el servidor primario se debe ingresar una frase cualquiera y se debe elegir la opción "*Generate Key*" para generar una llave, que luego será

ingresada en el servidor 2, que permita realizar la sincronización y formar el clúster (Ver Figura 20 y 21).

Figura 20: Servidor CA PAM primario

Fuente: Elaboración de autores

Nota: Se aplica la misma configuración para el servidor secundario

Figura 21: Servidor CA PAM secundario

Fuente: Elaboración de autores

Luego de generar las llaves de la conexión entre los dos servidores CA PAM, se procede a crear el clúster, que viene a ser una dirección lógica. Para ello se necesita ingresar la IP que será conocida como el equipo principal (Ver Figura 22).

Figura 22: Creación del clúster y el balanceador de carga

Fuente: Elaboración de autores

La siguiente imagen muestra el resultado de la creación del clúster entre ambos servidores CA PAM (Ver Figura 23).

Figura 23: Resultado del balanceo de carga

Fuente: Elaboración de autores

Paso 4: Sincronizar los usuarios del *Active Directory* con CA PAM

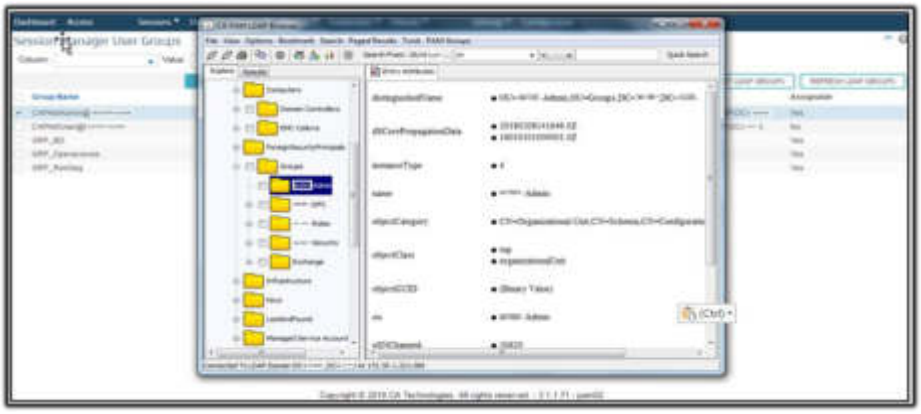
Se procede a sincronizar el servidor *active directory* con el servidor CA PAM, para que todos los usuarios registrados en el AD pasen a PAM. Y de este modo estos sean utilizados al momento de otorgar permisos de acceso (Ver Figura 24).

Figura 24: Sincronización de AD con CA PAM

Fuente: Elaboración de autores

Se procede a seleccionar a los usuarios que tendrán algún permiso dentro de todos los dispositivos que es administrado por CA PAM (Ver Figura 25).

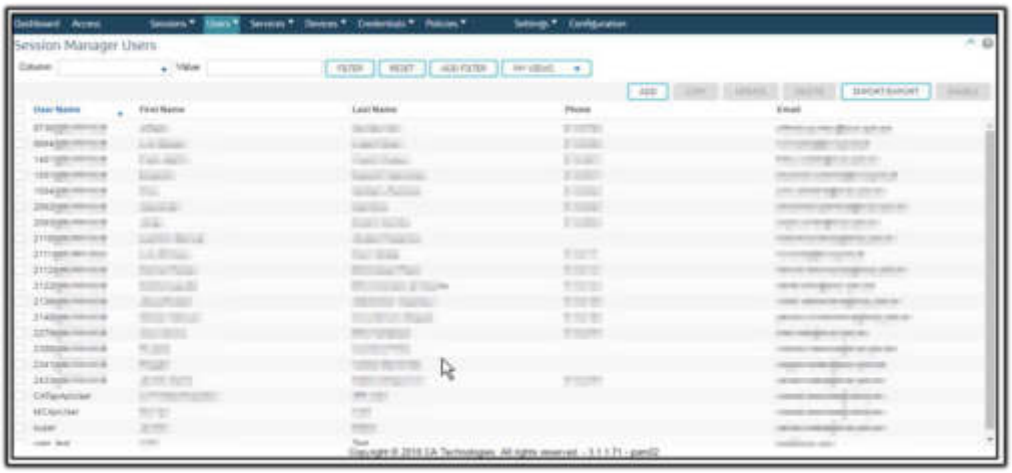
Figura 25: Importación de credenciales AD



Fuente: Elaboración de autores

Se lista todos los usuarios disponibles, que pueden ser asignados a algún permiso privilegiado (Ver Figura 26).

Figura 26: Resultado de las sincronizaciones de AD con CA PAM

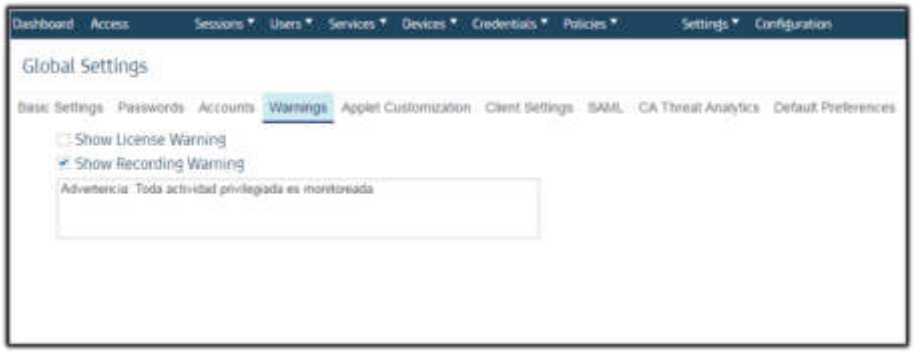


Fuente: Elaboración de autores

Paso 5: Creación de Notificaciones

Se configura la notificación que se les mostrará a los usuarios, cada vez que ingresen a los sistemas configurados dentro de la solución CA PAM, la siguiente imagen tiene como mensaje de la notificación “Advertencia: toda actividad privilegiada es monitoreada”, esto con el fin de que los usuarios sepan que su actividad está siendo grada y monitoreada, para que así no realicen actividades indebidas, que puedan afectar a la empresa (Ver Figura 27).

Figura 27: Creación de notificaciones

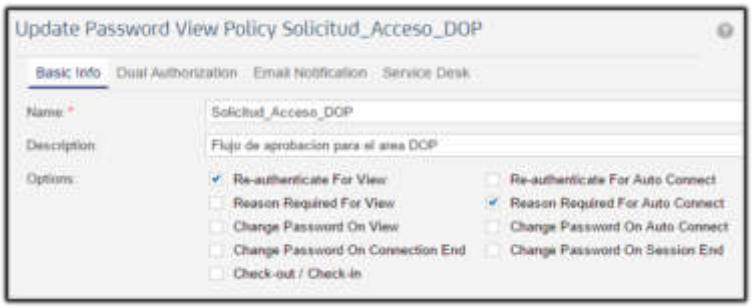


Fuente: Elaboración de autores

Paso 6: Política de Solicitud de Acceso

Las políticas de acceso a dispositivos críticos de la empresa de retail, se configuró “Solicitud_Acceso_DOP”, que consiste en solicitar doble autenticación para el ingreso del usuario (Ver Figura 28).

Figura 28: Política de solicitud de acceso

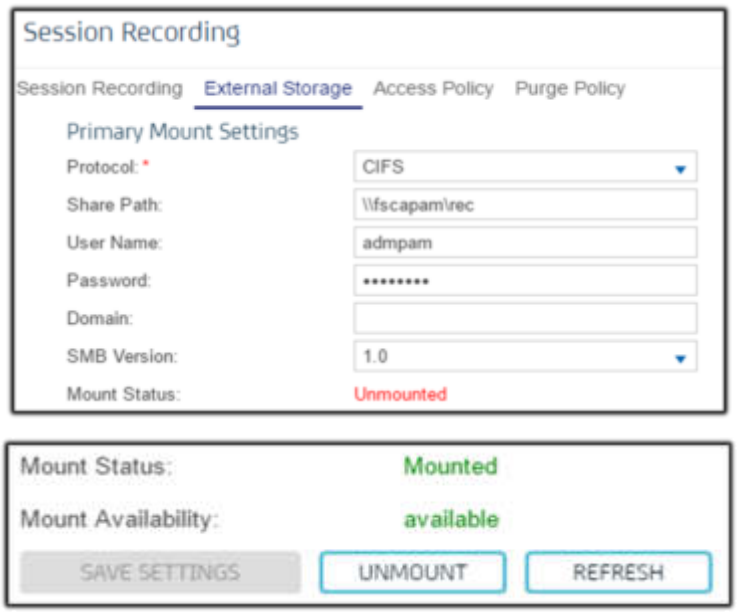


Fuente: Elaboración de autores

Paso 7: Grabación de la sesión

CA PAM enlaza la grabación a un repositorio externo que registrará todo el accionar del usuario desde el momento que acceda a la solución (Ver Figura 29).

Figura 29: Grabación de la sesión



Fuente: Elaboración de autores

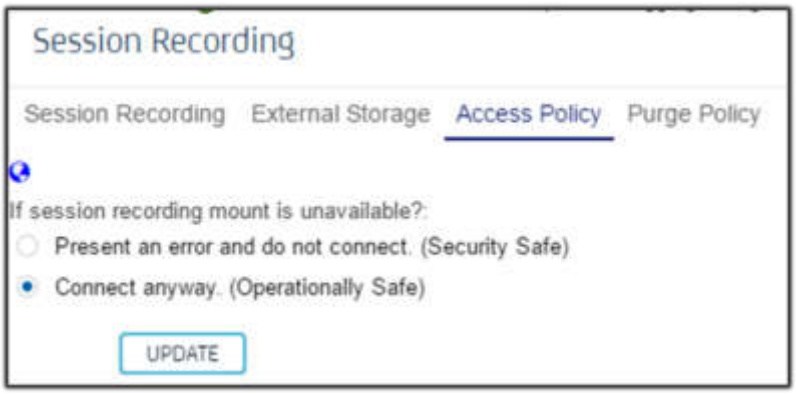
La configuración del tipo de grabado. CA PAM cuenta con 3 opciones de las cuales se ha habilitado dos de ellas. La primera permite grabar la sesión en base a los comandos utilizados, y la segunda opción es para el grabado gráficamente (Ver Figura 30).

Figura 30: Grabación de Inicio de sesión

Fuente: Elaboración de autores

Otra política aplicada en la configuración de seguridad es en caso de que CA PAM presente una avería con la función de grabado de sesión, esta puede permitir el ingreso a los dispositivos custodiados sin ser grabados (Ver Figura31).

Figura 31: Políticas de seguridad si CA PAM falla



Fuente: Elaboración de autores

Paso 8: Monitoreo

Se registra el usuario del administrador encargado de realizar el monitoreo de las acciones del personal que accede al sistema (Ver Figura 32).

Figura 32: Registro del administrador del monitoreo

Fuente: Elaboración de autores

Aplicar la política de grabación consiste en que automáticamente CA PAM empezará a grabar todo el movimiento que realice el usuario desde el momento que este ingrese al sistema (Ver Figura 33).

Figura 33: Grabación del monitoreo

Fuente: Elaboración de autores

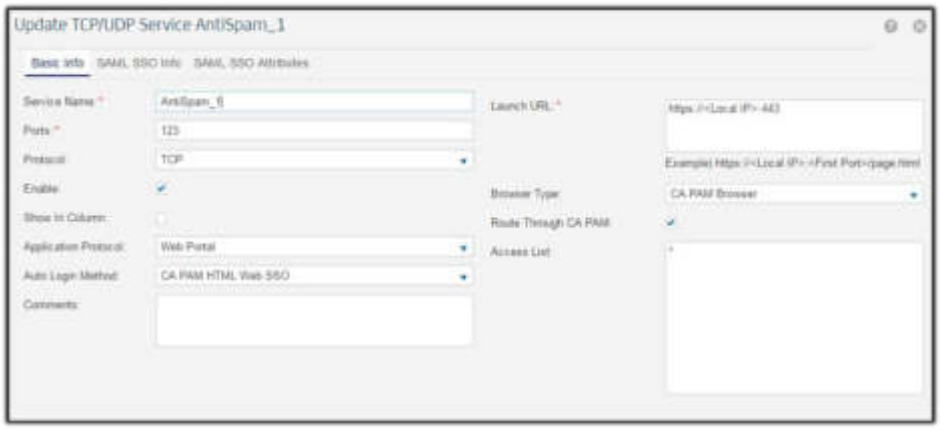
Después de haber culminado con la primera parte que es la preparación del servidor CA PAM, se procede a crear los servicios para los dispositivos que sean custodiados. Posteriormente se aplicó las políticas de acceso y se relacionó al usuario con los sistemas a los que tiene acceso.

b. Gestión de identidades privilegiadas en dispositivos Web

- **Creación del Servicio del aplicativo *AntiSpam***

Para la creación de un servicio Web se realiza una configuración en donde se ingresa el nombre que cubre el servicio, el puerto y el protocolo de conexión UDP o TCP, la dirección web. Además del protocolo de la aplicación que le identifica como un servicio web (Ver Figura 34).

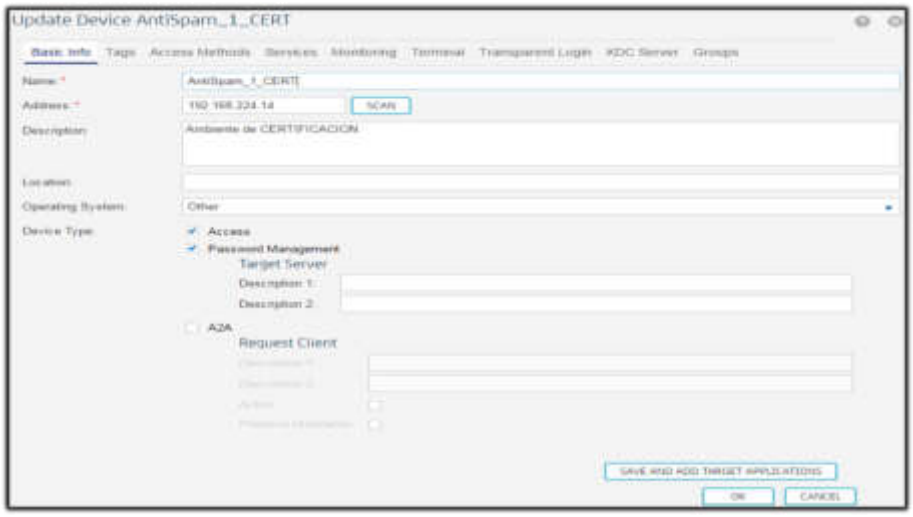
Figura 34: Creación de Servicio Web



Fuente: Elaboración de autores

Se procede a realizar la creación del dispositivo que va a contener un sistema, en este caso es el Antispam. Para ello se debe completar el nombre que tendrá el dispositivo web, la dirección IP, el sistema operativo, el tipo de acceso, y la opción *password Management* para que CA PAM rote la contraseña cada cierto tiempo (Ver Figura 35).

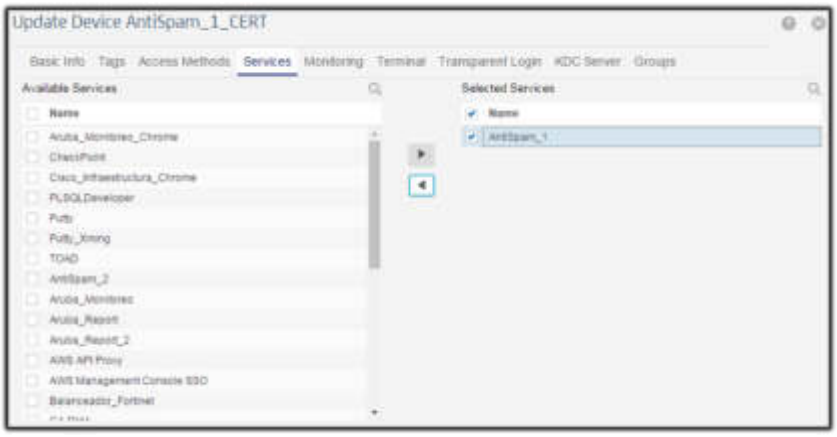
Figura 35: Creación del dispositivo Web



Fuente: Elaboración de autores

Después de tener creado el servicio y el dispositivo, se continua con la integración de ambos (Ver Figura 36).

Figura 36: Integración del servicio con el dispositivo Web

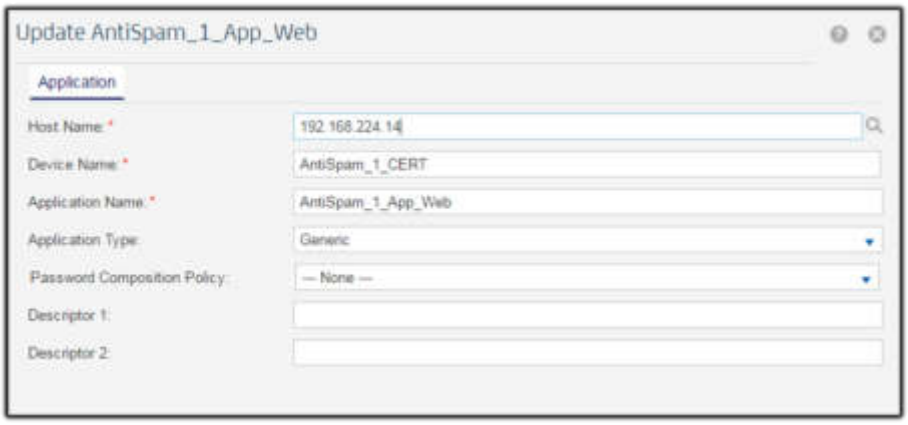


Fuente: Elaboración de autores

- **Creación de Aplicación Web**

Se registra la aplicación que contendrá al servidor a custodiar, para ello se necesita ingresar la dirección IP del servidor, nombre del servicio, nombre de la aplicación y el tipo de aplicación (Ver Figura 37).

Figura 37: Creación del aplicativo Web

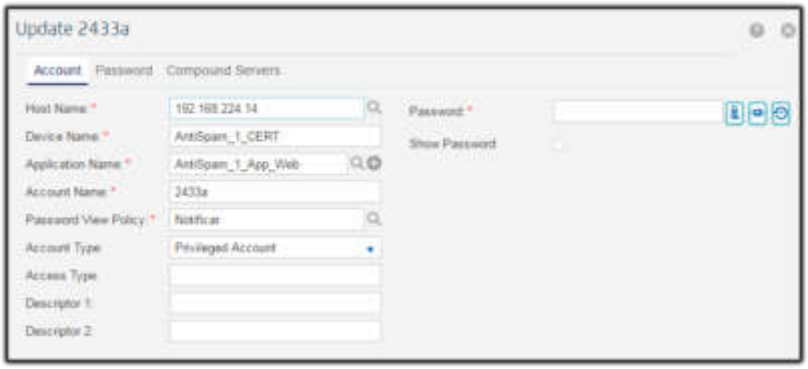


Fuente: Elaboración de autores

- **Creación de Cuenta**

Se crea la cuenta que va a administrar el aplicativo, para ello se debe ingresar la dirección IP del servidor, nombre del servicio, nombre de la aplicación creada previamente, nombre de la cuenta que va a administrar y también el tipo de cuenta. (Ver Figura 38).

Figura 38: Creación de la cuenta Web.

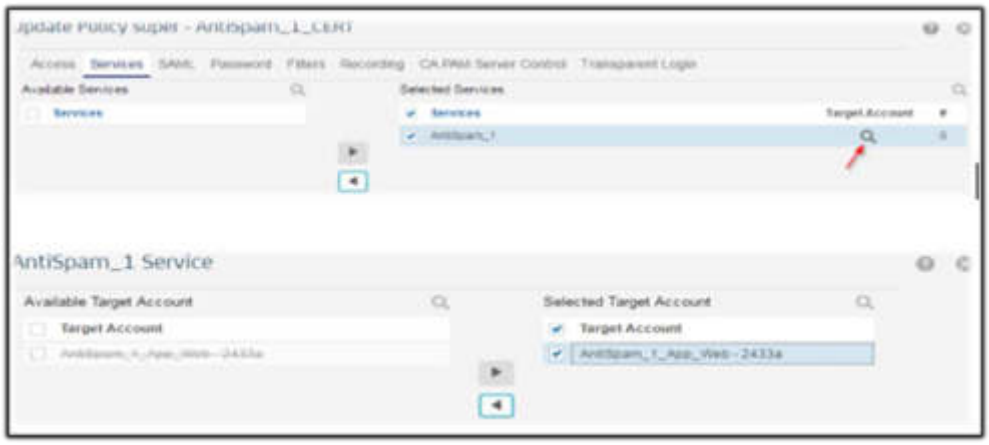


Fuente: Elaboración de autores

- **Creación de Políticas de Acceso**

En la siguiente imagen se procede a crear las políticas para que un usuario pueda acceder al dispositivo web y elija con que cuenta va a iniciar sesión (Ver Figura 39).

Figura 39: Integración de políticas de seguridad



Fuente: Elaboración de autores

Se configura el tipo de grabación que va a tener el servicio, al tratarse de un servicio web se elige la opción “portal web” para la grabación gráfica (Ver Figura 40).

Figura 40: Configuración del tipo de registro

Fuente: Elaboración de autores

La configuración descrita en las figuras anteriores es la primera parte de la implementación general realizada en la organización. Para evitar que esta fase contenga demasiadas imágenes, la implementación y configuración de la Gestión de identidades privilegiadas en dispositivos SSH, Cliente/Servidor y aplicativos RDP se muestra en la etapa de anexos (Ver Anexo 2).

- **ENTREGABLE: Plan de pruebas**

Se define el enfoque global de las pruebas, identificando el tipo y definición de cada una de ellas.

a. Tipos de Pruebas

Se detalla el procedimiento a seguir para validar el resultado esperado, teniendo en cuenta el uso de tipos de datos de entrada / salida que se detalla en la documentación.

Las pruebas unitarias y las pruebas funcionales serán realizadas por el equipo autor de la tesis y los clientes.

b. Casos de prueba

A continuación, se detalla cada prueba que será utilizada para validar la solución. Las pruebas realizadas deberán únicamente validar los requerimientos de la solución/negocio (casos de uso) o las métricas definidas, cualquier prueba adicional no debe ser realizada.

Los casos de pruebas que serán evaluados dentro de las pruebas funcionales son los siguientes (Ver tabla 40).

Tabla 40: Casos de pruebas funcionales

ID	Pruebas Funcionales	Recurso	Aprobador
CU-01	Inicio de sesión	Autores	Cliente 1 y 2
CU-02	Generación de Políticas de Acceso	Autores	Cliente 1 y 2
CU-03	Acceso a Dispositivo Windows	Autores	Cliente 1 y 2
CU-04	Acceso a Dispositivo Web	Autores	Cliente 1 y 2
CU-05	Acceso a Dispositivo C/S	Autores	Cliente 1 y 2
CU-06	Revisión de Pistas de Auditoria	Autores	Cliente 1 y 2
CU-07	Reproducir Grabación de Sesiones	Autores	Cliente 1 y 2
CU-08	Generación de Reportes Personalizados	Autores	Cliente 1 y 2
CU-09	Ejecución de Reportes predefinidos	Autores	Cliente 1 y 2

Fuente: Elaboración de autores

El caso de prueba que será evaluado dentro de las pruebas unitarias son los siguientes (Ver tabla 41).

Tabla 41: Caso de pruebas unitarias

ID	Pruebas Unitarias	Recurso	Aprobador
CU-10	Administración CA Privileged Access Manager	Autores	Cliente 1 y 2

Fuente: Elaboración de autores

Pruebas funcionales

CP-01 Inicio de sesión

CP-01	Inicio de sesión	
Referencia al Caso de Uso	N/A	
Objetivo	Otorgar acceso a CA PAM	
Actores	Administrador de CA PAM Usuario de CA PAM	
Pre-Requisitos	Cliente de CA PAM instalado Cuentas Privilegiadas registradas en la bóveda de CA PAM	
Descripción	El administrador y/o usuario privilegiado accederá a la solución CA PAM.	
Paso	**Acción**	**Resultado esperado**
1	En caso de iniciar sesión por el cliente CA PAM, El administrador ejecuta el cliente instalado a través del acceso directo en su escritorio.	Cargará la ventana de CA PAM con el campo de *address* y el tipo de conexión.
1.1	El administrador ingresará los siguientes datos y luego seleccionará *"Connect"*: • *Address:* pam.cpb • *Connect Mode*: WEB	Mostrará un cuadro de certificado de confianza.
1.2	El administrador acepta el cuadro de certificado de confianza.	Los cuadros de certificados de confianza se desaparecerán y se mostrará la ventana de inicio de sesión de CA PAM.
2	En caso de iniciar sesión por página web, se deberá abrir una página web con la siguiente ruta https://pam.cpb	Se mostrará la ventana de inicio de sesión de CA PAM.

Paso	Acción	Resultado esperado
3	El administrador ingresa los siguientes datos: • *Username*: 2433a • *Password*: ****** • *Authentication type*: LDAP • *Domain*: pam.cpb Y Seleccionar "*Login*".	Se mostrará la pantalla de menú del CA PAM.
Fin de la Prueba		

CP-02 Generación de Política de Acceso

CP-02	Generación de Política de Acceso
Referencia al Caso de Uso	CU-01 Inicio de sesión
Objetivo	Otorgar acceso a un usuario a un dispositivo.
Actores	Administrador de CA PAM Usuario de CA PAM
Pre-Requisitos	Servicio de CA PAM instalado Usuario y Dispositivo registrados en CA PAM Cuentas Privilegiadas registradas en la bóveda de CA PAM Política de Filtrado de Comando registrado
Descripción	El administrador de CA PAM genera la política de acceso para el usuario.

Paso	Acción	Resultado esperado
1	El administrador ejecuta la tarea *Policies/Manage Policies*, luego seleccionar *Add*.	Se mostrará las opciones disponibles para la creación de una política de acceso.
2	El administrador completa los datos de asociaciones: • *User:* user_test • *Device*: Cisco_Switch_2_Piso_CERT Y selecciona la pestaña Access.	Se mostrará las opciones disponibles para acceso nativo al dispositivo.
3	El administrador selecciona SSH dentro de la sección *Available Access* y selecciona el botón Agregar (>).	Se mostrará el acceso SSH dentro de la sección "*Selected Access*".
4	El administrador selecciona sobre la lupa de la columna Target Account.	Se mostrará las cuentas privilegiadas disponibles para el dispositivo.

Paso	Acción	Resultado esperado
5	El administrador selecciona la cuenta privilegiada netadmin dentro de la sección *Available Target Account* y selecciona el botón Agregar (>).	Se mostrará la cuenta privilegiada dentro de la sección "*Selected Target Account*".
6	El administrador selecciona el botón Ok.	Se mostrará las opciones de la pestaña Access.
7	El administrador selecciona la pestaña Filters.	Se mostrará las opciones de configuración para Filtrado de Comandos.
8	El administrador lista las opciones disponibles en el atributo *Command Filters* y selecciona la política Commands_Block.	La aplicación de filtrado de comandos estará configurada.
9	El administrador selecciona la pestaña *Recording*.	Se mostrará las opcicnes disponibles para grabar la sesión.
10	El administrador selecciona las siguientes. opciones: • *Command Line* • *Bidirectional* • *On Violation*	La aplicación de grabación de sesión estará configurada.
11	El administrador selecciona la pestaña *Transparent Login*.	Se mostrará las opciones disponibles para elevación de privilegios dentro del dispositivo.
12	El administrador lista las opciones disponibles en el atributo *Login* y selecciona la cuenta privilegiada "Cisco_Switch_1_App_SSH - cisco_enable".	La elevación de privilegios estará configurada.
13	El administrador selecciona Ok para que la política de acceso sea creada.	Se mostrará la política creada y las funcionalidades habilitadas.
14	El usuario inicia sesión a través del cliente de CA PAM.	Se mostrará la tabla de accesos con los dispositivos disponibles para el usuario.
15	El usuario selecciona el tipo de acceso SSH debajo de la columna *Acess Methods* del dispositivo "Cisco_Switch_2_Piso_CERT".	CA PAM mostrará el CLI autenticado al dispositivo. Adicionalmente, internamente se notificará por correo al equipo de Seguridad TI.

Paso	Acción	Resultado esperado
16	El usuario ejecuta un comando prohibido, por ejemplo: • Ls	Se mostrará un mensaje de advertencia y la cantidad de intentos de transgresión que tiene el usuario. Adicionalmente, internamente se notificará por correo el intento de transgredir al equipo de Seguridad TI.
17	El usuario eleva privilegios dentro del dispositivo, ejecutando el comando: • *Enable*	Se mostrará dentro del CLI la marca de la elevación de privilegios.
18	El usuario ejecuta un comando prohibido, por ejemplo: • Ls	Se mostrará un mensaje de advertencia y la cantidad de intentos de transgresión que tiene el usuario. Adicionalmente, internamente se notificará por correo el intento de violación al equipo Seguridad TI.
19	El usuario ejecuta un comando prohibido, por ejemplo: • Ll	Se mostrará otra ventana un mensaje de advertencia con los intentos de violación excedidos y se cerrará la sesión al dispositivo automáticamente. Adicionalmente, internamente se notificará por correo el intento de violación al equipo Seguridad TI.
Fin de la Prueba		

CP-03 Acceso a Dispositivo Windows

CP-03	Acceso a Dispositivo Windows	
Referencia al Caso de Uso	CU-01 Inicio de sesión	
Objetivo	Acceder a dispositivo de tipo Windows	
Actores	Usuario de CA PAM	
Pre-Requisitos	Servicio de CA PAM instalado Políticas de Acceso registrado en CA PAM para dispositivos de tipo Web	
Descripción	El usuario desde CA PAM accede a dispositivo Windows y transfiere un archivo.	
1	El usuario selecciona el tipo de acceso "RDP" debajo de la columna "*Acess Methods*" del dispositivo "Ms02_Jump_CERT".	Se mostrará la sesión RDP iniciada.

Paso	Acción	Resultado esperado
2	El usuario desglosa las opciones del tipo de acceso "RDP" debajo de la columna "*Acess Methods*" del dispositivo "Ms02_Jump_CERT".	Se mostrará las opciones de resolución y mapeo de unidades para el dispositivo.
3	El usuario selecciona los siguiente. datos: • *Resolutions: Fullscreen* • *Drive Mapping*: D:\ Y selecciona LAUNCH.	Se mostrará la sesión RDP iniciada. Adicionalmente, internamente se notificará por correo al equipo de Seguridad TI.
4	El usuario en la sesión del dispositivo realiza lo siguiente: • Clic derecho sobre el botón de Inicio y selección Open Windows Explorer.	Se mostrará el explorador de Windows.
5	El usuario selecciona la opción: • "D on xsuite" Dentro de "*Computer*".	Se mostrará el contenido de la unidad "D" del equipo del usuario.
6	El usuario copia un archivo del dispositivo a la unidad de su equipo.	Se mostrará el archivo en la unidad del equipo del usuario.
7	El usuario cierra la sesión al dispositivo Windows.	Se cerrará la ventana del dispositivo de Windows.
Fin de la Prueba		

CP-04 Acceso a Dispositivo Web

CP-04	Acceso a Dispositivo Web	
Referencia al Caso de Uso	CU-01 Inicio de sesión	
Objetivo	Acceder a dispositivo de tipo Web	
Actores	Usuario de CA PAM	
Pre-Requisitos	Servicio de CA PAM instalado Políticas de Acceso registrado en CA PAM para dispositivos de tipo Web	
Descripción	El usuario desde CA PAM accede a dispositivo Web	
1	El usuario selecciona el acceso "ANTISPAM_1" debajo de la columna "Web Portal" del dispositivo "AntiSpam_1_CERT".	Se abrirá el navegador web de CA PAM y se autenticará automáticamente a la aplicación Web. Adicionalmente, internamente se notificará por correo al equipo de Seguridad TI.

Descripción		El usuario desde CA PAM accede a dispositivo Web
2	El usuario cierra la sesión de la aplicación web.	Se cerrará la ventana de la aplicación web.
Fin de la Prueba		

CP-05 Acceso a Dispositivo C/S

CP-05	Acceso a Dispositivo C/S	
Referencia al Caso de Uso	CU-01 Inicio de sesión	
Objetivo	Acceder a dispositivo de tipo C/S	
Actores	Usuario de CA PAM	
Pre-Requisitos	Servicio de CA PAM instalado Políticas de acceso registrado en CA PAM para dispositivos de tipo C/S	
Descripción	El usuario desde CA PAM accede a dispositivo C/S	
Paso	**Acción**	**Resultado esperado**
1	El usuario desglosa las opciones "RDP *Applications*" del dispositivo (*Jump Server*) "Ms02_Jump_CERT".	Se mostrará las aplicaciones de tipo C/S disponibles para el usuario.
2	El usuario selecciona la aplicación "PLSQLDeveloper".	Se mostrará el entorno de la aplicación PL/SQL *Developer* autenticada de manera automática. Adicionalmente, se notificará al equipo de Seguridad TI por el acceso al servidor Windows y a la aplicación C/S.
3	El usuario cierra la aplicación C/S o la sesión Windows para finalizar sesión.	Se cerrará la ventana del aplicativo C/S o la sesión Windows.
Fin de la Prueba		

CP-06 Revisión de Pistas de Auditoria

CP-06	Revisión de Pistas de Auditoría	
Referencia al Caso de Uso	CU-01 Inicio de sesión	
Objetivo	Revisar *logs* de Auditoria	
Actores	Administrador de CA PAM	
Pre-Requisitos	Servicio de CA PAM instalado	
Descripción	El administrador de CA PAM realizará filtros de búsqueda dentro de los *logs*.	
Paso	**Acción**	**Resultado esperado**
1	El administrador ejecuta la tarea *Sessions/Logs*. Para visualizar los siguientes. campos: • Date/Time: Fecha y hora de la transacción. • *User Name*: Usuario que realizo la transacción. • *Device*: Dispositivo donde se realizó la transacción. • *Details*: Información adicional de la transacción.	Se mostrará todos los registros de actividad realizado en los dispositivos como en la consola de administración de CA PAM.
2	El administrador realiza un filtro de búsqueda: • *Columm: User Name* • *Valur: user_test* Y selecciona *Filter*.	Se mostrará todas las actividades realizadas por el usuario *user_test*.
3	El administrador selecciona *Add Filter*.	Se mostrará un criterio adicional de búsqueda.
4	El administrador realiza un filtro de búsqueda: (Sin eliminar el anterior filtro) • *Columm: Transaction* • *Value: Login, Connecctions, Violations.* Y selecciona *Filter*.	Se mostrará todos los registros de: • Inicio de Sesión a CA PAM • Conexión a dispositivos • Intentos de violación.
5	El administrador selecciona un registro y selecciona View.	Se mostrará detalle de la transacción.
Fin de la Prueba		

CP-07 Reproducir Grabación de Sesiones

CP-07	Reproducir Grabación de Sesiones
Referencia al Caso de Uso	CU-01 Inicio de sesión
Objetivo	Reproducir Sesiones
Actores	Administrador de CA PAM
Pre-Requisitos	Servicio de CA PAM instalado
Descripción	El administrador de CA PAM visualiza las sesiones en los dispositivos

Paso	Acción	Resultado esperado
1	El administrador ejecuta la tarea *Sessions/Session Recordings*.	Se mostrará todas las grabaciones de sesiones.
2	El Administrador realiza un filtro de búsqueda: • *Columm: User* • *Value: user_test*	Se mostrará todas las grabaciones de sesión del usuario *user_test*.
3	El administrador selecciona View Recording del dispositivo "Ms02_Jump_CERT" de tipo RDP.	Se abrirá una nueva ventana y se reproducirá la sesión del usuario a la aplicación C/S a través del Jump Server.
4	El administrador cierra la ventana de reproducción de sesiones.	Se mostrará todas las grabaciones de sesión del usuario *user_test*.
5	El administrador selecciona *View Recording* del dispositivo "AntiSpam_1_CERT" de tipo WEB.	Se abrirá una nueva ventana y se reproducirá la sesión del usuario a la aplicación Web a través del navegador de CA PAM.
6	El administrador cierra la ventana de reproducción de sesiones.	Se mostrará todas las grabaciones de sesión del usuario *user_test*.
7	El administrador selecciona *View Recording* del dispositivo "Ms02_Jump_CERT" de tipo RDP del siguiente registro.	Se abrirá una nueva ventana y se reproducirá la sesión de tipo RDP. Además, se mostrarán las marcas/hitos donde se realizó transferencia de archivos.
8	El administrador cierra la ventana de reproducción de sesiones.	Se mostrará todas las grabaciones de sesión del usuario *user_test*.
9	El administrador selecciona *View Recording* del dispositivo "Cisco_Switch_2_Piso_CERT" de tipo CLI resaltado en color rojo.	Se abrirá una nueva ventana y se reproducirá la sesión de tipo CLI. Además, se mostrará los siguientes datos: • Marcas/hitos de intento de violación de comandos. • Marca/hito de elevación de privilegios.

10	El administrador selecciona *Operation* y seguidamente *Find*.	Se mostrará un campo para realizar búsqueda de caracteres.
11	El administrador ingresa la siguiente. palabra: • ls Y presionar la tecla Enter.	Se mostrará el resaltado en blanco la palabra encontrada.
Fin de la Prueba		

CP-08 Generación de Reportes Personalizados

CP-08	**Generación de Reportes Personalizados**
Referencia al Caso de Uso	CU-01 Inicio de sesión
Objetivo	Realizar Reportes Personalizados en CA PAM
Actores	Administrador de CA PAM
Pre-Requisitos	Servicio de CA PAM instalado
Descripción	El Administrador de CA PAM generara reportes personalizados de acuerdo con los criterios disponibles.

Paso	**Acción**	**Resultado esperado**
1	El Administrador ejecuta la tarea *Sessions/Logs*.	Se mostrará todos los registros de actividad realizado en los dispositivos como en la consola de administración de CA PAM.
2	El Administrador realiza un filtro de búsqueda: • *Columm: Service* • *Value: PLSQLDeveloper* Y selecciona *Filter*.	Se mostrará todos los accesos a la aplicación C/S.
3	El administrador selecciona *Reports*, luego *Save As*	Se mostrará las opciones disponibles para generar una nueva plantilla de reportes.
4	El administrador completa los siguientes campos: • *Name*: Reporte de prueba Luego selecciona la pestaña "*Users/Groups*"	Se mostrará el listado de usuarios.
5	El administrador selecciona los usuarios 2433a y hace clic sobre el botón Agregar (**>**).	Se mostrará el usuario seleccionado en la sección "*Selected Users / Groups*".

Paso	Acción	Resultado esperado
6	El administrador selecciona la pestaña "Email".	Se mostrará las opciones disponibles para programar la ejecución y envió del reporte por correo.
7	El administrador selecciona la opción *Send* Emails y completa los siguiente. datos: • Emails: administrador_pam@pam.cpb • Seleccionar "*Weekly*" y luego Friday para que el reporte sea enviado todos los viernes de cada semana. • Finalmente seleccionamos Ok.	Se mostrará todos los *logs* filtrados.
8	El administrador selecciona *Reports*, luego Acceso a PLSQLDeveloper.	Se mostrará todos los registros acordes al filtrado del reporte creado anteriormente.
9	El administrador selecciona *Download*.	Se mostrará una venta de explorador de Windows.
10	El administrador selecciona donde guardar el reporte y selecciona *Save*.	Se mostrará una ventana de transferencia de archivos.
11	El administrador selecciona *Close*.	Se muestra la pantalla de menú del CA PAM.
Fin de la Prueba		

CP-09 Ejecución de Reportes Predefinidos

CP-09	Ejecución de Reportes Predefinidos	
Referencia al Caso de Uso	CU-01 Inicio de sesión	
Objetivo	Ejecutar Reportes de CA PAM	
Actores	Administrador de CA PAM	
Pre-Requisitos	Servicio de CA PAM instalado	
Descripción	El Administrador de CA PAM genera reportes.	
Paso	**Acción**	**Resultado esperado**
1	El Administrador ejecuta la tarea *Sessions* y luego *Logs*.	Se mostrará todos los registros y actividades.
2	El Administrador selecciona *Reports*, luego selecciona la siguiente opción: • PCI 10.2.1 *User Login*	Se mostrará el reporte de auditoría con datos de inicio de sesión a CA PAM.
3	El Administrador selecciona *Download*.	Se mostrará una venta de explorador de Windows.

Paso	Acción	Resultado esperado
4	El Administrador selecciona donde guardar el reporte y selecciona *Save*.	Se mostrará una ventana de transferencia de archivos.
5	El Administrador selecciona *Close*.	Se desaparecerá la ventana de Guardar reporte.
6	El Administrador ejecuta la tarea *Credentials/Reports/Run*	Se mostrará un listado de reportes predefinidos de CA PAM.
7	El Administrador selecciona *Accounts* y luego *Update*.	Se mostrará un conjunto de filtrados para generar el reporte.
8	El Administrador completa los siguientes datos: • *Account Type: Synchronized* • *Password State: All* • *Output Format: HTML* Y seleccionar Ok.	Se abrirá una nueva ventana el reporte generado.
Fin de la Prueba		

Pruebas funcionales

CP-10 Administración CA Privileged Access Manager

CP-10	Administración CA Privileged Access Manager	
Referencia al Caso de Uso	CU-01 Inicio de sesión	
Objetivo	Ver respuesta de acceso a Administración de CA *Privileged Access Manager*	
Actores	Administrador de CA PAM	
Pre-Requisitos	Servicio de CA PAM instalado	
Descripción	Validar el acceso con usuario administrador a la consola de CA PAM	
Paso	**Acción**	**Resultado esperado**
1	El administrador despliega el menú *Sessions* y ejecuta la opción *Logs* o *Session Recordings*.	Se mostrará el listado de actividades o pistas de auditoría ya sea realizado dentro de la consola de CA PAM o en los dispositivos.
2	El administrador despliega el menú *Users* y ejecuta la opción *Manage Users*.	Se mostrará el listado de usuarios importados a CA PAM desde AD.
3	El administrador despliega el menú *Devices* y ejecuta la opción *Manage Devices*.	Se mostrará el listado de dispositivos, entre ellos: RDP, SSH, Web, C/S.
Paso	**Acción**	**Resultado esperado**
4	El administrador despliega el menú de	Se mostrará el listado de políticas de

	Policies y ejecuta la opción *Manage Policies*.	acceso de usuarios a dispositivos.
5	El administrador ejecuta la opción *Configuration*.	Se mostrará un listado de opciones de configuración de CA PAM, siendo los más comunes para su administración: - *3rd Party* - *Clustering* - *Database* - *Diagnostics* - *Network* - *Tools*
Fin de Prueba		

4.3 Etapa Verificar

A Continuación, se hace una revisión del funcionamiento del sistema implementado, con la finalidad de detectar si existió fallas de configuración e implementación.

4.3.1 Fase de evaluación del desempeño.

A continuación, se desarrollan los entregables, resultado de la implementación y el resultado de plan de prueba, para detectar si cumplen con los requerimientos definidos en el plan de implementación del proyecto.

- **Entregable: Resultado de la implementación de CA PAM**

Se realizó un *checklist* interno de la operatividad de la solución implementada, que determina las fallas que estén suscitando.

Resultado de la implementación de las bases de datos

En la siguiente tabla se muestra el resultado de la implementación especificada en el levantamiento de información de equipos del área de base de datos (Ver Tabla 42).

Tabla 42: Resultado del monitoreo de la implementación de las bases de datos

Base de Datos	Nombre del Equipo	Nombre de la Aplicación	Tipo de Apliación	PVP	Both PA and Target System?	Rotacin Contraseña	Observación	Politica Acceso - Super	Config con Aprovacion	Politica Acceso - Cliente 1	Politica Acceso - Cliente 2
cpbpbd	CSRV0101_PROD	CSRV0101_CPBPBD_App_BD	Oracle	Notificar	Si	No	Error de Conexión	Si	No	Si	Si
cpbptd	CSRV011_PROD	CSRV011_CPBPBTD_App_BD	Oracle	Notificar	Si	No	Implementación con éxito	Si	No	Si	Si
cpbtrth	CSRV0107_PROD	CSRV0107_CPBTRTH_App_BD	Oracle	Notificar	No	No	No hay comunicacion desde server y PAM (resuelve nombre pero no hace ping por IP)	no	No	Si	Si
cpbtth	CSRV017_PROD	CSRV017_CPBTTH_App_BD	Oracle	Notificar	No	No	Implementación con éxito	no	No	Si	Si
cpbthru	ZSRV54_PROD	ZSRV54_CPBTHRU_App_BD	Oracle	Notificar	Si	No	Implementación con éxito	Si	No	Si	Si
cpbthru2	ZSRV542_PROD	ZSRV542_CPBTHRU2_App_BD	Oracle	Notificar	Si	No	Implementación con éxito	Si	No	Si	Si
cpblbtr	CSRV0103_PROD	CSRV0103_CPBLBTR_App_BD	Oracle	Notificar	Si	No	Implementación con éxito	Si	No	Si	Si
cpblbr	CSRV013_PROD	CSRV013_CPBLBR_App_BD	Oracle	Notificar	Si	No	Implementación con éxito	Si	No	Si	Si
cpbdwd	CSRV0105_PROD	CSRV0105_CPBDWD_App_BD	Oracle	Notificar	Si	No	Error de Conexión	Si	No	Si	Si
cpbdwd2	CSRV015_PROD	CSRV015_CPBDWD2_App_BD	Oracle	Notificar	Si	No	Implementación con éxito	Si	No	Si	Si
cpbdeal	CSRV0104_PROD	CSRV0104_CPBDEAL_App_BD	Oracle	Notificar	Si	No	Implementación con éxito	Si	No	Si	Si
cpbdeal2	CSRV014_PROD	CSRV014_CPBDEAL2_App_BD	Oracle	Notificar	Si	No	Implementación con éxito	Si	No	Si	Si
XE	DBPAM_PROD	DBPAM_XE_App_BD	Oracle		Si	No	Implementación con éxito	Si	No	Si	Si

Base de Datos	Nombre del Equipo	Nombre de la Aplicación	Tipo de Apliación	PVP	Both PA and Target System?	Rotacin Contraseña	Observación	Politica Acceso - Super	Config con Aprovacion	Politica Acceso - Cliente 1	Politica Acceso - Cliente 2
cpbsicap	CSRV0106_PROD	CSRV0106_CPBSICAP_App_BD	Oracle	Default	Si	No	Error de Conexión	Si	No	Si	Si
cpbsicap2	CSRV016_PROD	CSRV016_CPBSICAP2_App_BD	Oracle	Default	Si	No	Implementación con éxito	Si	No	Si	Si
oradmz	SRVORACLE_PROD	SRVORACLE_ORADMZ_App_BD	Oracle	Default	Si	No	Implementación con éxito	Si	No	Si	Si
oradmz2	SRVORACLE2_PROD	SRVORACLE2_ORADMZ_App_BD	Oracle	Default	Si	No	Implementación con éxito	Si	No	Si	Si
cpbolap	ZSRV52_PROD	ZSRV52_CPBOLAP_App_BD	Oracle	Default	Si	No	Implementación con éxito	Si	No	Si	Si
cpbolap2	ZSRV522_PROD	ZSRV522_CPBOLAP2_App_BD	Oracle	Default	Si	No	Implementación con éxito	Si	No	Si	Si
cpbmeta	Dispositivo ya registrado	ZSRV52_CPBMETA_App_BD	Oracle	Default	Si	No	Implementación con éxito	Si	No	Si	Si
cpbmeta2	Dispositivo ya registrado	ZSRV52_CPBMETA2_App_BD	Oracle	Default	Si	No	Implementación con éxito	Si	No	Si	Si
rmancat	ZSRV01a_PROD	ZSRV01a_RMANCAT_App_BD	Oracle	Default	Si	No	Implementación con éxito	Si	No	Si	Si
rmancat2	ZSRV02a_PROD	ZSRV02a_RMANCAT2_App_BD	Oracle	Default	Si	No	Implementación con éxito	Si	No	Si	Si
ovmmeta	Dispositivo ya registrado	ZSRV52_OVMMETA_App_BD	Oracle	Default	Si	No	Error de Conexión	Si	No	Si	Si
ovmmeta2	Dispositivo ya registrado	ZSRV52_OVMMETA2_App_BD	Oracle	Default	Si	No	Implementación con éxito	Si	No	Si	Si

Fuente: Elaboración de autores

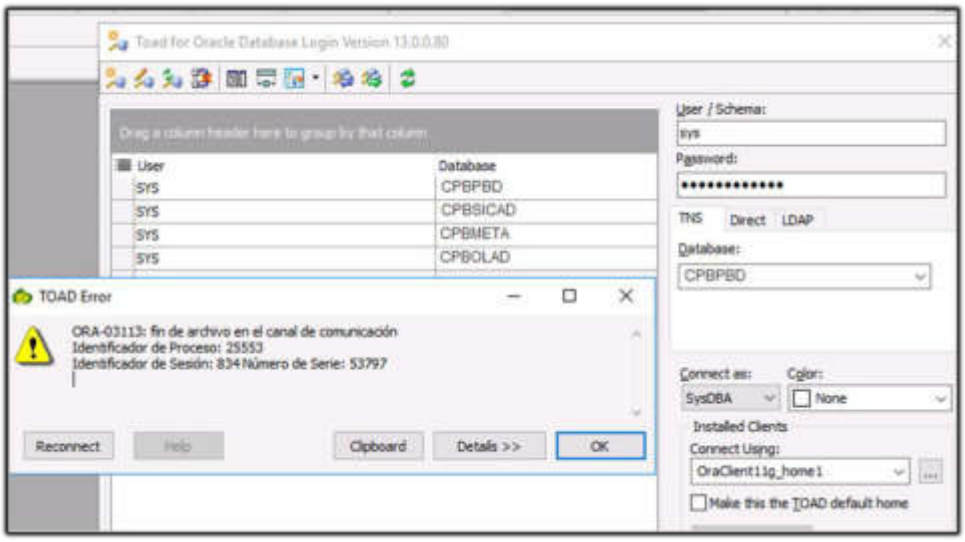
En la tabla se lista todas las bases de datos implementadas y configuradas dentro de CA PAM. Sin embargo, no todas las bases de datos tenían conexión con la solución CA PAM, lo cual generó un error de conexión al momento de acceder a estas. Por ello, se procede a listar y mostrar los errores de cada una.

Los cinco errores identificados de la conexión a las bases de datos son:

- **Base de datos CPBPBD**

En la siguiente imagen se muestra el error al momento de conectarse a la base de datos CPBBD (Ver Figura 41).

Figura 41: Error de conexión con la base de datos cpbpbd.



Fuente: Elaboración de autores

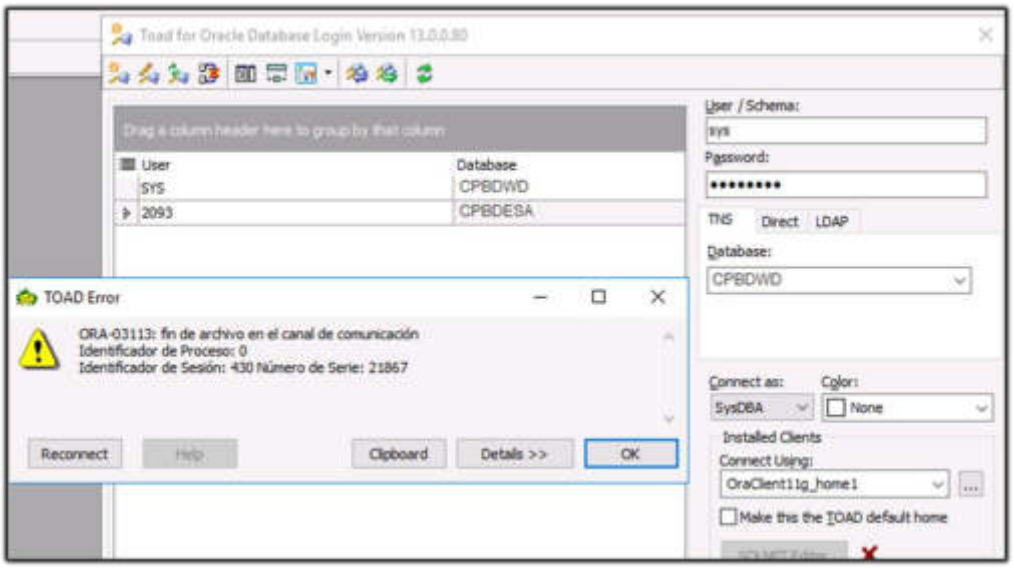
- **Base de datos CPBTRTH.**

El problema detectado en esta base de datos es al momento de establecer la conexión. Esta no carga y no muestra error, al momento de realizar una traza al servidor no se tiene llegada.

- **Base de datos CPBDWD**

En la siguiente imagen se muestra el error al momento de conectarse a la base de datos CPBDWD (Ver Figura 42).

Figura 42: Error de conexión con la base de datos cpbdwd.

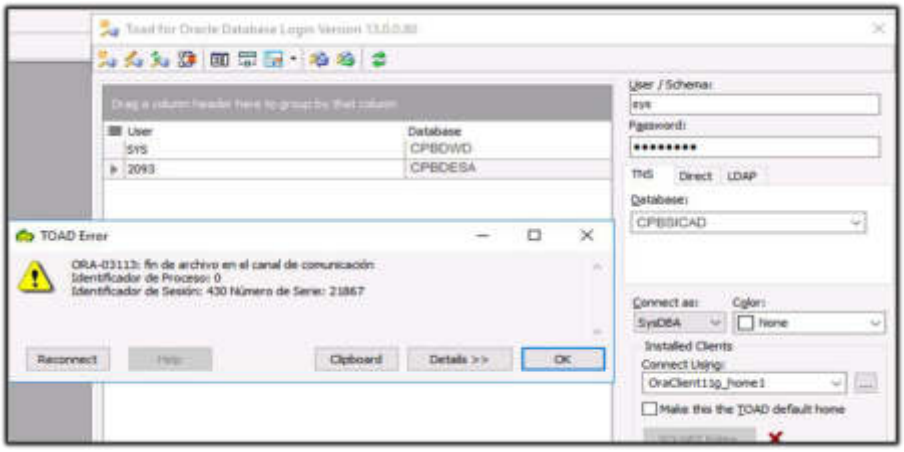


Fuente: Elaboración de autores

- **Base de datos CPBSICAD**

En la siguiente imagen se muestra el error al momento de conectarse a la base de datos CPBSICAD (Ver Figura 43).

Figura 43: Error de conexión con la base de datos cpbsicad.

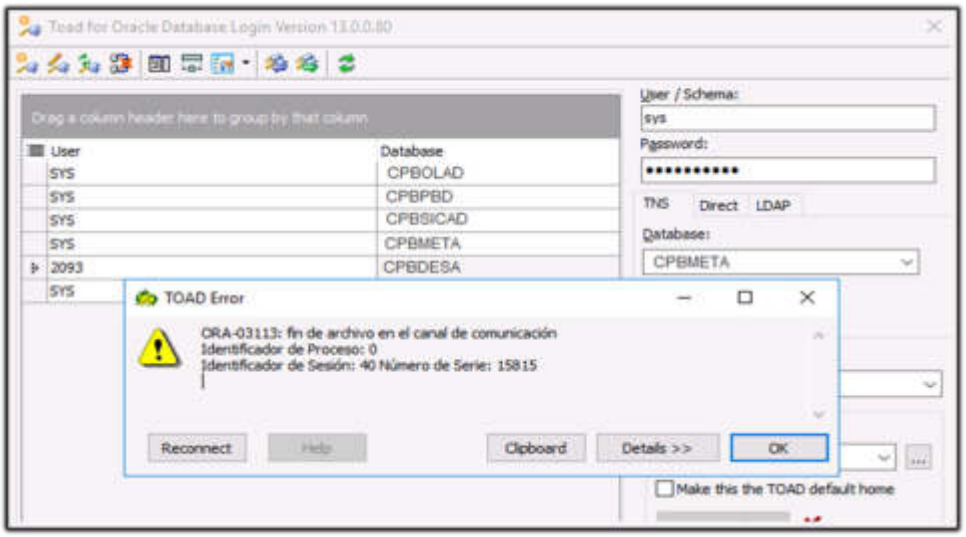


Fuente: Elaboración de autores

- **Base de datos CPBMETA**

En la siguiente imagen se muestra el error al momento de conectarse a la base de datos CPBMETA (Ver Figura 44).

Figura 44: Error de Conexión con la base de datos cpbmeta.



Fuente: Elaboración de autores

Resultado de la implementación de los equipos de seguridad

En la siguiente tabla se muestra el resultado de la implementación especificada en el levantamiento de información de equipos del área de seguridad de redes (Ver Tabla 43).

Tabla 43: Resultado de la implementación de los equipos de seguridad

Tipo Endpoint	Nombre del Equipo	Nombre de la Aplicación	tipo de Aplicación	Nombre de Cuenta	PVP	Rotacion Contraseña	Observación	Politica Acceso - Super	Config con Aprobación
Firewall Aplicaciones Web	Firewall_Aplicaciones_Web_PROD	Firewall_Aplicaciones_Web_App_Web	Generic	2433a	Notificar	No	Instalación con éxito	Si	No
Email Security (Antispam)	Mail.cpb.pe_PROD	Mail.cpb.pe_App_Web	Generic	2433a	Notificar	No	Instalación con éxito	Si	No
Email Security (Antispam)	Mail2.cpb.pe_PROD	Mail2.cpb.pe_App_Web	Generic	2433a	Notificar	No	Instalación con éxito	Si	No
Firewall Corporativo	Firewall_CheckPoint_PROD	Firewall_CheckPoint_App_CS	Generic	2433a	Notificar	No	Ya estaba en Certificacion Jump Server **Problema de caracteres especiales**	Si	No
Firewall (Nodo Principal - Sucursales)	Fortimanager-200D_PROD	Fortimanager-200D_App_Web	Generic	2433a	Notificar	No	Instalación con éxito	Si	No
Firewall (Sucursales)	Fortigate_50E_FW20_1	Fortigate_50E_FW20_1_App_Web	Generic	2433a	Notificar	No	Si, pero no hay comunicacion entre pam y fortinet para probar acceso	Si	No
	Fortigate_50E_FW20_2	Fortigate_50E_FW30_2_App_Web	Generic	2433a	Notificar	No	Si, pero no hay comunicacion entre pam y fortinet para probar acceso	Si	No
	Fortigate_50E_FW20_3	Fortigate_50E_FW40_3_App_Web	Generic	2433a	Notificar	No	Si, pero no hay comunicacion entre pam y fortinet para probar acceso	Si	No
	Fortigate_50E_FW20_4	Fortigate_50E_FW50__App_Web	Generic	2433a	Notificar	No	Si, pero no hay comunicacion entre pam y fortinet para probar acceso	Si	No
	Fortigate_50E_FW20_5	Fortigate_50E_FW60_Arequipa_App_Web	Generic	2433a	Notificar	No	Si, pero no hay comunicacion entre pam y fortinet para probar acceso	Si	No
	Fortigate_50E_FW20_6	Fortigate_50E_FW70_Huancayo_App_Web	Generic	2433a	Notificar	No	Si, pero no hay comunicacion entre pam y fortinet para probar acceso	Si	No
	Fortigate_50E_FW20_7	Fortigate_50E_FW80_Puno_App_Web	Generic	2433a	Notificar	No	Si, pero no hay comunicacion entre pam y fortinet para probar acceso	Si	No

Tipo Endpoint	Nombre del Equipo	Nombre de la Aplicación	tipo de Aplicación	Nombre de Cuenta	PVP	Rotacion Contraseña	Observación	Politica Acceso - Super	Config con Aprobación
Web Security (Proxy)	Mcafee_Web_Gateway_PROD	Mcafee_Web_Gateway_App_Web	Generic	2433a	Notificar	No	Se configuro Server (Firefox) y da error porque la contraseña tiene caracteres especiales "$". Cuando lo inyecta lo define como numerico "4"	Si	No
SSL/VPN	SSL-VPN_Junos_PROD	SSL-VPN_Junos_App_Web	Generic	2433a	Notificar	No	Instalación con éxito	Si	No
Balanceador de enlaces	Fortinet_Ascelink_PROD	Fortinet_Ascelink_PROD_App_Web	Generic	2433a	Notificar	No	No se tiene Conexión	Si	No
SIEM	SIEM_PROD	SIEM_App_Web	Generic	NGCP	Notificar	No	da error porque la contraseña tiene caracteres especiales "$". Cuando lo inyecta lo define como numerico "4"	Si	No
Antivirus	___	___	___	___	___	___	No se creo aun el dispositivo. Utiliza Microsoft Management Console para administrar la consola de antivirus.	___	___
Servidor Proxy	Squid_Proxy_PROD	Squid_Proxy_App_SSH	UNIX	2433a	Notificar	No	Instalación con éxito	Si	No
DNS Externo, DHCP	cpbNET_PROD	cpbNET_App_SSH	UNIX	2433a	Notificar	No	Instalación con éxito	Si	No

Fuente: Elaboración de autores

Durante la evaluación del funcionamiento de la solución implementada, se detectaron varios inconvenientes con los dispositivos integrados en CA PAM.

Lista de estos errores.

- Firewall Corporativo: No inyecta caracteres especiales, por ejemplo, al ingresar el carácter “$”, nos remplaza por el número 4.
- Firewalls sucursales: Los 7 firewall ubicados en Perú no tiene comunicación con la solución.
- En el servidor Web Security: No inyecta caracteres especiales, por ejemplo, al ingresar el carácter “$”, nos remplaza por el número 4.
- Balanceador de enlace: No hay comunicación.
- SIEM: No inyecta caracteres especiales, por ejemplo, al ingresar el carácter “$”, nos remplaza por el número 4.
- Aún está pendiente la implementación del servicio del Antivirus.

Resultado de la implementación de los equipos del área de redes

En la siguiente tabla se muestra el resultado del monitoreo de la implementación del área de redes (Ver Tabla 44).

Tabla 44: Resultado de equipos del área de redes

Tipo de Equipo	Modo de acceso	Name del Equipo	Plataforma	Direccion IP Privada	PVP	Rotacion Contraseña	Tipo de Conexión	Politica Acceso - Super	Puerto	Observación
Switch	SSH /Telnet	OP-SW-S3	Cisco IOS	172.30.4.37	Notificar	No	Local	Si	21/22/23	Instalación con éxito
Switch	SSH /Telnet	OP-SW-S1A	Cisco IOS	172.30.4.38	Notificar	No	Local	Si	21/22/23	Instalación con éxito
Switch	SSH /Telnet	OP-SW-S1C1	Cisco IOS	172.30.4.39	Notificar	No	Local	Si	21/22/23	Instalación con éxito
Switch	SSH /Telnet	OP-SW-S1C1	Cisco IOS	172.30.4.40	Notificar	No	Local	Si	21/22/23	Instalación con éxito
Switch	SSH /Telnet	OP-SW-P1A	Cisco IOS	172.30.4.41	Notificar	No	Local	Si	21/22/23	Instalación con éxito
Switch	SSH /Telnet	OP-SW-P1C	Cisco IOS	172.30.4.42	Notificar	No	Local	Si	21/22/23	Instalación con éxito
Switch	SSH /Telnet	OP-SW-P1C1	Cisco IOS	172.30.4.43	Notificar	No	Local	Si	21/22/23	Instalación con éxito
Switch	SSH /Telnet	OP-SW-P2A	Cisco IOS	172.30.4.44	Notificar	No	Local	Si	21/22/23	Instalación con éxito
Switch	SSH /Telnet	OP-SW-P2C	Cisco IOS	172.30.4.45	Notificar	No	Local	Si	21/22/23	Instalación con éxito
Switch	SSH /Telnet	OP-SW-P3	Cisco IOS	172.30.4.46	Notificar	No	Local	Si	21/22/23	Instalación con éxito
Switch	SSH /Telnet	OP-SW-P3A	Cisco IOS	172.30.4.47	Notificar	No	Local	Si	21/22/23	Instalación con éxito
Switch	SSH /Telnet	OP-SW-P3C	Cisco IOS	172.30.4.48	Notificar	No	Local	Si	21/22/23	Instalación con éxito
Switch	SSH /Telnet	OP-SW-P5	Cisco IOS	172.30.4.49	Notificar	No	Local	Si	21/22/23	Instalación con éxito
Switch	SSH /Telnet	OP-SW-P6	Cisco IOS	172.30.4.50	Notificar	No	Local	Si	21/22/23	Instalación con éxito
Switch	SSH /Telnet	OP-SW-P7	Cisco IOS	172.30.4.51	Notificar	No	Local	Si	21/22/23	Instalación con éxito
Switch	SSH /Telnet	MUSEO-SW-P4	Cisco IOS	172.30.4.52	Notificar	No	Local	Si	21/22/23	Instalación con éxito
Switch	SSH /Telnet	CNM-SW-2A	Cisco IOS	172.30.4.53	Notificar	No	Local	Si	21/22/23	Instalación con éxito
Switch	SSH /Telnet	CNM-SW-2B	Cisco IOS	172.30.4.54	Notificar	No	Local	Si	21/22/23	Instalación con éxito

Tipo de Equipo	Modo de acceso	Name del Equipo	Plataforma	Direccion IP Privada	PVP	Rotacion Contraseña	Tipo de Conexión	Politica Acceso - Super	Puerto	Observación
Switch	SSH /Telnet	CNM-SW-OCN	Cisco IOS	172.30.4.55	Notificar	No	Local	Si	21/22/23	Instalación con éxito
Switch	SSH /Telnet	CNM-SW-2C	Cisco IOS	172.30.4.56	Notificar	No	Local	Si	21/22/23	Instalación con éxito
Switch	SSH /Telnet	CID-SW-P1	Cisco IOS	172.30.4.57	Notificar	No	Local	Si	21/22/23	Instalación con éxito
Switch	SSH /Telnet	CID-SW-P4	Cisco IOS	172.30.4.58	Notificar	No	Local	Si	21/22/23	Instalación con éxito
Switch	SSH /Telnet	CID-SW-P4A1	Cisco	172.30.4.59	Notificar	No	Local	Si	21/22/23	Instalación con éxito
Switch	SSH /Telnet	CID-SW-P4A2	Cisco	172.30.4.100	Notificar	No	Local	Si	21/22/23	Instalación con éxito
Switch	SSH /Telnet	Switch LAB CU	Cisco	172.30.4.62	Notificar	No	Local	Si	21/22/23	No hay conexión con el equipo
controlador wifi	SSH /Telnet/Web	OP-SW-S3-Huawei	Huawei	172.30.4.102	Notificar	No	Local	Si	21/22/23/7000	Instalación con éxito
controlador wifi	SSH /Telnet/Web	OP-SW-S1C-huawei	Huawei	172.30.4.103	Notificar	No	Local	Si	21/22/23/7000	Instalación con éxito
controlador wifi	SSH /Telnet/Web	OP-SW-S3-1-huawei sala de capacitacion	Huawei	172.30.4.104	Notificar	No	Local	Si	21/22/23/7000	Instalación con éxito
Aruba AirWave	SSH /Telnet/Web	CPB1	Cisco Nexus Operating System (NX-OS)	172.30.2.146	Notificar	No	Local	Si	21/22/23	Instalación con éxito
Roouter	SSH /Telnet/Web	CPB1-CORE1	Cisco Nexus Operating System (NX-OS)	172.30.2.121	Notificar	No	Local	Si	21/22/23	No hay conexión con el equipo

Tipo de Equipo	Modo de acceso	Name del Equipo	Plataforma	Direccion IP Privada	PVP	Rotacion Contraseña	Tipo de Conexión	Politica Acceso - Super	Puerto	Observación
Roouter	SSH /Telnet/Web	CPB1-ENTERPRISE1	Cisco Nexus Operating System (NX-OS)	172.30.2.251	Notificar	No	Local	Si	21/22/23	No hay conexión con el equipo
Roouter	SSH /Telnet/Web	CPB2	Cisco Nexus Operating System (NX-OS)	172.30.2.147	Notificar	No	Local	Si	21/22/23	Instalación con éxito
Roouter	SSH /Telnet	CPB2-CORE2	Cisco Nexus Operating System (NX-OS)	172.30.2.122	Notificar	No	Local	Si	21/22/23	Instalación con éxito
Roouter	SSH /Telnet	CPB2-ENTERPRISE2	Cisco Nexus Operating System (NX-OS)	172.30.2.252	Notificar	No	Local	Si	21/22/23	Instalación con éxito
Roouter	SSH /Telnet	CPB3	Cisco Nexus Operating System (NX-OS)	172.30.2.148	Notificar	No	Local	Si	21/22/23	Instalación con éxito
Roouter	SSH /Telnet	CPB3-CORE3	Cisco Nexus Operating System (NX-OS)	172.30.2.123	Notificar	No	Local	Si	21/22/23	Instalación con éxito
	SSH /Telnet	CPB3-ENTERPRISE3	Cisco Nexus Operating System (NX-OS)	172.30.2.253	Notificar	No	Local	Si	21/22/23	Credenciales incorrectos
	SSH /Telnet	Brocade SAN0-OP	Cisco IOS	172.30.2.25	Notificar	No	Local	Si	21/22/23	Instalación con éxito
	SSH /Telnet	Brocade SAN1-OP	Cisco IOS	172.30.2.26	Notificar	No	Local	Si	21/22/23	Instalación con éxito
Administrador ancho de banda Equipos Core	SSH /Telnet	Brocade SAN0-CER	Cisco IOS	172.30.2.27	Notificar	No	Local	Si	21/22/23	Instalación con éxito
	SSH /Telnet	Brocade SAN1-CER	Cisco IOS	172.30.2.28	Notificar	No	Local	Si	21/22/23	Instalación con éxito
	SSH /Telnet	srv-op-xpc00	Expressway Core PUB	172.30.5.27	Notificar	No	Local	Si	21/22/23	Instalación con éxito
	SSH /Telnet	srv-op-xpe01	Expressway Edge PUB	192.168.79.4	Notificar	No	Local	Si	21/22/23	Instalación con éxito
	SSH /Telnet	srv-op-ts00	Telepresence Server	172.30.5.26	Notificar	No	Local	Si	21/22/23	Instalación con éxito

Fuente: Elaboración de autores

Durante el monitoreo se detectó que 4 equipos presentaron problemas, los equipos en mención son:

- Switch LAB CU: Mensaje error de Conexión.
- CPB1-CORE1: Mensaje error de Conexión.
- CPB1-ENTERPRISE1: Mensaje error de Conexión.
- CPB3-ENTERPRISE3: Las credenciales registradas en el levantamiento de información no coincidían con la que estaba registrada en el sistema.

Nota: Los errores identificados son corregidos en el entregable Levantamiento de observaciones de la implementación.

- **ENTREGABLE: Resultado de Plan de Prueba**

El presente plan de prueba aplicado ha sido previamente aprobado por los clientes 1 y 2 de la empresa de retail.

A continuación, el resultado de las pruebas funcionales (Ver tabla 45) y el resultado de la prueba unitaria (Ver tabla 46).

Pruebas funcionales

Tabla 45: Resultado de las pruebas funcionales

ID	Pruebas Funcionales	Aprobador	Resultado
CP-01	Inicio de sesión	Cliente 1 y 2	OK
CP-02	Generación de Políticas de Acceso	Cliente 1 y 2	OK
CP-03	Acceso a Dispositivo Windows	Cliente 1 y 2	OK
CP-04	Acceso a Dispositivo Web	Cliente 1 y 2	OK
CP-05	Acceso a Dispositivo C/S	Cliente 1 y 2	OK
CP-06	Revisión de Pistas de Auditoria	Cliente 1 y 2	OK
CP-07	Reproducir Grabación de Sesiones	Cliente 1 y 2	OK
CP-08	Generación de Reportes Personalizados	Cliente 1 y 2	OK
CP-09	Ejecución de Reportes predefinidos	Cliente 1 y 2	OK

Fuente: Elaboración de autores

Pruebas Unitarias

Tabla 46: Resultado de las pruebas unitarias

ID	Pruebas Unitarias	Aprobador	Estado
CU-10	Administration CA Privileged Access Manager	Cliente 1 y 2	OK

Fuente: Elaboración de autores

4.4 Etapa Actuar

A continuación, se lleva a cabo la corrección de los errores encontrados en la etapa anterior, con la finalidad de cumplir con los objetivos propuestos al inicio de este proyecto.

4.4.1 Fase de mejora.

Durante la evaluación del funcionamiento de la solución, se ha detectado varias fallas acerca de las funcionalidades de los servicios implementados, por tal motivo, se procede a analizar y a discutir acerca de los posibles causantes de estos problemas. Una vez detectada y plasmada la solución, se pone en marcha la corrección con la finalidad de cubrir las brechas que puedan afectar el cumplimento de los objetivos propuestos en el plan de implementación del proyecto.

- **Entregable: Levantamiento de observaciones de la implementación**

En este documento se muestra las correcciones aplicadas a las fallas detectadas en la etapa de verificar.

a. Levantamiento de observaciones en el área de base de datos

En la siguiente tabla se hace una descripción de las fallas detectadas en la verificación de la conexión y funcionamiento de los dispositivos del área de BD. Además, se muestran las soluciones aplicadas para corregir los errores (Ver Tabla 47).

Tabla 47: Dispositivos observados del área de base de datos

Fallas	Solución
Error de conexión a cpbpbd.	El equipo estuvo en mantenimiento, al conectar a la red de la empresa se validó correcto funcionamiento.
No tiene llegada a cpbtrth.	El servidor fue dado de baja por el cliente, por tal motivo presenta el problema.
Error de conexión a cpbdwd.	Se cambió el pach cord que va desde el servidor de base de datos al switch.
Error de conexión a cpbsicad.	El servidor estuvo apagado, se encendió y se restableció la conexión.
Error de conexión a cpbmeta.	El administrador de red detectó y solucionó el problema de una duplicidad de direccionamiento IP.

Fuente: Elaboración de autores

b. Levantamiento de observaciones en el área de seguridad de la información

En la siguiente tabla se hace una descripción de las fallas detectadas durante la verificación de la conexión y del funcionamiento de los dispositivos del área de seguridad de la información. Además, se muestran las soluciones aplicadas para corregir los errores (Ver Tabla 48).

Tabla 48: Dispositivos observados del área de seguridad de la información

Fallas	Solución
Error de conexión a cpbpbd.	El equipo estuvo en mantenimiento, al conectar a la red de la empresa se validó correcto funcionamiento.
No tiene llegada a cpbtrth.	El servidor fue dado de baja por el cliente, por tal motivo presenta el problema.
Error de conexión a cpbdwd.	Se cambió el pach cord que va desde el servidor de base de datos al switch.
Error de conexión a cpbsicad.	El servidor estuvo apagado, se encendió y se restableció la conexión.
Error de conexión a cpbmeta.	El administrador de red detectó y solucionó el problema de una duplicidad de direccionamiento IP.

Fuente: Elaboración de autores

c. Levantamiento de observaciones en el área de redes

En la siguiente tabla se hace una descripción de las fallas detectadas durante la verificación de la conexión y del funcionamiento de los dispositivos del área de redes. Además, se muestran las soluciones aplicadas para corregir los errores (Ver Tablas 49)

Tabla 49: Dispositivos observados del área de redes

Fallas	Solución
Sin conexión a Cisco *Prime Infrastructure*	El equipo estuvo apagado, se encendió y se restableció la conexión.
Sin conexión a Cisco DCNM.	El equipo fue dado de baja por el cliente, por tal motivo presenta el problema
Sin conexión a Switch_Switch LAB CU_PROD.	Puerto del equipo averiado, se cambia a otro puerto de conexión, se restablece la gestión.
Credenciales incorrectas para acceder a *clearpass*	El cliente brinda credenciales correctas.

Fuente: Elaboración de autores

- **Entregable: Guía de Usuario**

El propósito del documento es orientar al usuario administrador para que pueda acceder a las plataformas de la empresa de retail, a través de una autenticación segura en CA PAM (Ver Anexo 3).

- **Entregable: Plan de Recuperación del Servicio**

Los procedimientos que se describen en este punto permiten recuperar el servicio *CA Privileged Access Manager*. Los *backups* de ambos PAM están configurados para que se guarden automáticamente y puedan ser enviados a un repositorio externo definido por la empresa de retail. Estos *backups* permitirán recuperar la solución *CA Privileged Access Manager* ante incidentes o desastres (Ver Anexo 4).

- **Entregable: Guía de Proveedor**

El propósito del documento es orientar a los proveedores de la empresa de retail a que puedan acceder a las plataformas (routers, switch, servidores base de datos, correo, archivo, etc.) que tiene implementada la empresa a través de la consola de CA PAM (Ver Anexo 5).

En el siguiente capítulo se describen las pruebas y resultados obtenidos luego de la implementación de la solución.

CAPÍTULO V
PRUEBAS Y RESULTADOS

En este capítulo se presenta la planificación de las pruebas y técnicas usadas para garantizar el correcto funcionamiento de la solución *Privileged* Access *Manager*. La cual permite disminuir el riesgo interno de seguridad informática con los activos de TI y tiene la trazabilidad de todas las actividades realizadas por los administradores del área de redes, seguridad y base de datos de la empresa de retail.

Los resultados esperados se muestran en relación con cada objetivo específico propuesto al inicio de la tesis.

5.1 Pruebas de objetivos

- **Objetivo Específico 1: Reducir el tiempo del proceso de autenticación en los activos de TI, mejorando la eficiencia operacional**

Se midió el cumplimiento de este objetivo específico realizando una encuesta a los usuarios que tienen cuentas privilegiadas, para acceder a los activos de TI en la empresa de retail. Las encuestas se basaron en 7 preguntas (Ver Anexo 6).

- **Objetivo Específico 2: Mitigar el riesgo de extracción de información de los activos de TI por usuarios no autorizados.**

Se mide en base al reporte del registro del log que se realiza en CA PAM. Esto consiste en registrar todas las acciones que el cliente debe realizar

desde el momento que accede al sistema CA PAM hasta finalizar la sesión.

- **Objetivo Específico 3: Reducir el tiempo del proceso de aprobación de acceso a dispositivos críticos en producción de la empresa.**

El objetivo se midió realizando una comparación entre el proceso que estaba antes con el proceso existente luego de la implementación de la solución.

- **Objetivo General: Mejorar la gestión de identidades privilegiadas de los administradores de las plataformas de TI en la empresa de retail**

Se midió en base al reporte del registro del log realizado por la solución CA PAM, esto consiste en registrar todas las acciones del cliente tal como se ha descrito en el resultado del objetivo 2 del capítulo 5.2 de este documento.

5.2 Resultados de objetivos

- **Objetivo Específico 1: Reducir el tiempo del proceso de autenticación en los activos de TI, mejorando la eficiencia operacional**

Se muestran los resultados de la encuesta realizada a los usuarios de la empresa de retail.

Pregunta 1: ¿A cuántos activos de TI tiene acceso? (Ver Figura 45). La cantidad de accesos a los activos es la misma antes y después de la implementación de la solución. Como respuesta se obtuvo que el 34.8% de usuarios tienen de 16 a 20 cuentas de acceso a los activos de TI.

Figura 45: Resultado de encuesta: Pregunta 1.

Fuente: Elaboración de autores

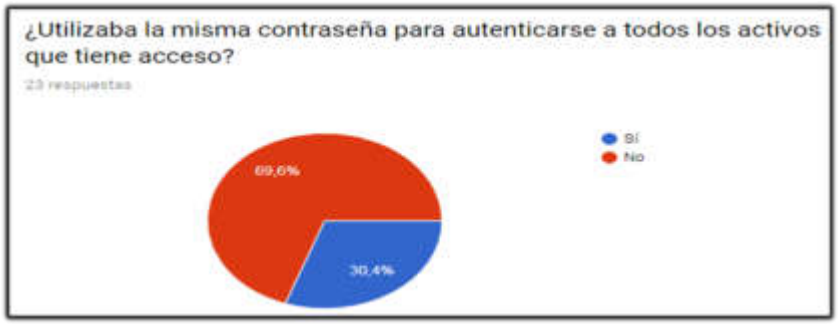
Pregunta 2: ¿A cuántos activos de TI accede al día? (Ver Figura 46). La cantidad de veces que accede a los activos en un día es la misma antes y después de la implementación de la solución. Como respuesta se obtuvo que el 34.8% de usuarios accede entre 6 a 10 activos de TI al día.

Figura 46: Resultado de encuesta: Pregunta 2.

Fuente: Elaboración de autores

Pregunta 3: ¿Utilizaba la misma contraseña para autenticarse a todos los activos que tiene acceso? (Ver Figura 47). De esta pregunta se obtuvo que más del 69% de usuarios utilizaban la misma cuenta para acceder a todos los activos que tenía acceso.

Figura 47: Resultado de encuesta: Pregunta 3.



Fuente: Elaboración de autores

Pregunta 4: Fue respondida solo por las personas que contestaron NO en su respuesta de la pregunta 3. ¿Cuántas credenciales en total utiliza para autenticarse a todos los activos de TI? (Ver Figura 48). Como respuesta a esta pregunta se obtuvo que más del 37% de los usuarios utiliza entre 6 a 10

credenciales, esto origina el problema descrito en la pregunta 5.

Figura 48: Resultado de encuesta: Pregunta 4.

Fuente: Elaboración de autores

Pregunta 5: ¿Tenía registrado sus contraseñas en algún post-it, bloc de notas, celular o en algún otro lugar? (Ver Figura 49). El resultado que se obtuvo de esta pregunta es que el 85 % de usuarios si utilizaba uno de esos medios para registrar sus contraseñas y no olvidarse. Esto se debía a que tenían diferentes contraseñas y aprendérselas era complejo.

Figura 49: Resultado de encuesta: Pregunta 5.

Fuente: Elaboración de autores

Pregunta 6: ¿Cuánto tiempo tardaba en autenticarse a un activo de TI? (Ver Figura 50). Los usuarios tardaban en promedio de 1 a 2 minutos, esto se debía a que primero tenían que ubicar la nota donde estaba anotada la contraseña para luego recién ingresarla.

Figura 50: Resultado de encuesta: Pregunta 6.

Fuente: Elaboración de autores

Pregunta 7: ¿Cuánto tiempo tarda en autenticarse a CA PAM? (Ver Figura 51). Como respuesta se obtuvo que el usuario para autenticarse y acceder a CA PAM se demora un tiempo promedio de 31 a 59 segundos. Sin embargo, desde el momento que accede al sistema el usuario ya no necesita ingresar credenciales para acceder a los activos que tiene autorizado ya que estos activos están integrados en CA PAM.

Figura 51: Resultado de encuesta: Pregunta 7.

Fuente: Elaboración de autores

Se concluye tal como se muestra en la tabla (Ver Tabla 50), que el usuario tiene en promedio 20 accesos a identidades privilegiadas, al día accede en promedio de 6 a 10 activos y para cada uno tiene una contraseña distinta lo cual origina que tenga que anotarlo en algún lugar para no olvidarse. Por ello el tiempo de conexión a un activo es de 1 a 2 minutos de manera que se determina que el usuario se tarda en promedio 20 minutos en autenticarse a todos sus activos que utiliza durante el día. En cambio, con la solución CA PAM el tiempo se reduce como máximo a un minuto, tal como se muestra en el resultado de la pregunta número 7.

Tabla 50: Resultado tiempo de autenticación

Evaluación	Antes	Actual
Cantidad de accesos totales a los activos de TI.	20 accesos	20 accesos
Cantidad de acceso al día a los activos de TI	10 accesos	10 accesos
Cantidad de credenciales	10 credenciales	1 credencial
Credenciales anotadas en algún lugar	SI	NO
Tiempo en autenticarse a un activo de TI	2 minutos	1 minuto
Tiempo total en autenticarse	**20 minutos**	**1 minuto**

Fuente: Elaboración de autores

- **Objetivo Específico 2: Mitigar el riesgo de extracción de información de los activos de TI por usuarios no autorizados.**

Se muestra el resultado de las pruebas realizadas del registro de las actividades de los usuarios cuando se encuentran dentro de los dispositivos.

a. El registro de inicio de sesión.

En la siguiente tabla se muestra el registro del log de los usuarios que accedieron y los que fueron denegados el acceso al sistema de CA PAM. Los datos que se muestran son: la fecha de autenticación, el nombre de usuario, el tipo de proceso (*login o logout*), el grupo al que pertenece el usuario, la dirección IP de la máquina de donde se está conectando y por último el detalle de la conexión (conexión exitosa o error de conexión) (Ver tabla 51).

Tabla 51: Registro de acceso al sistema CA PAM

Fecha	Username	Transaction	Grupos de Usuario	Nat/Proxy IP	Detalle
20181010152416	super	login	--	172.30.1.200	PAM-CMN-0917: User super logged in successfully via local authentication.
20181010173111	super	login	--	172.30.1.200	PAM-CMN-0900: Bad User ID or Password.
20181010173209	system	login	--	172.30.1.200	PAM-CMN-0917: User super logged in successfully via local authentication.
20181010173419	__xcd_cluster__(Cluster member pam01)	login	--	172.30.2.242	PAM-CMN-0917: User super logged in successfully via local authentication.
20181010174520	CN=2138,OU=TI,OU=OP,OU=CPB,DC=CPB.	login	CN=CAPAMUser,CN=Users,DC=CPB.	172.30.18.94	PAM-CMN-0917: User super logged in successfully via local authentication.
20181010174721	system	login	--	172.30.18.94	PAM-CMN-0917: User super logged in successfully via local authentication.
20181010182422	__xcd_cluster__(Cluster member pam01)	login	--	172.30.2.242	PAM-CMN-0917: User super logged in successfully via local authentication.
20181010180428	CN=2092,OU=TI,OU=OP,OU=CPB,DC=CPB.	login	CN=CAPAMAdmin,CN=Users,DC=CPB.	172.30.18.92	PAM-CMN-0917: User super logged in successfully via local authentication.
20181010181430	system	login	--	172.30.18.92	PAM-CMN-0917: User super logged in successfully via local authentication.
20181010181622	CN=2341,OU=TI,OU=OP,OU=CPB,DC=CPB.	login	CN=CAPAMUser,CN=Users,DC=CPB.	172.30.18.121	PAM-CMN-0917: User super logged in successfully via local authentication.
20181010182428	system	login	--	172.30.18.121	PAM-CMN-0917: User super logged in successfully via local authentication.
20181010182433	CN=2341,OU=TI,OU=OP,OU=CPB,DC=CPB.	login	CN=CAPAMUser,CN=Users,DC=CPB.	172.30.18.121	PAM-CMN-0900: Bad User ID or Password.
20181010182459	system	login	--	172.30.18.121	PAM-CMN-0917: User super logged in successfully via local authentication.
20181010183418	CN=2341,OU=TI,OU=OP,OU=CPB,DC=CPB.	login	CN=CAPAMUser,CN=Users,DC=CPB.	172.30.18.121	PAM-CMN-0900: Bad User ID or Password.
20181010183525	CN=2341,OU=TI,OU=OP,OU=CPB,DC=CPB.	login	CN=CAPAMUser,CN=Users,DC=CPB.	172.30.18.121	PAM-CMN-0900: Bad User ID or Password.
20181010183910	system	login	--	172.30.18.121	PAM-CMN-0900: Bad User ID or Password.
20181010184332	2341	login	--	172.30.18.121	PAM-CMN-0900: Bad User ID or Password.
20181010184423	2341	login	--	172.30.18.121	PAM-CMN-0900: Bad User ID or Password.
20181010184416	2341	login	--	172.30.18.121	PAM-CMN-0900: Bad User ID or Password.
20181010184504	2341	login	--	172.30.18.121	PAM-CMN-0900: Bad User ID or Password.
20181010184838	system	login	--	172.30.18.92	PAM-CMN-0629: LDAPS connection made to CPB..636.
20181010185048	CN=2138,OU=TI,OU=OP,OU=CPB,DC=CPB.	login	CN=CAPAMUser,CN=Users,DC=CPB.	172.30.18.94	PAM-CMN-0917: User 2138 logged in successfully via ldap+radius authentication.
20181010185225	system	login	--	172.30.18.94	PAM-CMN-0629: LDAPS connection made to CPB..636.
20181010185429	CN=2138,OU=TI,OU=OP,OU=CPB,DC=CPB.	login	CN=CAPAMUser,CN=Users,DC=CPB.	172.30.18.94	PAM-CMN-0917: User 2138 logged in successfully via ldap+radius authentication.
20181010185432	system	login	--	172.30.18.94	PAM-CMN-0629: LDAPS connection made to CPB..636.

Fuente: Elaboración de autores

A continuación, se presenta de forma gráfica los valores con respecto a la gestión de identidades, los datos fueron extraídos de los registros de inicio de sesión (Ver Figura 52).

Figura 52: Resultado de estado de autenticación.

Fuente: Elaboración de autores

La evaluación de esta gráfica se basa en una muestra de un total de 142 registros de inicios de sesión, de los cuales el 81% del proceso de autenticación se dio de manera satisfactoria y el 19% del acceso fue rechazado. En cifras, se estima que fueron 115 autenticaciones correctas y 27 autenticaciones fallidas, esto se debe a que ingresaron el usuario y/o *password* incorrectos o que la cuenta estaba deshabilitada.

b. Gestión de acceso al activo de TI.

En la siguiente tabla se muestra el registro de los usuarios que accedieron a los activos de TI. Además de las actividades que realizaron estando dentro, de este reporte se consideraron los siguientes datos: la fecha y hora de la modificación, creación o eliminación de un dato del activo de TI, el nombre del usuario que realizó esta actividad, el nombre del activo al que ingresó y el detalle de los cambios que realizó (Ver tabla 52).

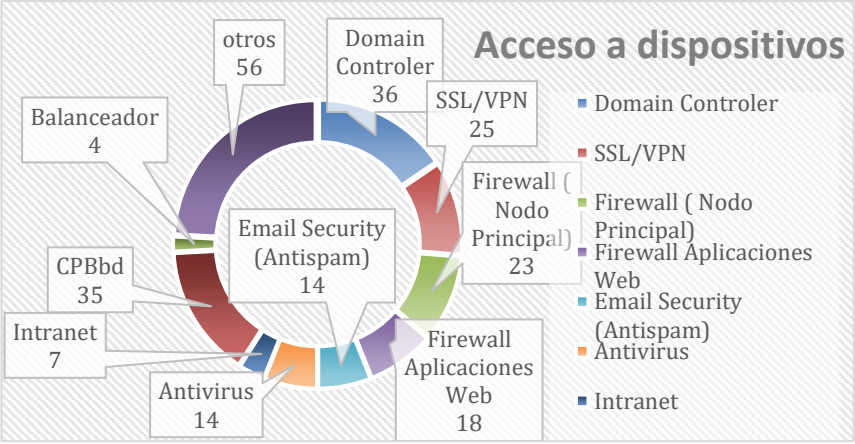
Tabla 52: Gestión de acceso a los activos de TI con CA PAM

DateTime	Usernam	Device	Detalle del proceso
20181010183490	super	--	Log records viewed
20181010183491	super	Domain Controler	Log records viewed
20181010183500	2138	CPBbd	Possibly the remote server is powered off or security settings are too high. Deleting the file: pam02-0000000114-1534792258372_VNC
20181010183501	2138	CPBbd	Starting post-processing of session recording pam02-0000000114-1534792258372_VNC
20181010183505	2138	CPBbd	Starting post-processing of session recording pam02-0000000110-1534792068876_VNC
20181010183507	2092	Domain Controler	Possibly the remote server is powered off or security settings are too high. Deleting the file: pam02-0000000108-1534517117324_VNC
20181010183508	2092	Domain Controler	Starting post-processing of session recording pam02-0000000096-1534517025792_VNC
20181010183510	2092	--	Log records viewed
20181010183516	2341	SSLVPN	Possibly the remote server is powered off or security settings are too high. Deleting the file: pam02-0000000091-1533671292329.txt
20181010183517	2341	SSLVPN	Starting post-processing of session recording pam02-0000000091-1533671292329.txt
20181010183525	2092	SSLVPN	Log records viewed
20181010183526	2138	SSLVPN	Completed post-processing of session recording for pam02-0000000083-1532983235829.vsr.
20181010183527	2138	CPBbd	Starting post-processing of session recording pam02-0000000083-1532983235829_VNC
20181010183553	2341	SICAP	Completed post-processing of session recording for pam02-0000000105-1532122999698.txt.
20181010183555	2341	SICAP	Starting post-processing of session recording pam02-0000000105-1532122999698.txt
20181010183656	2341	SICAP	Starting post-processing of session recording pam02-0000000103-1532122863041.txt
20181010183535	2433	Domain Controler	Log records viewed
20181010183603	736	Email Security (Antispam)	Completed post-processing of session recording for pam02-0000000095-1532024624932.txt.
20181010183617	736	Email Security (Antispam)	Starting post-processing of session recording pam02-0000000095-1532024624932.txt
20181010183912	736	Domain Controler	Completed post-processing of session recording for pam02-0000000091-1532024499111.vsr.
20181010183949	736	CPBbd	Starting post-processing of session recording pam02-0000000091-1532024499111_VNC
20181010184320	736	Email Security (Antispam)	Completed post-processing of session recording for pam02-0000000088-1532024457928.vsr.
20181010184632	736	Email Security (Antispam)	Starting post-processing of session recording pam02-0000000088-1532024457928_VNC
20181010184723	super	Email Security (Antispam)	Completed post-processing of session recording for pam02-0000000077-1532019768415.vsr.
20181010184754	2433	Email Security (Antispam)	Starting post-processing of session recording pam02-0000000077-1532019768415_VNC
20181010184905	1401	CPBbd	Completed post-processing of session recording for pam02-0000000073-1532019736131.vsr.

Fuente: Elaboración de autores

A continuación, se presenta de forma gráfica los valores de los aplicativos que tuvieron mayor concurrencia de sesión (Ver Figura 53).

Figura 53: Resultado de acceso a activos TI.



Fuente: Elaboración de autores

La muestra fue recopilada del registro de acceso a los activos de TI de un total de 176 accesos, esta gráfica fue elaborada con el objetivo de determinar los aplicativos de mayor concurrencia y para determinar el motivo por el cual los usuarios acceden en exceso. Por esta razón, en caso de que se encuentre en riesgo se apliquen nuevas políticas de acceso y así se procura mayor atención en el monitoreo del activo entre otras medidas de seguridad. Asimismo, se considera siempre en salvaguardar y disminuir los riesgos de vulnerabilidad de los activos de información de la empresa de retail.

De lo expuesto en líneas anteriores, los usuarios tienen conocimiento de que todo intento de modificación, extracción o eliminación de datos en los activos de TI será registrado. Esta acción antes de la implementación de la solución no podía ser controlada.

En la siguiente tabla se realizó una comparación entre el resultado antes y después de la implementación de la solución, para mitigar el riesgo de extracción de información (Ver tabla 53).

Tabla 53: Resultado de la mitigación de extracción de información

Antes	Actual
Se desconoce la cantidad de usuarios que acceden al activo de TI.	Registra la cantidad de veces que un usuario accede a un activo de TI.
No se tiene trazabilidad de las actividades que realizan cuando ingresan al activo de TI.	Registra toda trazabilidad de las actividades que realiza el usuario cuando está dentro de CA PAM hasta que cierre sesión.
El usuario modifica las contraseñas manualmente.	El sistema tiene una política de rotación de contraseña, la rotación de la contraseña en la empresa es de cada 30 días.
La contraseña es conocida por los usuarios y administrada por los jefes de las áreas.	CA PAM administra las contraseñas de los dispositivos custodiados.
Por la vasta cantidad de credenciales que maneja, el usuario se ve en la necesidad de guardarla en algún lugar, tal como es descrito en la respuesta de la pregunta 5 de la encuesta realizada a los usuarios.	Para acceder a los activos de TI solo se requiere autenticarse en la solución CA PAM, es decir solo se necesita una credencial.
Al autenticarse a todos los activos de TI consume tiempo operacional.	Tras la configuración de single sign-on se reduce el tiempo operacional.
No existe notificación cuando un usuario está tratando de transgredir una política.	Envía notificaciones al administrador de la solución, para realizar una acción ante la transgresión de una política, como bloquear cuenta, solicitar re-autenticación o cerrar sesión.

Fuente: Elaboración de autores

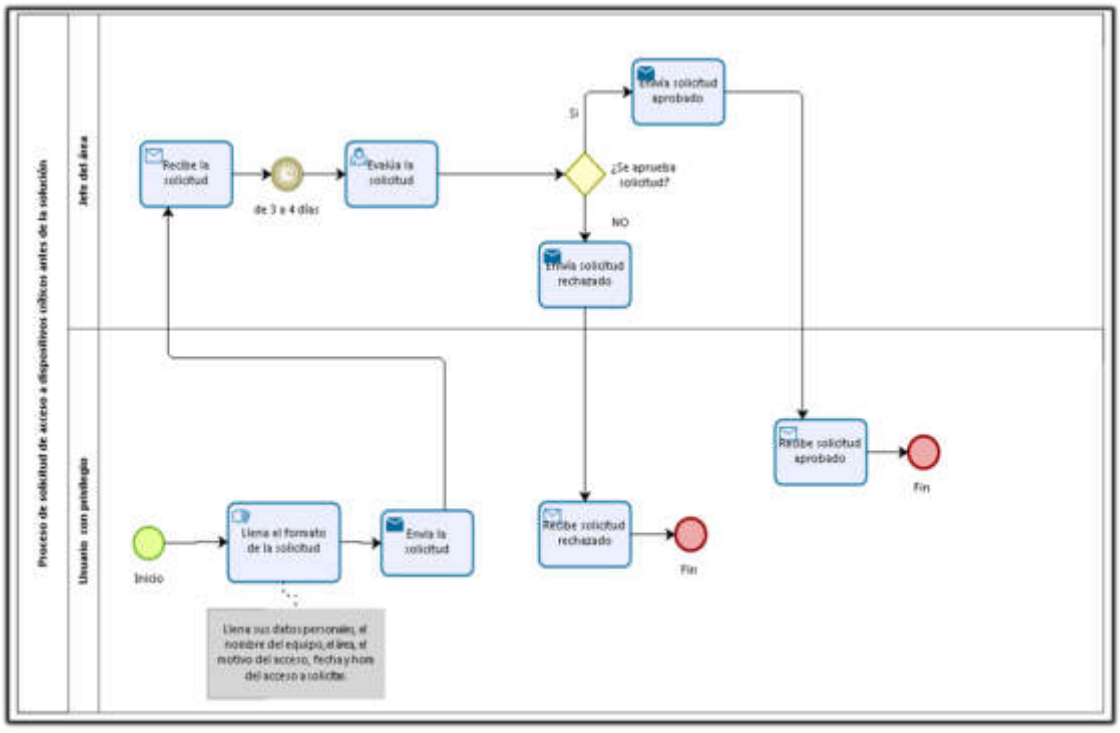
- **Objetivo Específico 3: Reducir el tiempo del proceso de aprobación de acceso a dispositivos críticos en producción de la empresa.**

Se muestra el resultado de la comparación entre el proceso de solicitud de acceso a dispositivos críticos antes y después de la implementación de la solución realizada en el registro de las actividades de los usuarios cuando se encuentran dentro del activo de TI.

c. Proceso de solicitud de acceso a dispositivos críticos antes de implementar la solución

La siguiente gráfica representa el proceso de solicitud de acceso a dispositivos críticos antes de la implementación de la solución. El proceso no estaba estructurado, debido a que el jefe para revisar la solicitud se tardaba en promedio entre 3 a 4 días, debido a que esta era proclive a perderse con la llegada de otras. Para realizar esta solicitud el usuario tenía que llenar sus datos y luego explicar el motivo de la solicitud para después ser enviada al jefe de área, luego él evaluaba y determinaba si aceptaba o no la solicitud. Sin embargo, a veces la respuesta del jefe no era respetada, ya que el usuario al tener las credenciales realizaba las modificaciones. Por otro lado, en caso de que esto generase un error no se sabía quién había sido y cuál fue la modificación realizada porque no se tenía registrado el cambio efectuado (Ver Figura 54).

Figura 54: Proceso de solicitud de acceso a dispositivos críticos antes de la solución



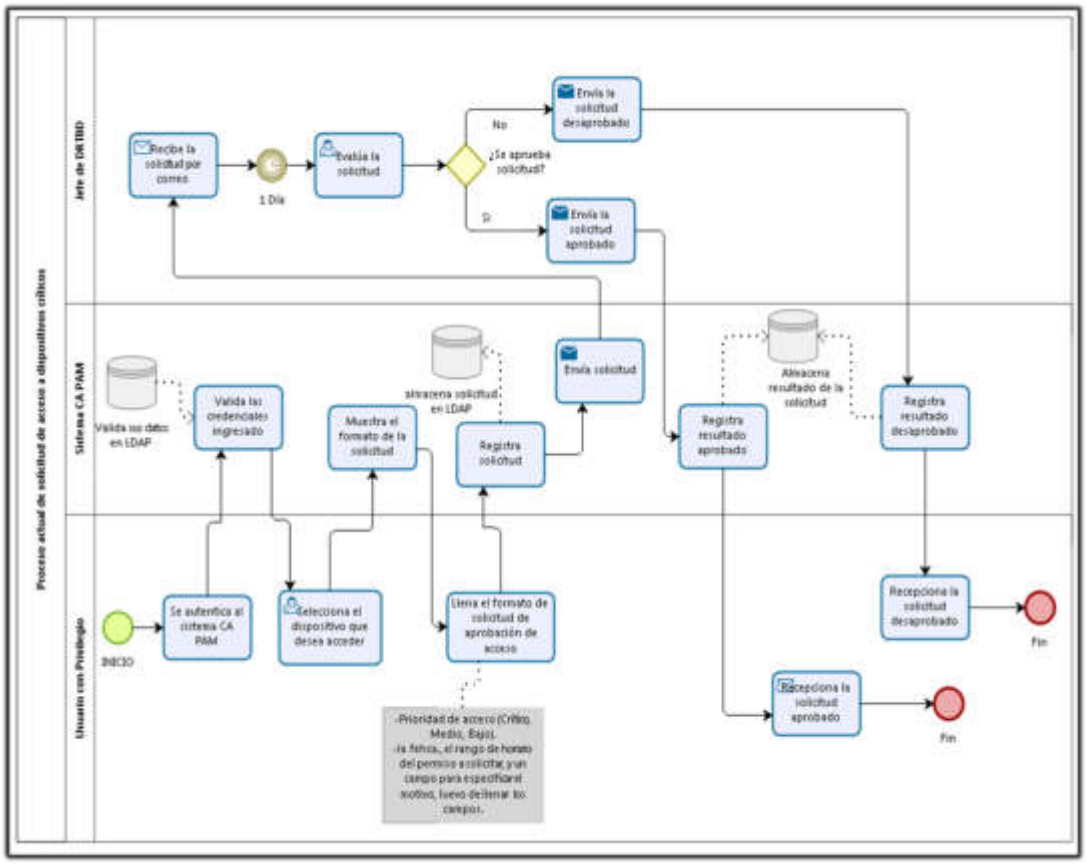
Fuente: Elaboración de autores

d. Proceso de solicitud de acceso a dispositivos críticos después de implementar la solución

Con la implementación de la solución, se resuelve el problema descrito en el proceso anterior. Dado que cuando el cliente desee acceder a un activo de TI crítico y al no contar con las credenciales, debe enviar una solicitud de acceso al jefe del DRTBD. No obstante, esto se realiza directamente en la solución CA PAM llenando los datos del formato mencionado, en el proceso solicitud de aprobación a dispositivos críticos (Ver Figura 55). Luego esta solicitud es registrada en la base de datos que tiene integrada la solución, posteriormente el jefe evalúa la solicitud de acceso y registra la respuesta ante la solicitud. De esta manera se tiene un proceso estructurado en la solicitud de acceso, además se tiene un registro de todas las modificaciones que realizan los usuarios. Es preciso señalar que, en caso crítico, se presente un problema luego de la configuración en el dispositivo, se conoce el nombre del usuario y actividades realizadas. Con esta información se trabajará más rápido para revertir el problema presentado.

En la siguiente figura se muestra un proceso de solicitud de aprobación de acceso a dispositivos críticos más estructurado a comparación del que tenían antes de la implementación de la solución. con esta integración el tiempo de aprobación o desaprobación de solicitud de acceso a dispositivos críticos se redujo a un día lo que normalmente se demoraba un tiempo promedio de 3 a 4 días. Además, con esta solución se tiene un registro del control de cambio (Ver Figura 55).

Figura 55: Proceso actual de solicitud de acceso a dispositivos críticos



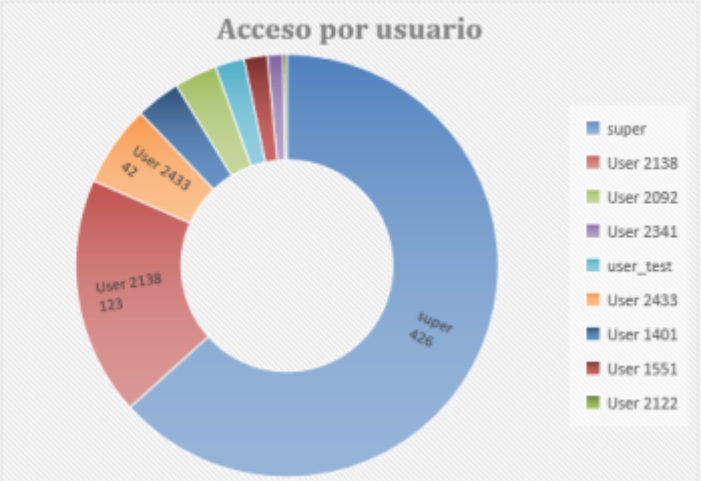
Fuente: Elaboración de autores

- **Mejorar la gestión de identidades privilegiadas de los administradores de las plataformas de TI en la empresa de retail.**

En la siguiente figura se muestra la lista de interacción de los usuarios con la solución de CA PAM. El usuario súper (administrador de PAM), 2138 y 2433 del LDAP del dominio CPB son los que mayor interacción tuvieron ya que accedieron a la solución y dispositivos agregados a este (Ver Figura 56).

Esta gráfica y las que se muestran en el capítulo 5.2 (Ver Figura 52 y 53) son los resultados que evidencian la mejora en la administración de los accesos privilegiados, porque se tiene una trazabilidad de las actividades de los usuarios desde el momento de iniciar sesión hasta que este finalice cerrando la sesión.

Figura 56: Administración de acceso por usuario a los dispositivos.



Fuente: Elaboración de autores

CAPÍTULO VI
DISCUSIÓN Y APLICACIONES

En este capítulo se realizó la discusión del resultado obtenido luego de la implementación de la solución en base al método PDCA. Además, se realiza una descripción breve de las funciones que cumple el aplicativo que usamos para el cumplimiento de nuestros objetivos.

6.1 Discusión de objetivos y resultados

En la siguiente tabla se realizó la comparación entre el estado inicial y el resultado esperado luego de la implementación de la solución en cuanto al cumplimiento de los objetivos tanto general como específico establecidos en este proyecto (Ver Tabla 54).

Tabla 54: Discusión de objetivos y resultados

Objetivo	Antes	Resultado esperado
Objetivo General: Mejorar la gestión de identidades privilegiadas de los administradores de las plataformas de TI en la empresa de retail.	Los usuarios utilizaban cuentas privilegiadas compartidas, cuando realizaban modificaciones y si algo salía mal no se sabía quién era esa persona, no se tenía un control de cambio, no se sabía quiénes ingresaban al dispositivo, con qué fin lo hacían, y tampoco se	Con la solución implementada se mejoró la gestión de identidades privilegiadas, poniendo fin el uso de cuentas compartidas, desde entonces el único encargado de administrar las credenciales es la solución CA PAM. Es así, que el acceso a las cuentas privilegiadas se fue asignando de acuerdo a la

Objetivo	Antes	Resultado esperado
	tenía un control de las informaciones que salían de los activos críticos.	función del usuario y del cual se tiene un registro de todo el accionar del usuario al que se le fue conferido el permiso.
Objetivo Específico 1: Reducir el tiempo del proceso de autenticación en los activos de TI, mejorando la eficiencia operacional.	Los usuarios para autenticarse a todos sus activos de TI necesitaban tener entre 10 credenciales distintas y es por ello que estaban obligados a registrarlos en cualquier lugar, esto generaba que ellos al momento de autenticarse tarden en promedio 1 a 2 minutos, y al día era más de 20 minutos, esto causaba una sobre carga operacional.	El tiempo de autenticación de un usuario a todos los activos de TI en un día, lo que antes le tomaba 20 minutos ahora con la solución implementada solo tarda un minuto como máximo, de esta manera se evidencia la reducción importante en el tiempo de acceso, además reduce el trabajo operacional del usuario
Objetivo Específico 2: Mitigar el riesgo de extracción de información de los activos de TI por usuarios no autorizados.	Con el anterior servicio no se sabía que usuario accedía al activo de TI, las actividades que realizaba estando dentro, el usuario tenía un registro de sus contraseñas, el sistema no informaba de los intentos de vulnerar las políticas de acceso.	Con la solución implementado se logra registrar todas las actividades de los usuarios desde el momento de inicio de sesión hasta el cierre, las credenciales de los activos solo son conocido por el sistema y es cambiado automáticamente cada 30 días.
Objetivo Específico 3: Reducir el tiempo del proceso de aprobación de acceso a dispositivos críticos en producción de la empresa.	El proceso que existía no estaba bien estructurado, cuando el usuario enviaba su solicitud de acceso, esto tardaba entre 3 a 4 días debido a que la solicitud se juntaba con otros correos, además había el problema de que cuando la solicitud era rechazada, el solicitante no aceptaba la decisión y al tener las credenciales solo accedía y realizaba las modificaciones sin tener un documento que registre el cambio efectuado.	Con la solución implementada se reduce el tiempo de aprobación a las solicitudes de acceso a 1 día como máximo, debido a que el proceso es más estructurado, además se terminó el problema del control de acceso, las solicitudes de acceso a activos críticos ahora son solicitados a través del sistema implementado, en caso de la solicitud no sea aceptada, el usuario no tiene forma alguna de cómo acceder al activo, pero si la solicitud es aprobada, la solución registra la solicitud de cambio.

Fuente: Elaboración de autores

6.2 Aplicaciones

La solución *CA Privilleged Access Manager* puede aplicarse en cualquier empresa que tenga una infraestructura definida de TI y maneje información de importancia crítica. Principalmente está realizada para empresas medianas y grandes debido al costo de licenciamiento e implementación. Esta solución sirve de apoyo para conseguir la certificación ISO 27001, ya que ayuda a tener control de los accesos de la empresa. Por otro lado, esta solución es solo destinada para integrarla con dispositivos del área de infraestructura de TI que tengan dispositivos de redes, base de datos, plataformas virtuales, sistemas operativos o aplicaciones cliente/servidor (C/S).

CONCLUSIONES

1. Reducción del tiempo del proceso de autenticación en los activos de TI: antes tardaba un promedio de 20 minutos en acceder a 10 dispositivos, ahora es un minuto como máximo con la función de *single sign-on*. De este modo, con el tiempo ganado se incrementó la eficiencia operacional.

2. Mitigación del riesgo de extracción de información de los activos de TI por usuarios no autorizados, teniendo una administración de accesos basado en roles.

3. Reducción del tiempo de aprobación de acceso a los activos críticos de TI: antes tardaba un tiempo promedio de 3 a 4 días, ahora es un máximo de 1 día, al integrar a los involucrados del proceso en una misma plataforma.

4. Mejora de la gestión de identidades privilegiadas de los administradores de las plataformas de TI en la empresa de Retail al tener la trazabilidad de las actividades realizadas en cada uno de los dispositivos.

RECOMENDACIONES

1. Contratar un proveedor externo que brinde servicios de análisis de vulnerabilidades, para detectar las brechas de inseguridad y efectuar las acciones correctivas.

2. Cambiar las contraseñas periódicamente de los dispositivos custodiados que no son administrados por CLI y actualizarlo en la solución CA PAM, con el fin de evitar inconvenientes con la función *single sign-on*.

3. Asignar un responsable a cargo del monitoreo de las actividades de los administradores de TI, para así poder identificar intentos de transgresión de las políticas establecidas.

4. Establecer políticas y directivas de seguridad para realizar periódicamente auditorías a las actividades efectuadas por los usuarios dentro de CA PAM.

5. Verificar periódicamente la capacidad disponible de almacenamiento del repositorio de grabación de sesión, para mantener disponible la función de grabación de sesión y evitar la pérdida de la trazabilidad de las actividades de los usuarios administradores de TI.

6. Adquirir licencia CA PAM con modalidad de usuarios ilimitados, para

que permita registrar a más usuarios y lograr integrar otras áreas de TI de la empresa de retail.

7. Adquirir una bóveda física que permita guardar las credenciales en sobres físicos, para tener la opción de recuperar las credenciales ante un desastre crítico, como es la caída del servicio de ambos nodos de *CA Privileged Access Manager* (PAM).

8. Complementar la solución de CA PAM con la solución de doble factor de autenticación *CA Strong Authentication* (OTP móvil), para fortalecer la seguridad de acceso a la solución CA PAM.

9. Mantener actualizada la solución CA PAM para el aprovechamiento de correcciones y posiblemente nuevas funcionalidades.

10. Integrar los registros del CA PAM con una base de datos externa para generar reportes más personalizados con gráficas.

FUENTES DE INFORMACIÓN

Bibliográficas:

Hibbert, B. & Haber, M. (2018) *Privileged Attack Vectors: Building Effective Cyber-Defense Strategies to Protect Organizations*. Florida: Editorial

Cruz, M & Fukusaki, L. (2017) *Diseño e implementación de un sistema de gestión de seguridad de la información para proteger los activos de información de la clínica Medcam Perú S.A.C.* (Tesis de pregrado, Universidad San Martín de Porres. Lima, Perú)

Giraldo, L. (2016) *Análisis para la Implementación de un Sistema de Gestión de la Seguridad de la Información según la Norma ISO 27001 en la empresa SERVIDOC S.A.* (Tesis de pregrado, Universidad Nacional Abierta y a Distancia Colombia. Cali, Colombia)

Talavera, V. (2015) *Diseño de un Sistema de Gestión de Seguridad de la Información para una entidad estatal de Salud de acuerdo a la ISO/IEC 27001:2013.* (Tesis de pregrado, Pontificia Universidad Católica del Perú. Lima, Perú)

ISO/IEC 27000 (2014) *ISO/IEC 27000:2014 Tecnología de la Información, Técnicas de seguridad, Sistemas de gestión de seguridad de la información visión de conjunto y vocabulario*. 3ª ed. Madrid: Aenor.

Sohner, M. (2014) *Gestión de usuarios privilegiados en contraseñas entornos compartidos.* (Tesis de maestría, Universidad Técnica de Múnich. Múnich, Alemania)

Guarnizo, J, & Prieto, E. (2014) *Diseño de un sistema de gestión de seguridad de la información (SGSI) para la empresa Agility S.A*. (Tesis de pregrado, Universidad Distrital Francisco José de Caldas. Bogotá, Colombia)

Villena, M. (2014) *Diseño de un sistema de gestión de seguridad de información para servicios postales del Perú S.A.* (Tesis de pregrado, Pontificia Universidad Católica Del Perú. Lima, Perú)

ISO/IEC 27002 (2013) *ISO/IEC 27002:2013 Tecnología de la Información, Técnicas de seguridad, Código de prácticas para los controles de seguridad de la información*. 3ª ed. Madrid: Aenor

ISO/IEC 27001 (2013) *ISO/IEC 27001:2013 Tecnología de la Información, Técnicas de seguridad, Sistemas de gestión de seguridad de la información, Requisitos.* 3ª ed. Madrid: Aenor.

Apress.Telefónica, T. (2009) *Las TIC en la justicia del futuro*. Madrid: Editorial Ariel

Hemerográficas:

Caro, J. (2013) Más sobre la amenaza cibernética. *Artículos ESUP*, (6) 3-6

Manjusha, R. & Ramachandran, R. (2015) Secure Authentication and Access System for Cloud Computing Auditing Services Using Associated Digital Certificate. DOI: 10.17485/ijst/2015/v8iS7/65321

Suntana, K., Martini, B.,Hunt, R. & Raymond, K. (2015) A Taxonomy of Cloud Attack Consequences and Mitigation Strategies The Role of Access Control and Privileged Access Management. *Revista Institute of Electrical and Electronics Engineers*, (1) 1073-1080. DOI:

10.1109/Trustcom.2015.485.

Shackleford, D. (2015) Combatting Cyber Risks in the Supply Chain. *Revista Institute SANS,* (1) 3-15.

Fadida, I., Balzam, G., Jerbi, A. & Barak, N. (2014*) CA Technologies Inc: Privileged shared account password sanitation*. DOI: 2016-06-30US20160191495A1

Centro Integral de Educación Continua (2009) Enfoques del control interno. Universidad de Lima. Lima, Perú.

Electrónicas:

CA Technologies. (2018) *CA Privileged Access Manager - 3.2*. Recuperado de https://docops.ca.com/ca-privileged-access-manager/3-2/EN (Consulta: 27 de agosto del 2018)

Gemalto NV. (2018) *Data Breach Statistics*. Recuperado de https://breachlevelindex.com/#sthash.RZhGQkVZ.dpbs (Consulta: 15 de septiembre del 2018)

Identity Force. (2018) *2018 Data Breaches - The worst so far*. Recuperado de https://www.identityforce.com/blog/2018-data-breaches (Consulta: 21 de septiembre del 2018)

Kaspersky Lab. (2016) *Chasing Lazarus: A hunt for the infamous hackers to prevent large bank robbeeries*. Recuperado de https://www.kaspersky.com/about/press-releases/2017_chasing-lazarus-a-hunt-for-the-infamous-hackers-to-prevent-large-bank-robberies (Consulta: 20 de octubre del 2018)

Gilart, I. (2016) *Buenas prácticas para la gestión de cuentas privilegiadas*

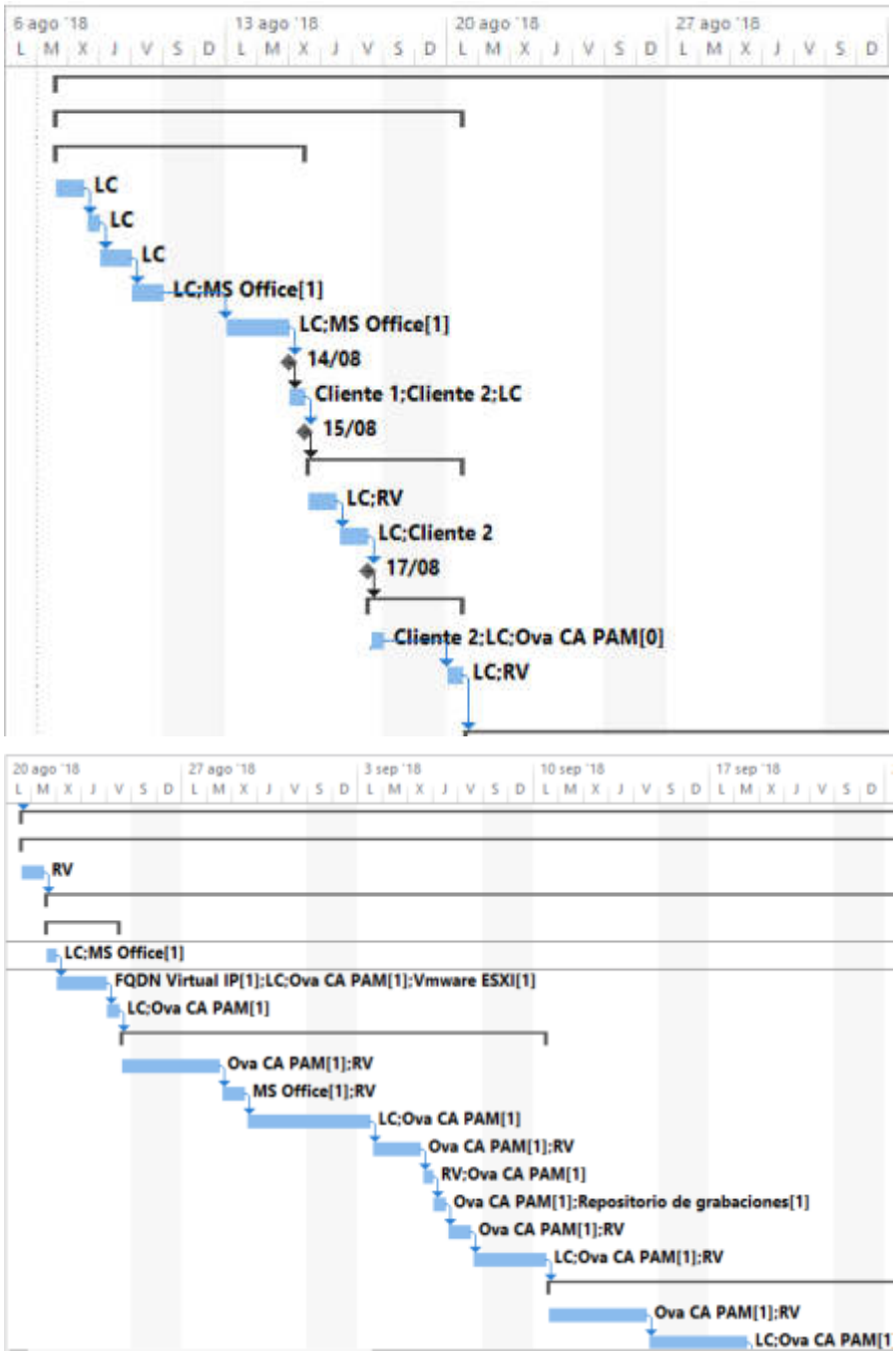
consolidación de identidades. Recuperado de https:// https://www.whitebearsolutions.com/buenas-practicas-para-la-gestion-de-cuentas-privilegiadas-consolidacion-de-identidades/
(Consulta: 18 de septiembre del 2018)

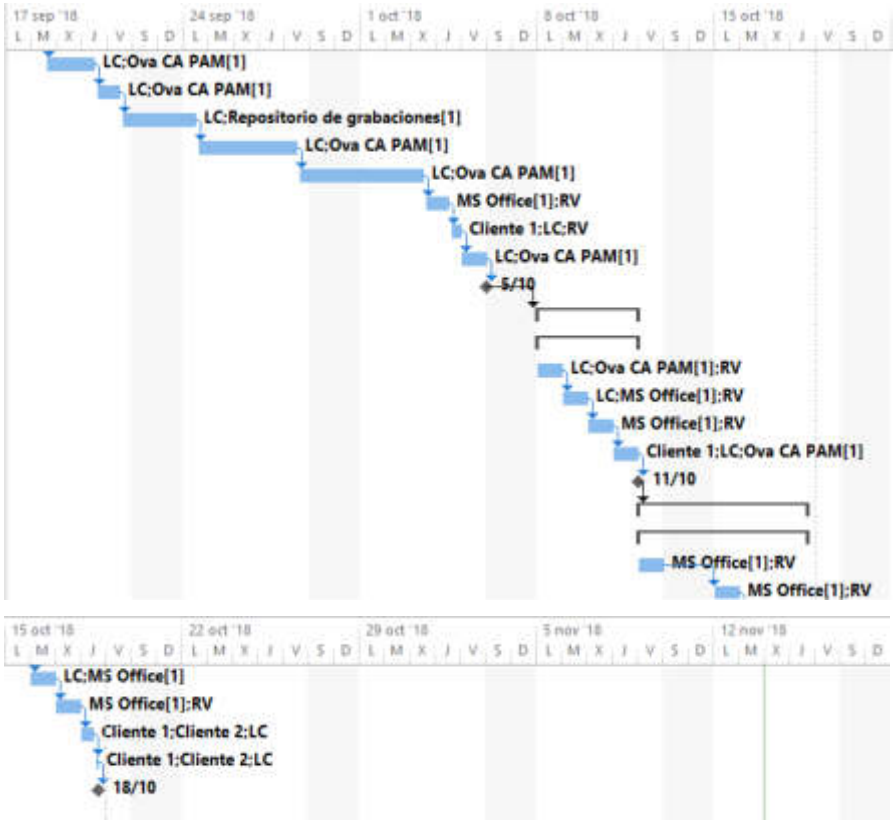
Rouse, M. (2016) *IAM o Sistema de gestión de accesos e identidades*. Recuperado de https://searchdatacenter.techtarget.com/es/definicion/IAM-o-Sistema-de-gestion-de-accesos-e-identidades
(Consulta: 21 de septiembre del 2018)

González, I & Padrón, M. (2014) *Módulos de autenticación conectables, versión 1.0*. Recuperado de http://sopa.dis.ulpgc.es/ii-aso/portal_aso/leclinux/seguridad/pam
(Consulta: 18 de septiembre del 2018)

ÍNDICE DE ANEXOS

Anexo 1: Diagrama de Gantt



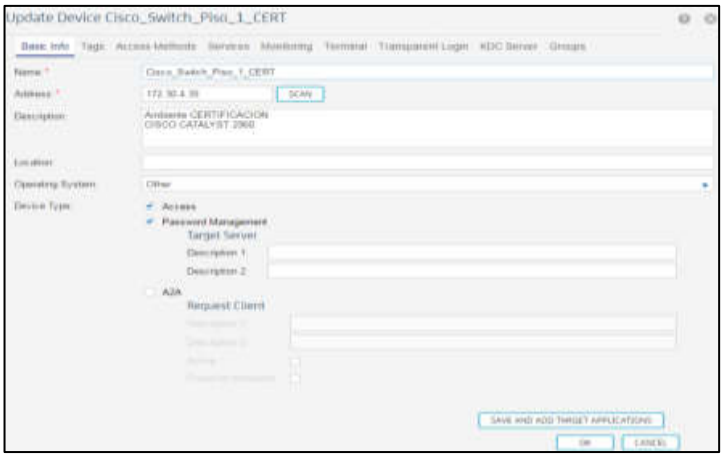

17 sep '18
24 sep '18
1 oct '18
8 oct '18
15 oct '18
L M X J V S D
LC:Ova CA PAM[1]
LC:Ova CA PAM[1]
LC:Repositorio de grabaciones[1]
LC:Ova CA PAM[1]
LC:Ova CA PAM[1]
MS Office[1]:RV
Cliente 1:LC:RV
LC:Ova CA PAM[1]
5/10
LC:Ova CA PAM[1]:RV
LC:MS Office[1]:RV
MS Office[1]:RV
Cliente 1:LC:Ova CA PAM[1]
11/10
MS Office[1]:RV
MS Office[1]:RV
15 oct '18
22 oct '18
29 oct '18
5 nov '18
12 nov '18
L M X J V S D
LC:MS Office[1]
MS Office[1]:RV
Cliente 1;Cliente 2:LC
Cliente 1;Cliente 2:LC
18/10

Anexo 2: Resumen de Configuración CA PAM

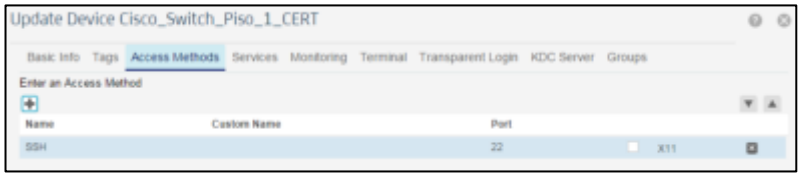
a. Ambiente de Certificación

- **Dispositivos Tipo SSH**
  - **Creación de Dispositivo Aplicativo Cisco Switch 1**

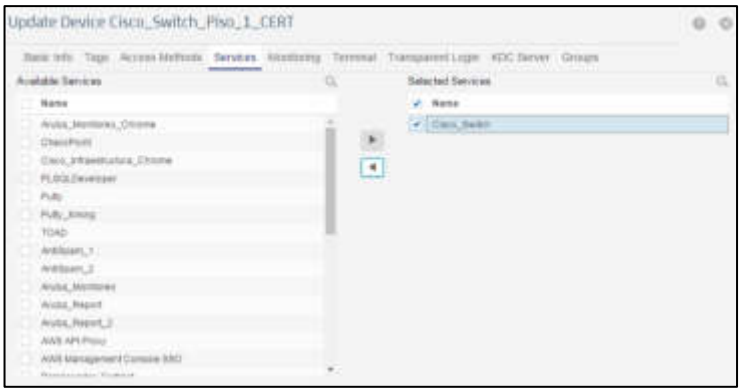
La siguiente imagen representa la creación del equipo de tipo SSH, equipos de conexión de red (Router, Switch, AP), para ello se debe completar el nombre que tendrá el equipo web, la IP, el sistema operativo, el tipo de acceso, y el pasword Management para que CA PAM rote la contraseña en cada cierto tiempo.



En esta imagen representa la configuración del modo de acceso al dispositivo, para este dispositivo se activó el puerto 22.

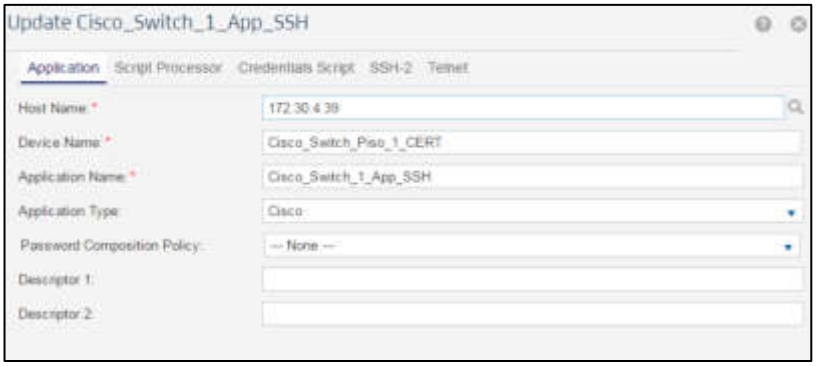


La imagen siguiente representa la selección del tipo de servicio que será configurado. Previo a ello se debió de haber creado.



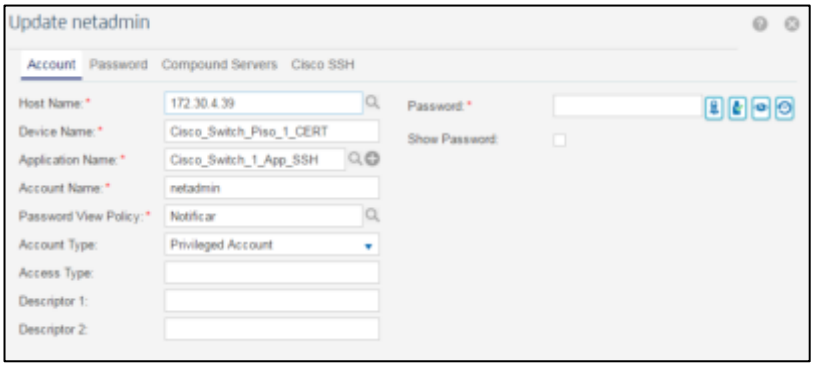
- **Creación de Aplicación SSH**

Se registra la aplicación que será implementado en el servicio creado, para ello se necesita ingresar el nombre de la máquina, del servicio, de la aplicación y el tipo de aplicación.



- **Creación de Cuenta**

Se crea la cuenta que va a administrar el aplicativo, para ello se debe ingresar el nombre de la máquina, del servicio, de la aplicación, de la cuenta que va a administrar, además del tipo de cuenta



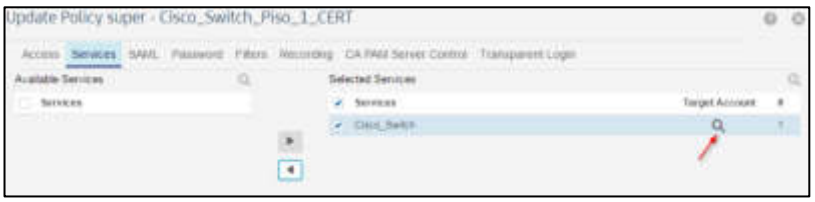
En la siguiente imagen se procede a configurar la contraseña que será utilizado del sistema CA PAM.

- **Creación de la Política de Acceso**

En la siguiente imagen se procede a configurar el tipo de acceso que tendrá este dispositivo, en el caso de la imagen es de tipo SSH.

En la siguiente imagen se agrega el nombre del administrador.

En la siguiente imagen se integra el servicio, que viene a ser el de SSH.



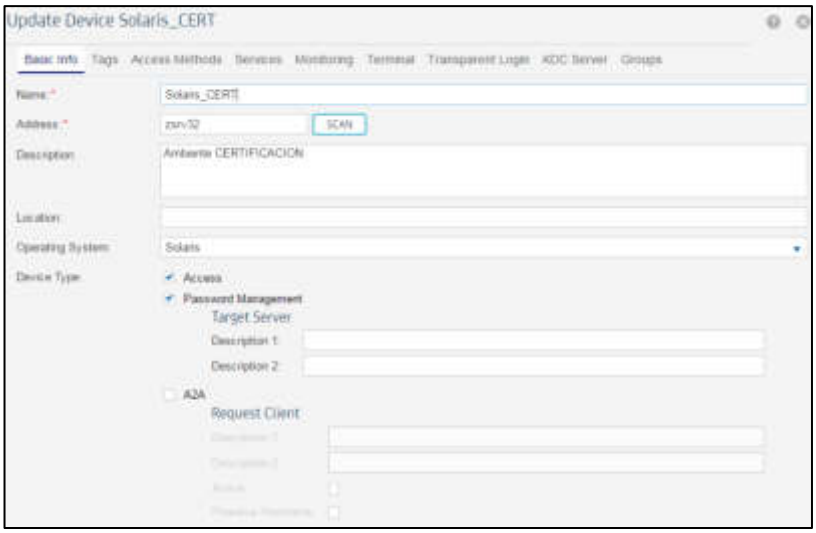
En la siguiente imagen se procede a crear restricciones para que no se utilice la combinación de teclados

En la siguiente imagen se procede a configurar el tipo de registro, para este servicio se habilita el grabado de comandos, las teclas bidireccionales.

En la siguiente imagen se activa la transparencia de acceso, para que sea restringido ciertas teclas y el clic derecho del mouse.

- **Equipo tipo SSH Solaris**
  - **Creación de Dispositivo Solaris**

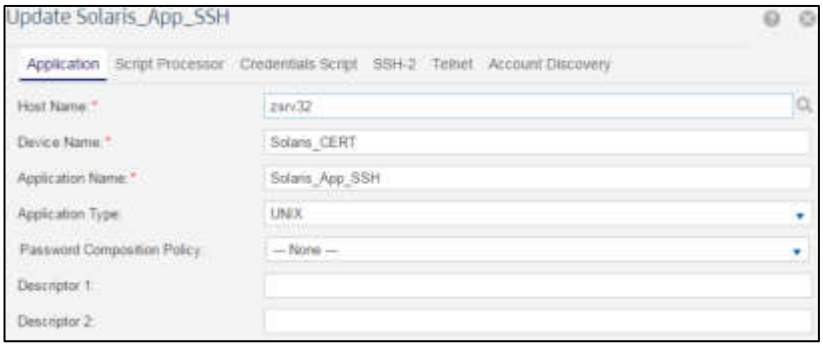
    La siguiente imagen representa la creación del equipo de sistema Solaris, para ello se debe completar el nombre que tendrá el equipo web, la IP, el sistema operativo, el tipo de acceso, y el pasword Management para que CA PAM rote la contraseña en cada cierto tiempo.



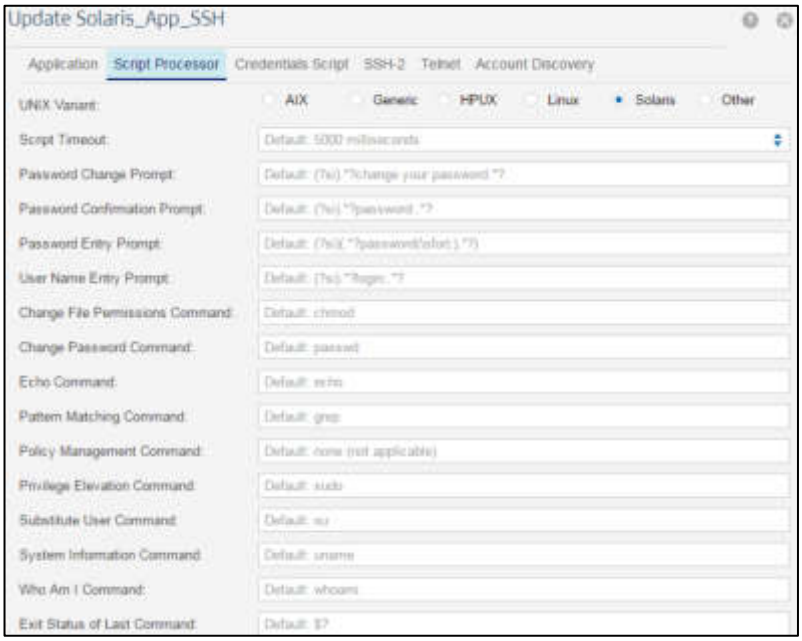
En esta imagen representa la configuración del modo de acceso al dispositivo, para este dispositivo se activó el puerto 22.

- **Creación del Conector de la Aplicación**

En la siguiente imagen se procede a crear el tipo de aplicativo que será integrado al servicio y posterior a ello al equipo, para ello se debe registra el nombre del host, nombre del dispositivo, nombre de la aplicación y el tipo de aplicación.

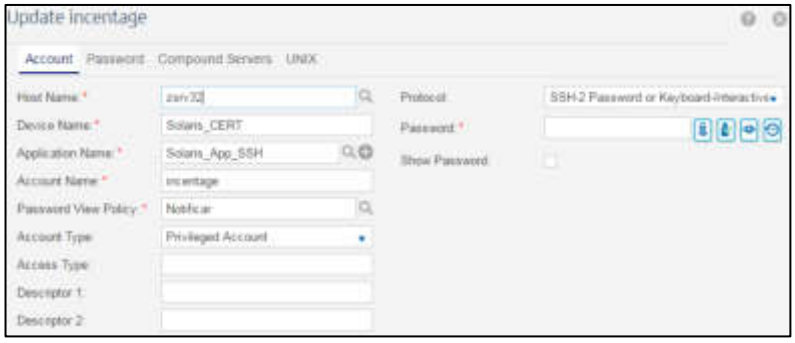


En la siguiente imagen se configura el tipo sistema operativo con lo que va a trabajar el servicio creado.

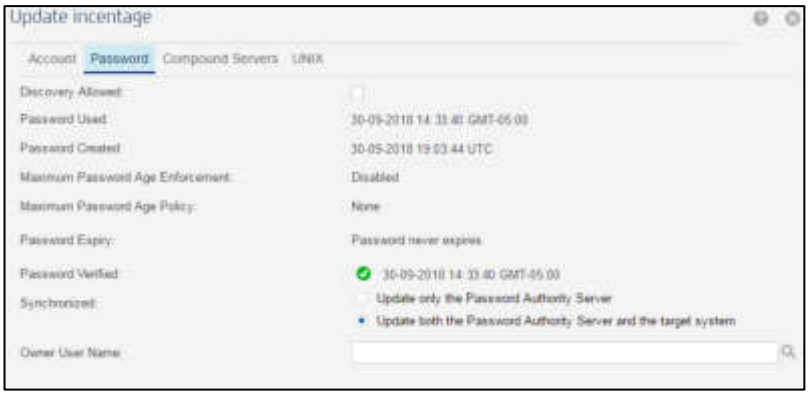


- **Creación de Cuenta**

En la siguiente imagen se procede a crear el nombre de la cuenta que administrará el servicio.

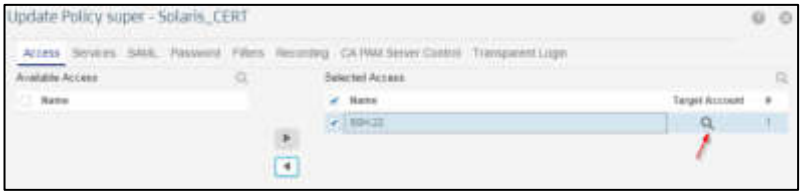


En la siguiente imagen se habilita la sincronización de las contraseñas, para que sea utilizado el que está encriptada en CA PAM.



- **Creación de Política de Acceso**

En la siguiente imagen se procede aplicar las políticas de acceso, primero se elige el tipo de acceso que se requiere para tener acceso al dispositivo, para el servicio es de tipo SSH.

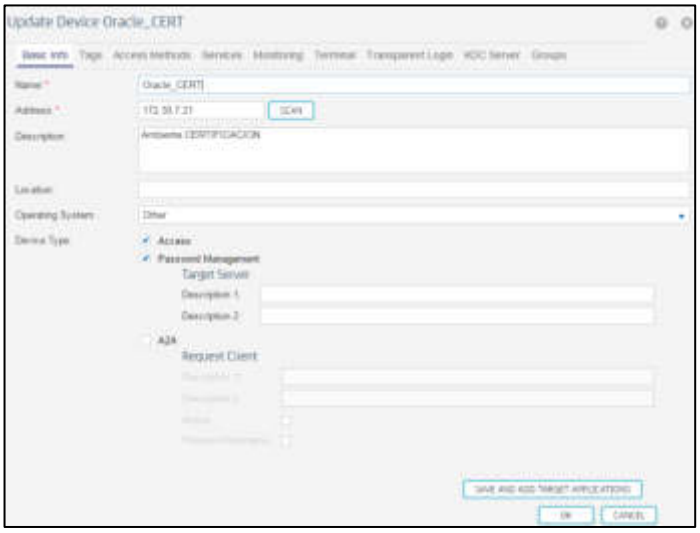


En la siguiente imagen se procede a integrar el nombre del administrador de este servicio.

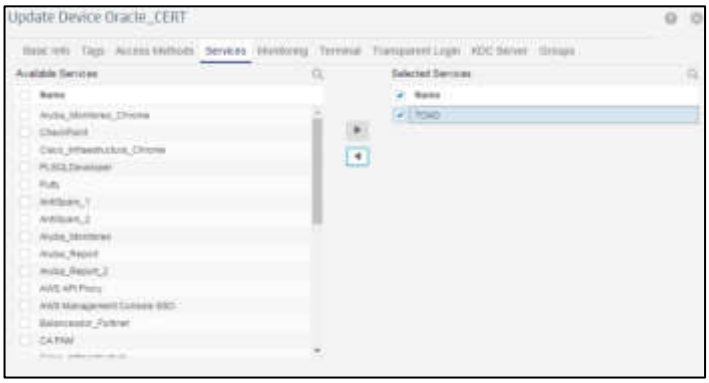
En la siguiente imagen se procede a configurar el tipo de registro, para este servicio se habilita el grabado de comandos, las teclas bidireccionales.

- **Dispositivos Tipo Cliente/Servidor**
  - **Creación de Dispositivo TOAD For Oracle**

    La siguiente imagen representa la creación del equipo oracle, para ello se debe completar el nombre que tendrá el equipo web, la IP, el sistema operativo, el tipo de acceso, y el pasword Management para que CA PAM rote la contraseña en cada cierto tiempo.

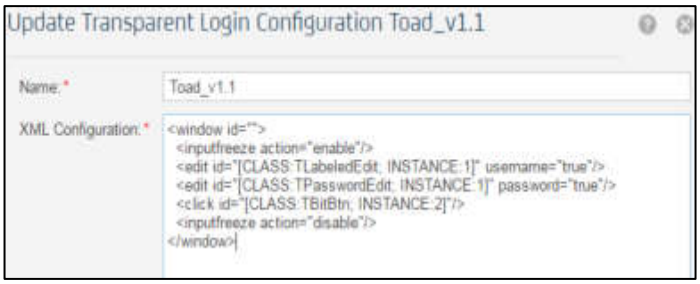


En la siguiente imagen se procede a integrar el servicio de Oracle.



  - **Creación de Transparent Login.**

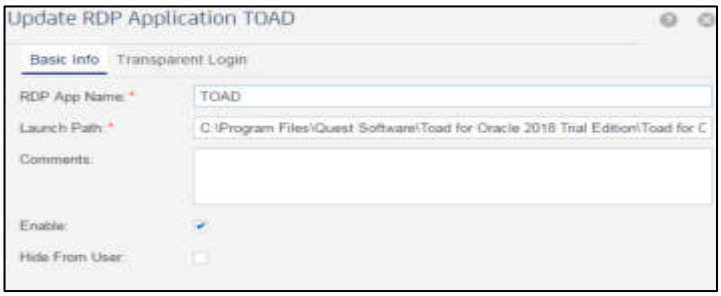
    En la siguiente imagen se procede activar el transparent login, para que cuando solicite al usuario ingresar su nombre se deshabilite el anti-clic derecho, y solo funcione las teclas y el clic izquierdo.



- **Creación de RDP Application**

Launch Path: C:\Program Files\Quest Software\Toad for Oracle 2018 Trial Edition\Toad for Oracle 13.0 Trial\Toad.exe

En la siguiente imagen se procede a configurar desde donde se ejecutará el aplicativo.



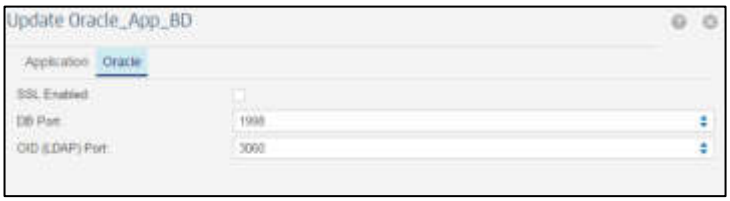
Windows Title: Toad for Oracle Database Login Version 13.0.0.80

En la siguiente imagen se activa la configuración realizado en la imagen anterior

- **Creación del Conector de la Aplicación**

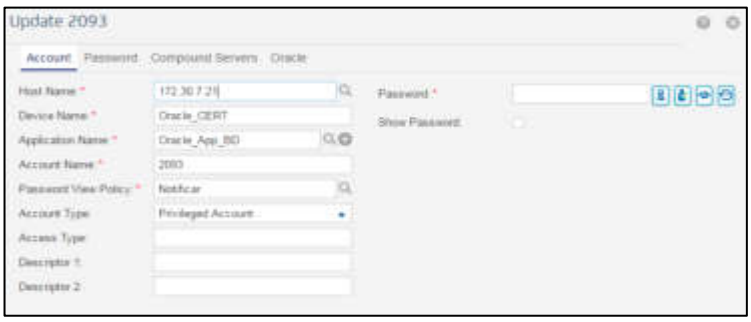
En la siguiente imagen se procede a crear el servidor que contendrá a la base de datos creado líneas anteriores.

En la siguiente imagen se procede a configurar los puertos por donde se tendrá conexión a la base de datos.

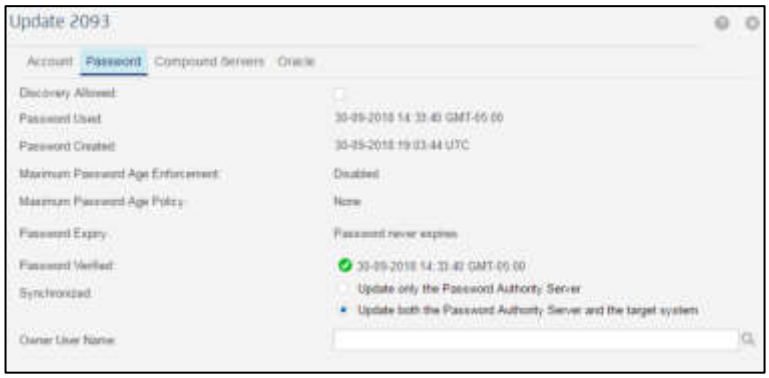


- **Creación de Cuenta**

En la siguiente imagen se procede a configurar el nombre de la cuenta del usuario que tendrá acceso a la base de datos.



En la siguiente imagen se habilita la sincronización de las contraseñas, para que sea utilizado el que está encriptada en CA PAM.



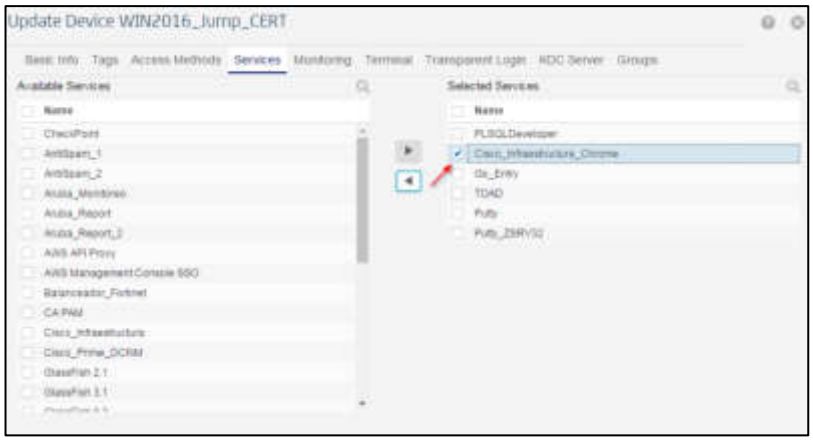
- **Creación de Política de Acceso**

  En la siguiente imagen se procede a integrar el servicio al equipo.

  En la siguiente imagen se integra el nombre del administrador del servicio.

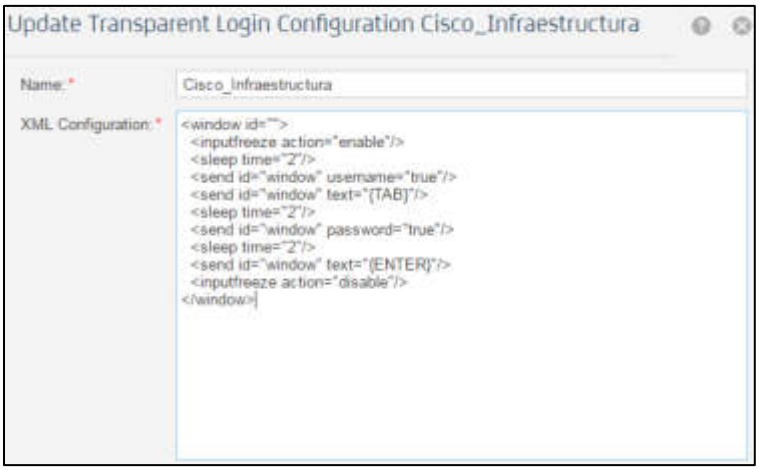
- **Aplicativo Cisco Infraestructura**
  - **Creación del Servicio.**

    En la siguiente imagen se procede a configurar el servicio.



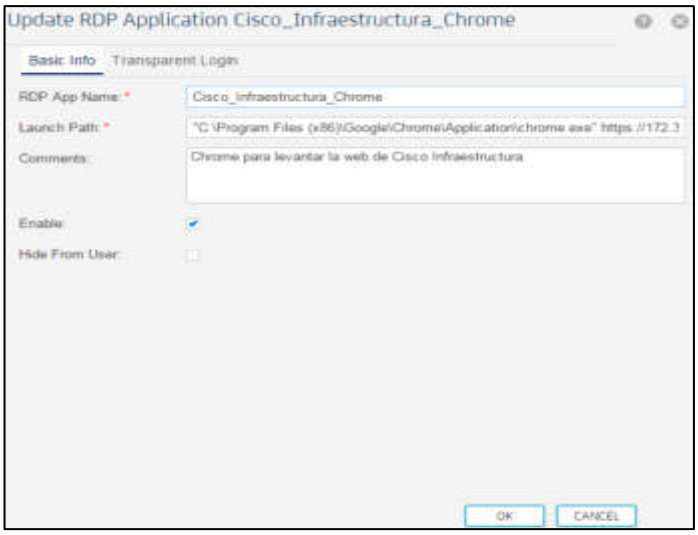
- **Creación de Configuración de Transparent Login**

  En la siguiente imagen se procede activar el transparent login, para que cuando solicite al usuario ingresar su nombre se deshabilite el anti-clic derecho, y solo funcione las teclas y el clic izquierdo.

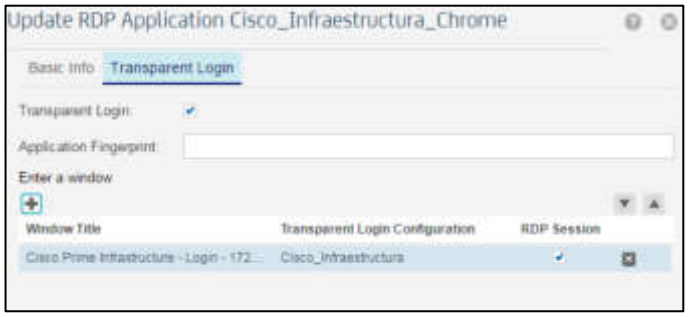


- **Creación de RDP Aplicación**

  En la siguiente imagen se procede a configurar desde donde se ejecutará el aplicativo.

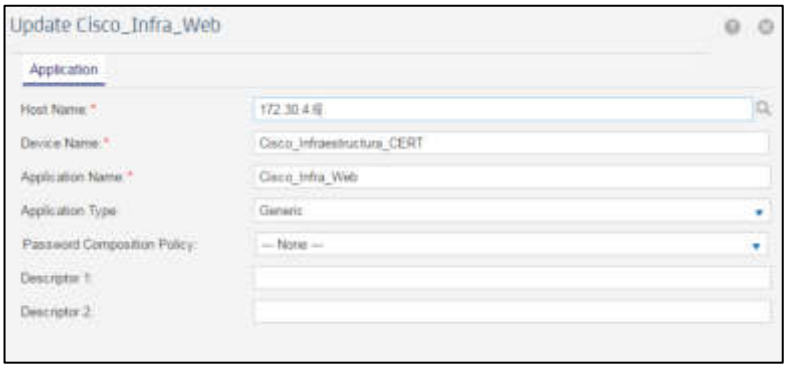


En la siguiente imagen se activa la configuración realizado en la imagen anterior



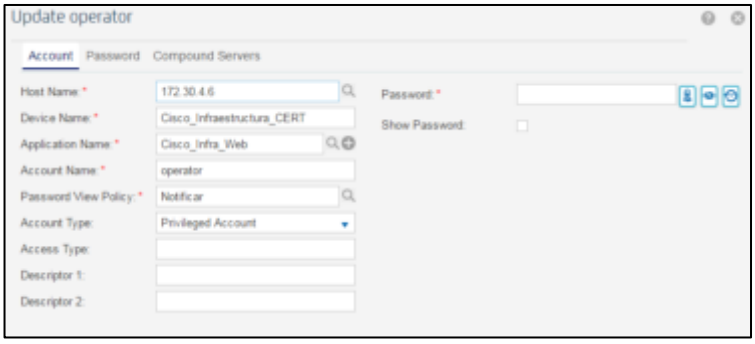
- **Creación del Conector de la Aplicación**

En la siguiente imagen se procede a crear el servidor que contendrá a la base de datos creado líneas anteriores.



- **Creación de Cuenta**

En la siguiente imagen se procede a crear la cuenta del conector.



- **Creación de Política de Acceso.**

En la siguiente imagen se procede a configurar las políticas de acceso al equipo.

En la siguiente imagen se procede a elegir la cuenta del administrador del servicio conector.

Luego de haber integrado el servicio con el equipo se procede agregar al encargado del aplicativo.

- **Aplicativos RDP**
  - **Requisitos de Windows Remote Windows 2008 – MS02**

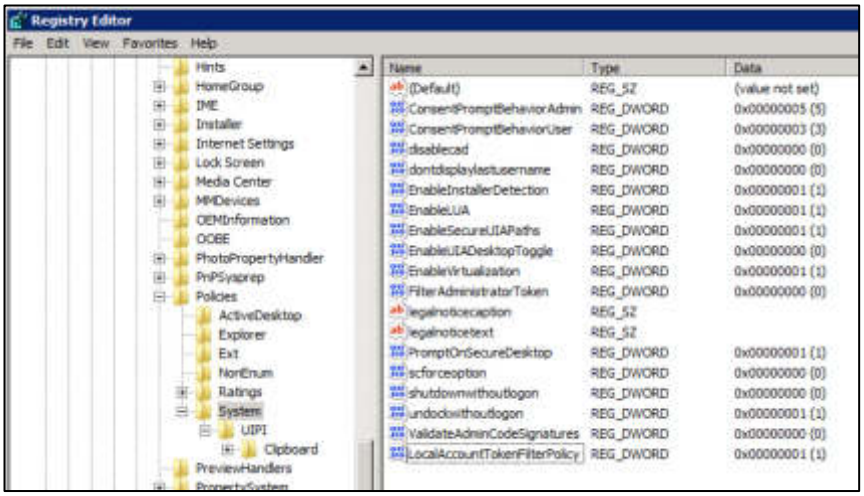
    El conector remoto de Windows requiere que los puertos 445 y 135 se habiliten en el firewall.

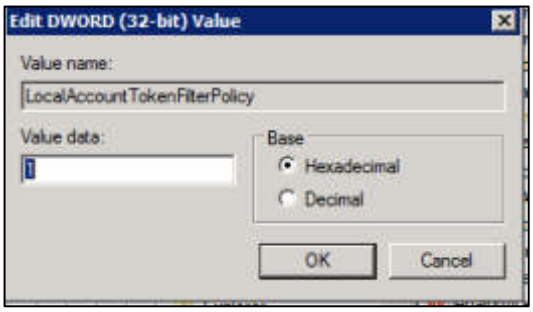
    SMB: Puerto 445

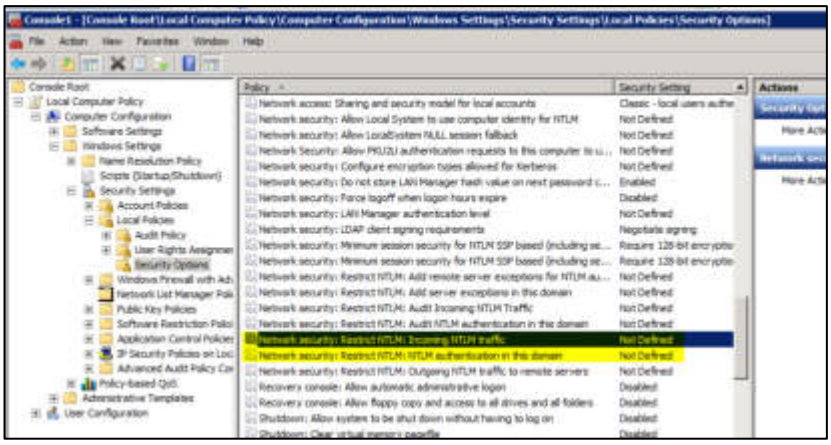
    WMI: Puerto 135

    Establecer el siguiente valor de registro para que el conector remoto de Windows tenga acceso para realizar operaciones.

    HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System\LocalAccountTokenFilterPolicy = dword:00000001

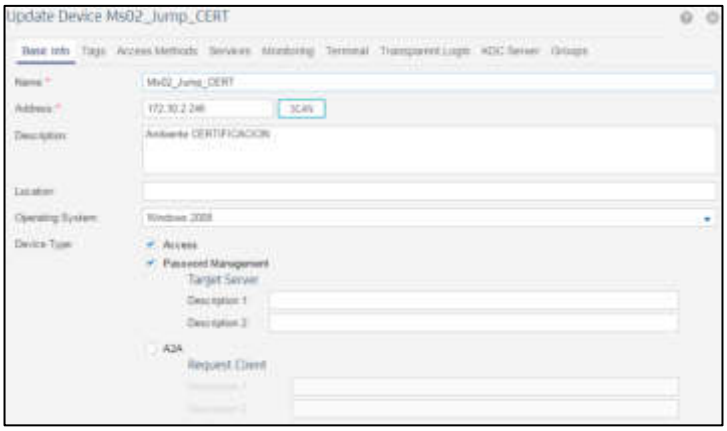






- **Creación del Dispositivo**

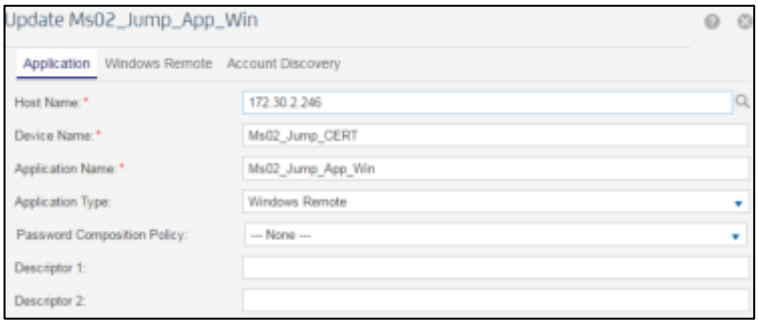
En la siguiente imagen se procede a crear el equipo que contendrá al servicio de tipo RDP, para ello se debe completar el nombre que tendrá el equipo web, la IP, el sistema operativo, el tipo de acceso, y el pasword Management para que CA PAM rote la contraseña en cada cierto tiempo.



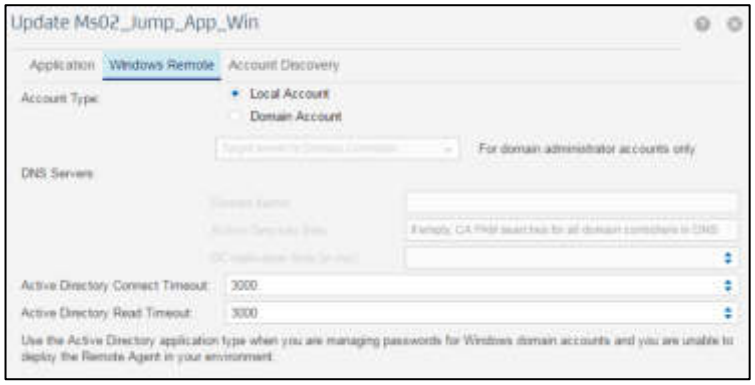
En la siguiente imagen se procede activar el puerto del protocolo de conexión remota, para ello es el 3389.

- **Creación del Conector de la Aplicación**

Se registra la aplicación que será implementado en el servicio creado, para ello se necesita ingresar el nombre de la máquina, del servicio, de la aplicación y el tipo de aplicación.

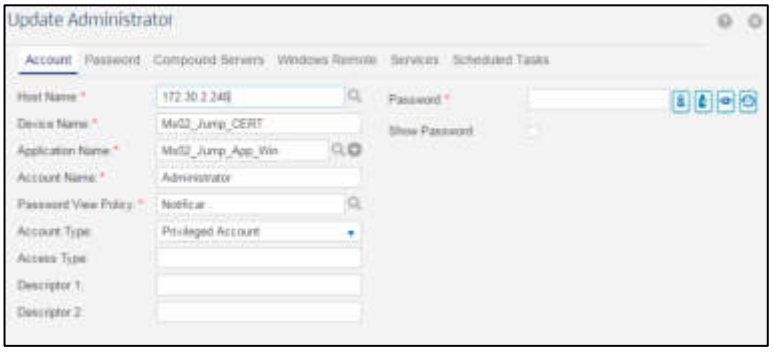


En la siguiente imagen se activa la funcionalidad de conexiones remotas solo locales.

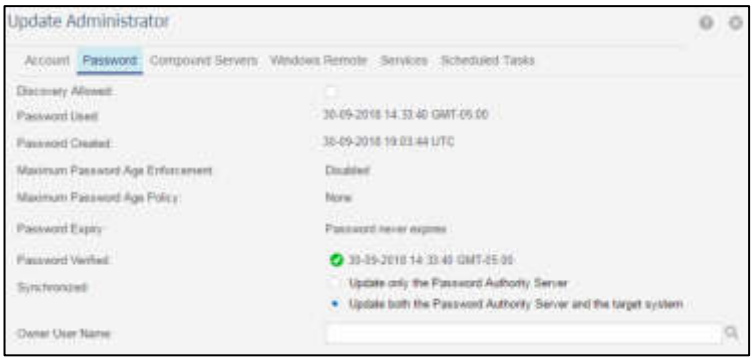


- **Creación de Cuenta**

En la siguiente imagen se procede a crear la cuenta administradora del servicio de tipo RDP.

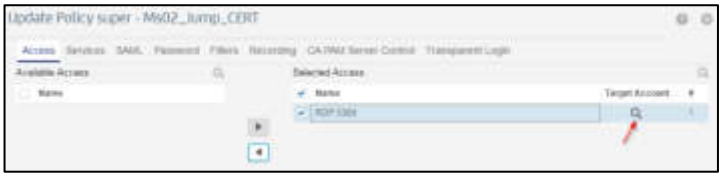


En la siguiente imagen se sincroniza la contraseña que será utilizado por el administrador del servicio.



- **Creación de Política de Acceso**

En la siguiente imagen se procede a integrar el servicio con el equipo que contendrá este servicio.



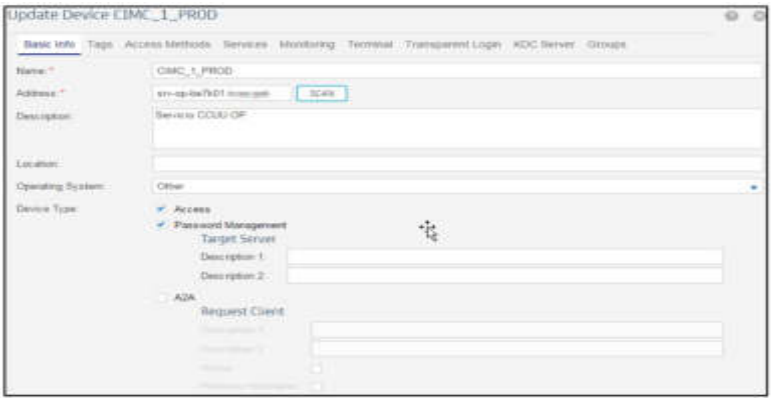
En la siguiente imagen se elige el nombre del administrador que se hará cargo del servicio.

En la siguiente imagen se configura el tipo de grabación que hará el sistema cuando utilicen este servicio. Para ello se activó de tipo gráfico y de violación de comandos.

b. Ambiente Producción

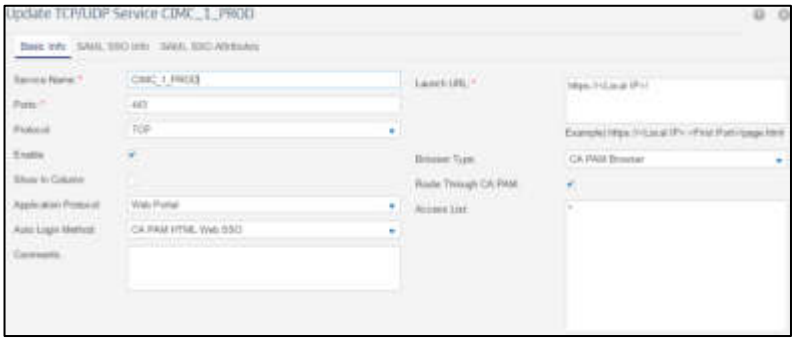
- **Aplicativos tipo Web**
  - **Creación del Dispositivo CIMC_1_PROD**

    La siguiente imagen representa la creación del equipo CIMC_1_PROD, para ello se debe completar el nombre que tendrá el equipo web, la IP, el sistema operativo, el tipo de acceso, y el pasword Management para que CA PAM rote la contraseña en cada cierto tiempo.



  - **Creación del Servicio**

    En la siguiente imagen se procede a crear el servicio que será integrado en el dispositivo creado.

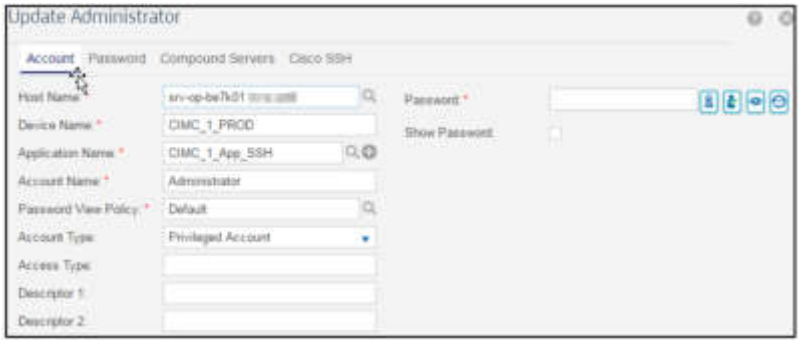


  - **Creación del Conector de la Aplicación**

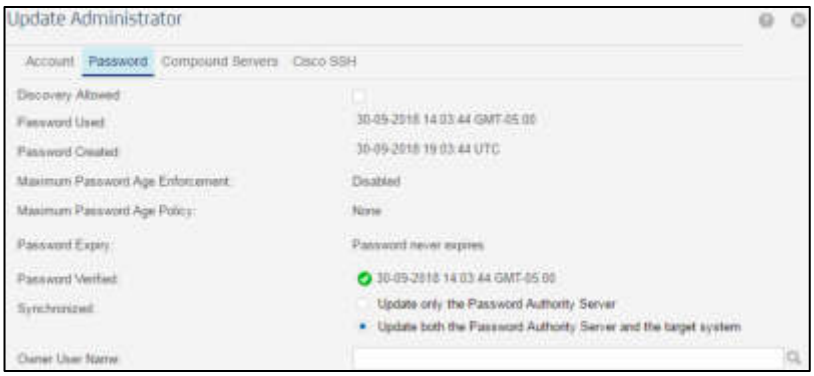
    En la siguiente imagen se procede a crear el aplicativo que será integrado al servicio para ello se necesita ingresar el nombre de la máquina, del servicio, de la aplicación y el tipo de aplicación.

- **Creación de Cuenta**

En la siguiente imagen se procede a configurar el nombre de la cuenta del usuario administrador que tendrá acceso al aplicativo creado.



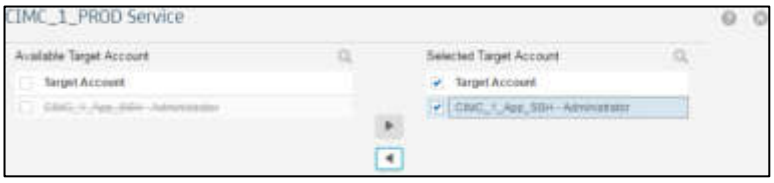
En la siguiente imagen se procede a sincronizar la contraseña del administrador del aplicativo registrado.



- **Creación de Política de Acceso**

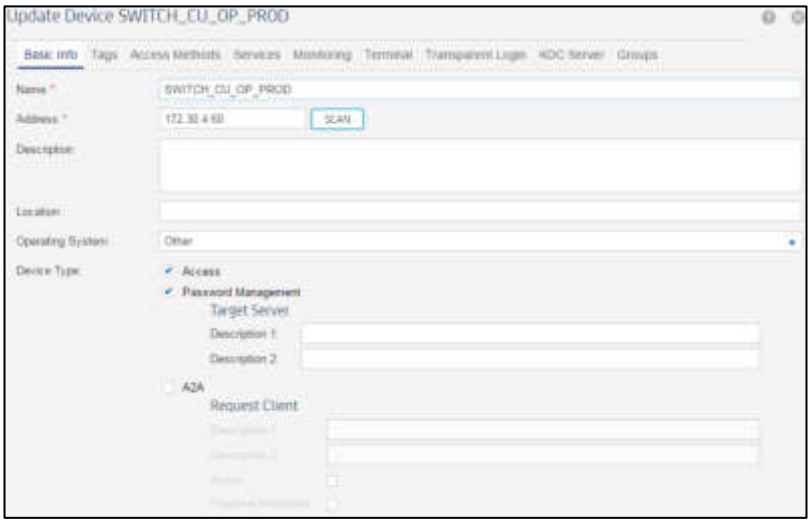
En la siguiente imagen se procede a integrar el servicio con el equipo creado imágenes anteriores

Luego de haber integrado el servicio con el equipo se procede agregar al encargado del aplicativo.



- **Aplicativos tipo SSH**
  - **Creación del Dispositivo Switch CU OP**

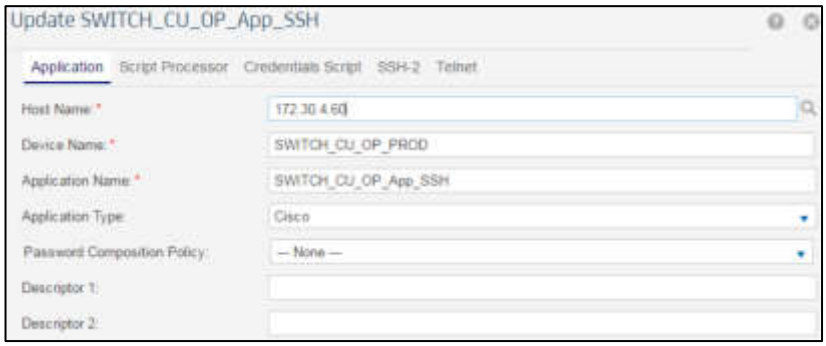
La siguiente imagen representa la creación del equipo Switch CU OP, para ello se debe completar el nombre que tendrá el equipo web, la IP, el sistema operativo, el tipo de acceso, y el pasword Management para que CA PAM rote la contraseña en cada cierto tiempo.



En la siguiente imagen se procede a configurar el modo de acceso y el puerto que se necesita para conectarse al equipo.

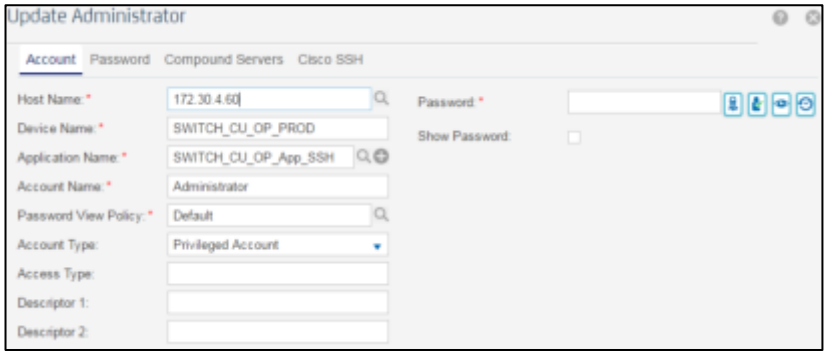
- **Creación del Conector de la Aplicación**

En la siguiente imagen se procede a crear el aplicativo que será integrado al servicio para ello se necesita ingresar el nombre de la máquina, del servicio, de la aplicación y el tipo de aplicación

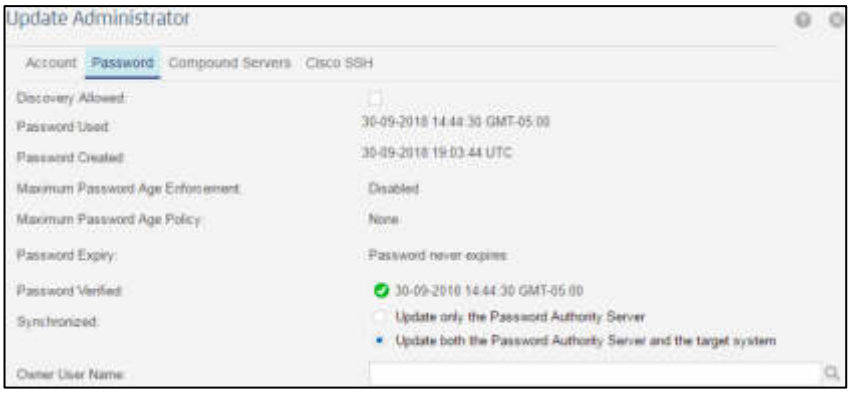


- **Creación de Cuenta**

En la siguiente imagen se procede a configurar el nombre de la cuenta del usuario administrador que tendrá acceso al aplicativo creado.



En la siguiente imagen se procede a sincronizar la contraseña del administrador del aplicativo registrado.



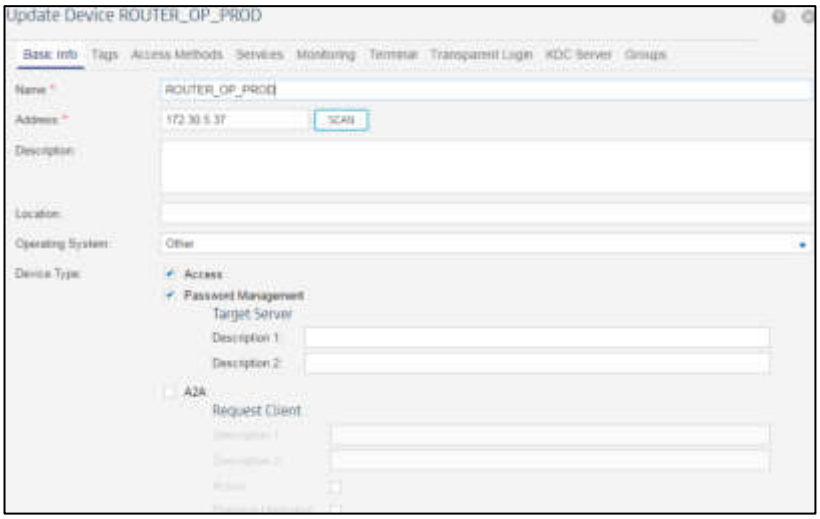
- **Creación de Política de Acceso**

En la siguiente imagen se procede a integrar el servicio con el equipo creado imágenes anteriores

Luego de haber integrado el servicio con el equipo se procede agregar al encargado del aplicativo.

- **Creación del Dispositivo Router OP**

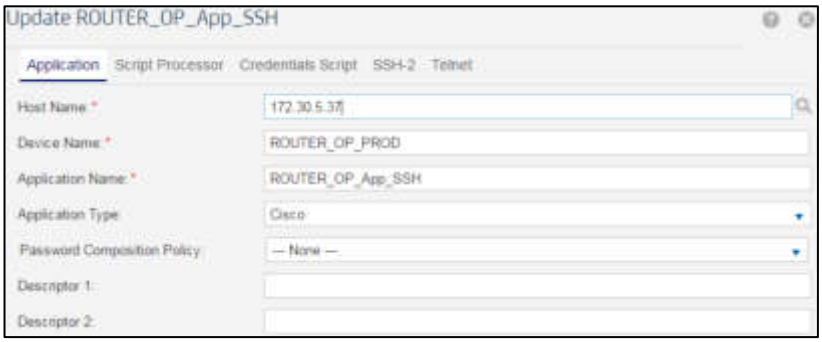
La siguiente imagen representa la creación del equipo Router OP, para ello se debe completar el nombre que tendrá el equipo web, la IP, el sistema operativo, el tipo de acceso, y el pasword Management para que CA PAM rote la contraseña en cada cierto tiempo.



En la siguiente imagen se procede a configurar el modo de conexión y el puerto que se necesita para acceder al equipo.

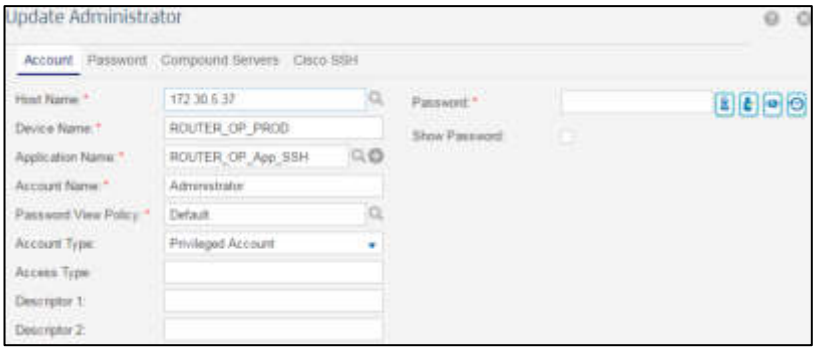
- **Creación del Conector de la Aplicación**

En la siguiente imagen se procede a crear el aplicativo que será integrado al servicio para ello se necesita ingresar el nombre de la máquina, del servicio, de la aplicación y el tipo de aplicación



- **Creación de Cuenta**

En la siguiente imagen se procede a configurar el nombre de la cuenta del usuario administrador que tendrá acceso al aplicativo creado.



En la siguiente imagen se procede a sincronizar la contraseña del administrador del aplicativo registrado.

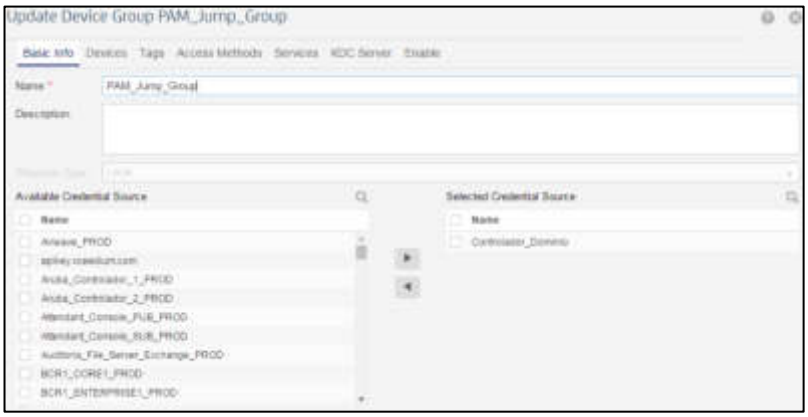
- **Creación de Política de Acceso**

En la siguiente imagen se procede a integrar el servicio con el equipo creado imágenes anteriores

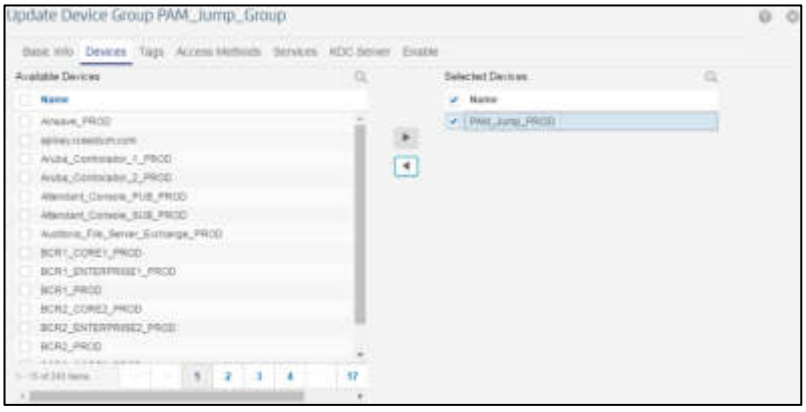
Luego de haber integrado el servicio con el equipo se procede agregar al encargado del aplicativo.

- **Aplicativos tipo Cliente / Servidor**
  - **Creación del Grupo de Dispositivo Xming CSRV07**

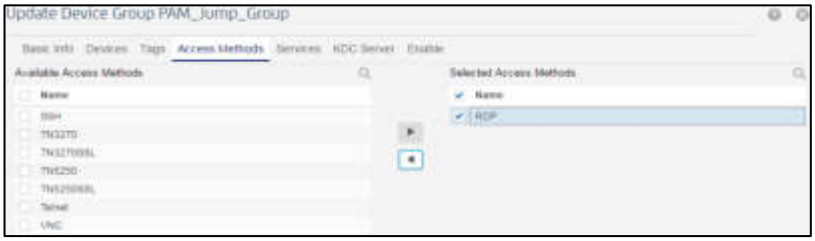
En la siguiente imagen se procede a crear el grupo que contendrá a un conjunto de dispositivos.



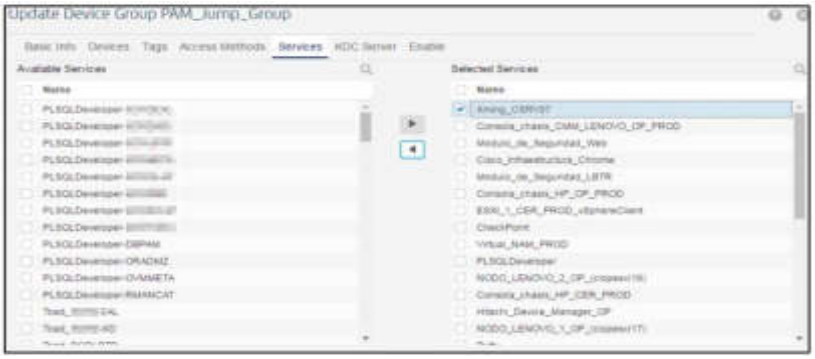
En la siguiente imagen se procede a integrar el dispositivo con el servicio.



En la siguiente imagen se configura el método de acceso al servicio.

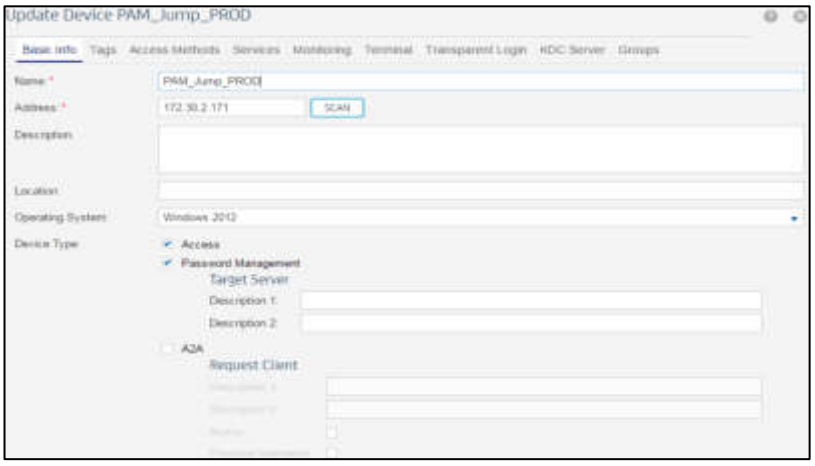


En la siguiente imagen se integra el servicio cliente servidor con el equipo

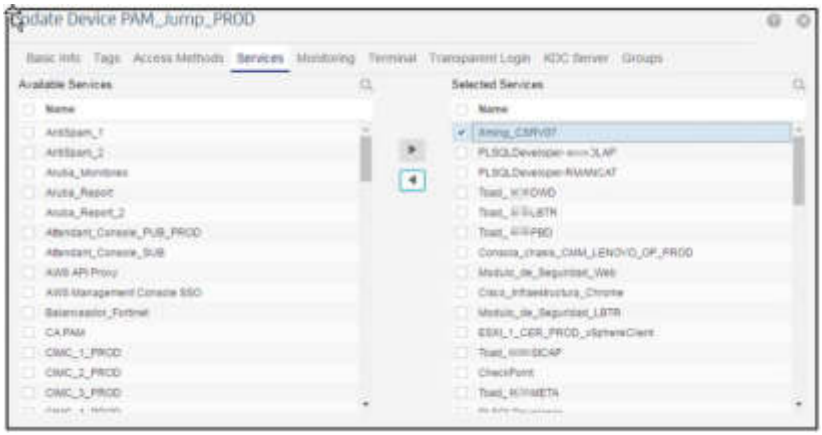


- **Creación de Dispositivo**

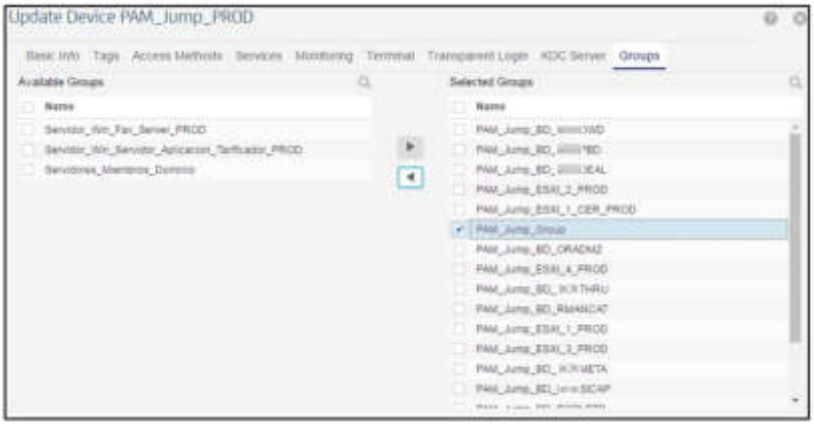
  La siguiente imagen representa la creación del dispositivo para ello se debe completar el nombre que tendrá el equipo web, la IP, el sistema operativo, el tipo de acceso, y el password Management para que CA PAM rote la contraseña en cada cierto tiempo.



En la siguiente imagen se elige el tipo de servicio a integrar al equipo.



En la siguiente imagen se activa el grupo que contiene el servicio.



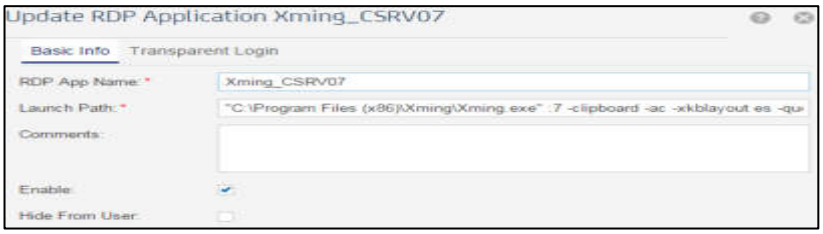
- **Creación de Transparent Login**

Se procede a crear las políticas de transparencia del login.

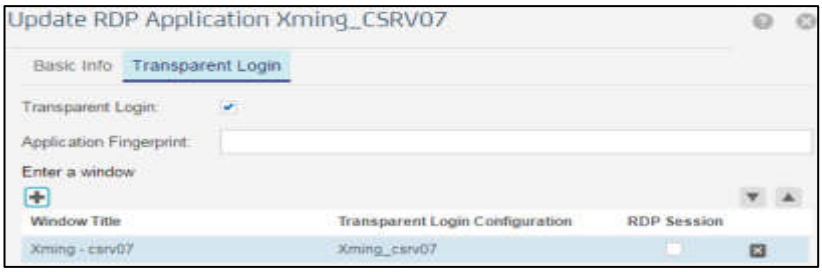
- **Creación de RDP Application**

Launch Path: “C:\Program Files (x86)\Xming\Xming.exe" :7 -clipboard -ac -xkblayout es -query csrv07

En la siguiente imagen se configure la ruta desde donde será ejecutado el servicio creado.

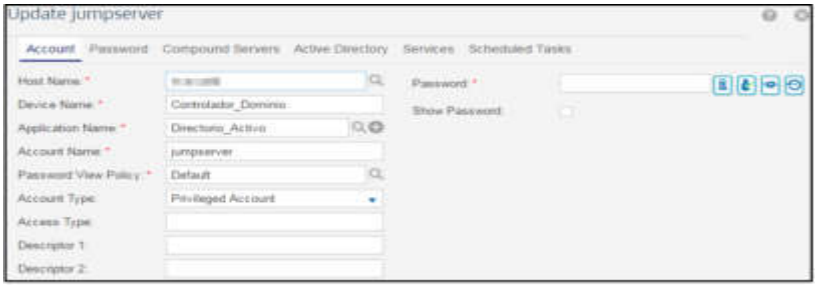


En la siguiente imagen se activa que la transparencia del login esté activo.

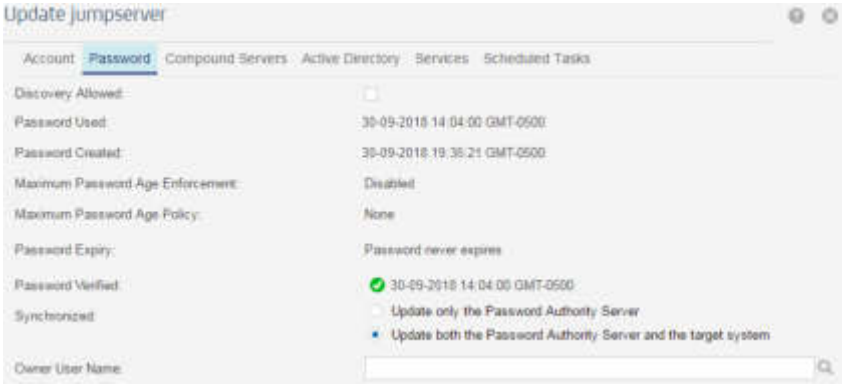


- **Creación de Cuenta**

En la siguiente imagen se crea la cuenta que administrará el servicio de dominio creado.

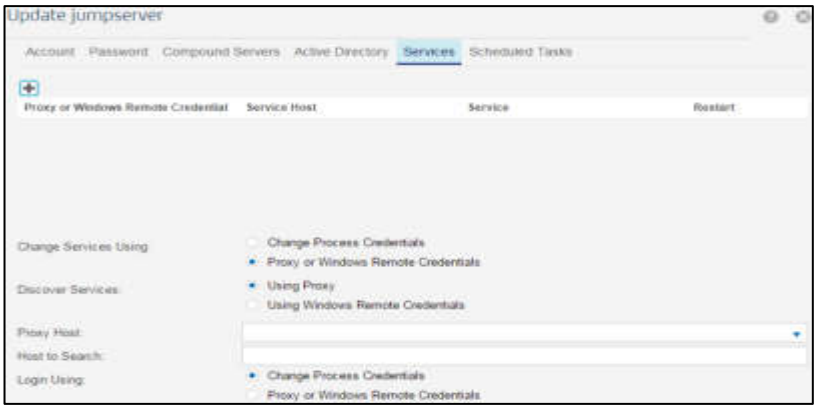


En la siguiente imagen se activa la sincronización de las credenciales con el servidor CA PAM.

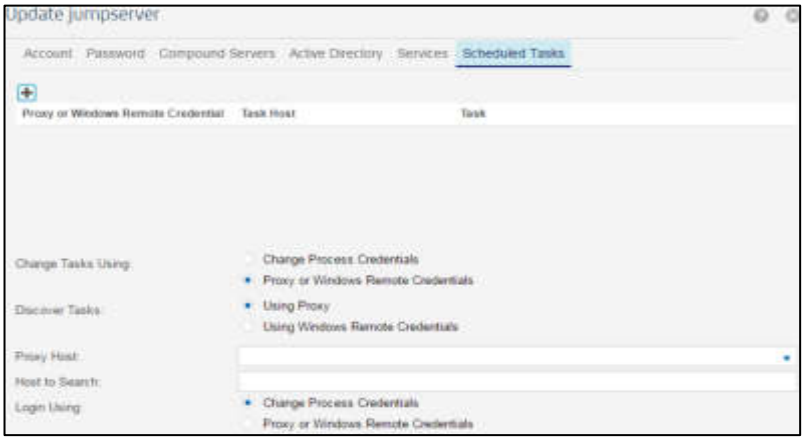


En la siguiente imagen se procede a activar el directorio del servicio.

En la siguiente imagen se procede activar el tipo de servicio.



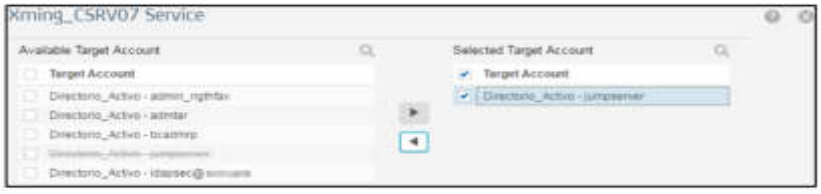
En la siguiente imagen se cambia la configuración de conexión remota, para ello se crean tareas.



- **Creación de Política de Acceso**

Se procede a crear políticas de acceso, se empieza primero integrando el servicio al equipo.

En la siguiente imagen se procede a activar la cuenta del administrador del servicio.

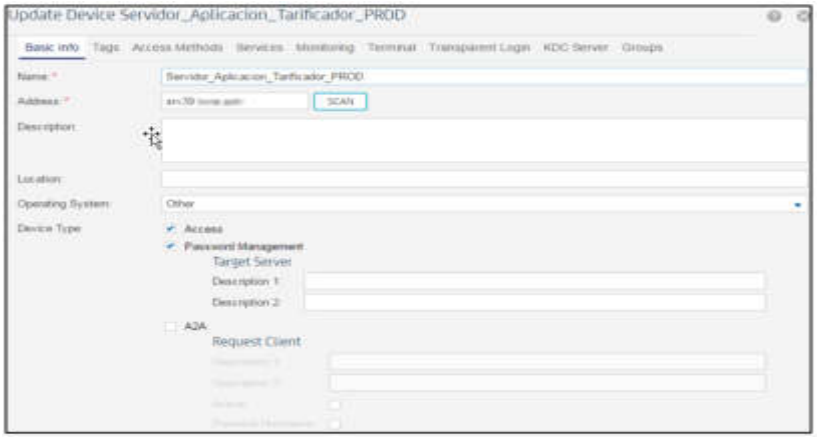


En la siguiente imagen se activa el tipo de grabado que tendrá para este servicio.

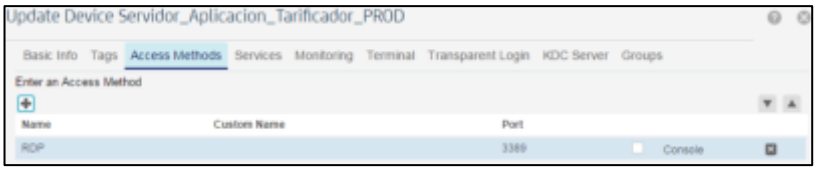
En la siguiente imagen se habilita que el login sea transparente, para que no sea utilizado teclas especiales y tampoco el clic derecho.

- **Aplicativos Tipo RDP**
  - **Creación del Dispositivo Tarificador**

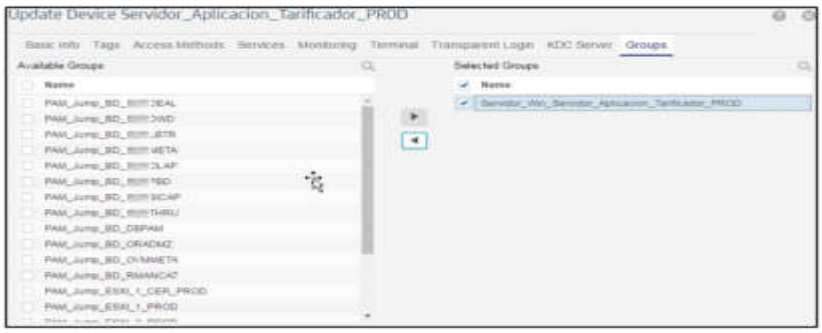
En la siguiente imagen se procede a crear el equipo que contendrá el servicio.



En la siguiente imagen se activa el tipo de puerto a utilizar para la conexión remota, para este tipo de servicio se habilita el puerto 3389.

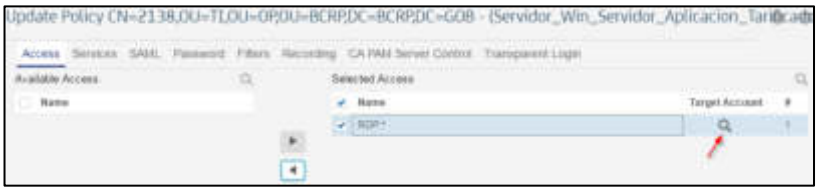


En la siguiente imagen se integra el servicio al grupo.

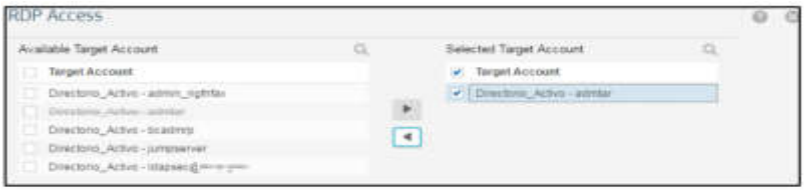


- **Creación de Política de Acceso**

En la siguiente imagen se elige el tipo de servicio a integrar al equipo.



En la siguiente imagen se elige la cuenta del administrador del servicio.



En la siguiente imagen se procede activar el tipo de grabado que tendrá este servicio, para este caso es gráfica y violaciones.

Anexo 3: Guía de Usuario CA PAM

Acceso Seguro a CA PAM

Para el acceso a los sistemas de información de la empresa de retail es necesario que cada usuario administrador realice los siguientes pasos con el objetivo de otorgar un acceso seguro a la consola de identidades privilegiadas.

- **Instalación cliente CA PAM**

  A continuación, se describe los pasos a realizar para la instalación de CA PAM Client. Realizar los siguientes pasos:

Actividad	Secuencia
Instalación de CA PAM Client	Acceder a la siguiente ruta: • G:\util\pam
	Copiar instalador "CAPAMClientInstall_V3.1.1.exe" a su equipo Windows.
	Ejecutar el instalador.
	Seleccionar la opción "Next".
	Aceptar la licencia y seleccionar "Next".
	Elegir la opción "Typical" y seleccionar "Next".
	Definir la ubicación donde se instalará el cliente. De lo contrario, instalará sobre la ruta por defecto.
	Seleccionar "Next" y por último seleccionar "Install".
	Seleccionar "Next".
	Seleccionar "Yes" y luego seleccionar "Done".

- **Acceso a CA PAM**

  A continuación, se describe los pasos a realizar para iniciar sesión en CA PAM con 2FA. Realizar los siguientes pasos:

Actividad	Secuencia
Autenticar en CA PAM	Ejecutar el cliente de CA PAM y definir los siguientes datos: • Address: pam. cpb.pe • Connect Mode: WEB Y seleccionar “Connect”.
	Ingresar los siguientes datos: • Username: [Cuenta de AD] • Password: [Contraseña de AD] • Authentication type: LDAP+RADIUS • Domain: CPB.PE Y seleccionar “Login”.

- **Acceso a Sistemas**

  A continuación, se describe los pasos a seguir para autenticarse a CA PAM.

Actividad	Secuencia

Acceder a un Sistema desde CA PAM	Una vez autenticado a CA PAM, dentro de la sección “Access” tendrá las siguientes columnas:
	• Datos de los Dispositivos:
	  • Device Name: [Nombre del dispositivo]
	  • Address: [Dirección IP del dispositivo]
	  • Operating System: [Plataforma del dispositivo]
	• Formas de Acceso acorde a la App:
	  • Access Methods: [Tipo de acceso que utilizará para acceder al sistema operativo. Por ejm: SSH, RDP]
	  • Web Portal: [Tipo de acceso que utilizará para acceder a aplicaciones web]
	  • RDP Applications: [Tipo de acceso para aplicaciones de tipo C/S alojadas en el servidor terminal]

	Para acceder a un dispositivo, seleccionar el botón acorde a la aplicación que requiere acceder.

- **Acceso a Sistemas con Flujo de Aprobación**

Actividad	Secuencia

Solicitar Acceso	Una vez autenticado a CA PAM, dentro de la sección “Access” tendrá las siguientes columnas:
	• Datos de los Dispositivos:
	  ◦ Device Name: [Nombre del dispositivo]
	  ◦ Address: [Dirección IP del dispositivo]
	  ◦ Operating System: [Plataforma del dispositivo]
	• Formas de Acceso acorde a la App:
	  ◦ Access Methods: [Tipo de acceso que utilizará para acceder al sistema operativo. Por ejm: SSH, RDP]
	  ◦ Web Portal: [Tipo de acceso que utilizará para acceder a aplicaciones web]
	  ◦ RDP Applications: [Tipo de acceso para aplicaciones de tipo C/S alojadas en el servidor terminal]

	Para generar una solicitud de acceso, seleccionar el dispositivo que requiere acceder.
	Seleccionar la cuenta con la que se desea acceder al dispositivo.
	En la ventana Auto Connect llenar los siguientes campos • Request Password From: [Fecha de Inicio de Acceso al Dispositivo] • Request Password To: [Fecha Final de Acceso al Dispositivo] • Reason: [Razón o motivo de la Solicitud de Acceso] • Reason Description: [Detalle de la Solicitud de Acceso] • Reference Code: [Código de Referencia de la Solicitud] Y seleccionar Ok.
	La solicitud será notificada al aprobador definido. Una vez aprobada o rechazada la solicitud, será notificado.

Autoservicio CA PAM

- **Personalización de Cuenta**

A continuación, se describe los pasos a seguir para personalizar la cuenta de CA PAM acorde a las preferencias del usuario.

Actividad	Secuencia
Personalización	Iniciar Sesión en CA PAM. (Según el punto 2.4)
	seleccionar sobre su nombre y el sistema le mostrara las siguientes pestañas: • Administration Podrá habilitar la opción de recibir notificación cada vez su cuenta es utilizada para acceder a CA PAM. • Terminal Customization Podrá personalizar consola CLI con diversas opciones como: Dimensiones, tamaño de letra, color de cursos, color de fono entre otros según su elección. Podrá definir resolución de la consola RDP. (Recomendado Fullscreen)
	Seleccionar la opción “OK” para aplicar los cambios.

Anexo 4: Plan de Recuperación del Servicio

a. Servicio Clúster Falla

A continuación, se describirá las acciones a realizar ante alguna incidencia en el servicio de clúster, ya sea por: latencia en la red, falla del sistema, *datacenter* caído u otro factor que afecte el servicio de acceso privilegiado a los especialistas desde el balanceador.

El siguiente procedimiento permitirá que los usuarios logren acceder directamente a un nodo, de tal forma que se mantenga el servicio disponible para los especialistas.

Pasos	Descripción
1. Detener Clúster	➢ Acceder a un nodo de CA PAM https://pam01.cpb.pe o https://pam02. cpb.pe ➢ Apagar cluster o Ir a Configuration, luego Clustering o Clic en Turn Cluster Off
2. Desbloquear Credential Manager	➢ Acceder a un nodo PAM o Ir a Configuration, luego Clustering o Clic en Unlock Me **Nota:** Es necesario desbloquear la base de datos del nodo que dará servicio mientras el clúster se encuentre apagado.

Notas Importantes:

- CA PAM Client debe apuntar a uno de los 2 nodos que se encuentra habilitado para acceder mientras el clúster se encuentre apagado.
- Cuando el clúster está apagado, es importante que todos los cambios, modificaciones, creaciones se realicen únicamente sobre un nodo de PAM. Cuando se enciende nuevamente el clúster, el nodo de PAM que tiene los nuevos cambios, modificaciones, creaciones debe ser miembro primario en el clúster para evitar des-sincronización con el otro nodo de PAM.

b. Generación de Backups

Para restaurar las instancias de CA PAM por cualquier razón, es necesario ejecutar los respaldos de base de datos y/o configuración. Los backups son

administrados desde la consola UI de CA PAM.

Backup de Base de Datos: Respaldo que contiene todos los datos aprovisionados, incluye:

- Usuarios y Grupos de Usuarios
- Dispositivos y Grupo de Dispositivos
- Configuración de Command Filter
- Políticas
- Datos de Credendial Manager

Este respaldo puede ser restaurado en otro appliance mas no se podrá desencriptar las contraseñas almacenas en la base de datos “Credential Manager”.

Backup de Configuración: Respaldo que contiene información de definiciones y configuración de una instancia de CA PAM.

A continuación, se detallan los pasos a realizar para ejecutar los respaldos de base de datos y configuración de cada nodo de CA PAM.

Paso	Descripción
1. Respaldo de Ambiente	➢ Respaldos o Acceder a un nodo de CA PAM https://pam01. cpb.pe o https://pam02. cpb.pe o Ir a Configuration, luego Database o Clic en Save Database and Configuration Se crearán 2 archivos: ▪ **Respaldo de Configuración:** File Type: Config File Name: gk[Año/Mes/Dia][Hora-UTC].cfg ▪ **Respaldo de Base de Datos:** File Type: Database File Name: gkdatabase[Año/Mes/Dia][Hora-UTC].gz o Seleccionar cada tipo de archivo y clic en Download. **Nota:** Repetir el procedimiento en el otro nodo de PAM del clúster.

Notas Importantes:

- Cada nodo de PAM está configurado para realizar el backup de manera automática y enviarlo a un repositorio externo.

- Es importante diferenciar los respaldos que se generen tanto del nodo PAM01 como del nodo PAM02. No es posible restaurar la base de datos y/o configuración del nodo PAM01 en el nodo PAM02 o viceversa por seguridad.

c. Recuperación del Ambiente

El proceso de recuperación de ambiente permitirá restaurar las bases de datos y/o configuración a partir de los respaldos previamente ejecutados.

A continuación, se describirá los pasos a realizar para restaurar la base de datos y/o configuración.

Pasos	Descripción
1. Restauración de Ambiente	➢ Restaurar respaldos o Acceder al nodo de PAM https://pam01. cpb.pe o https://pam02. cpb.pe o Ir a Configuration, luego Database. o Clic en Restore, luego en Choose File para seleccionar la base de datos/configuración apropiado al nodo que se restaurará. o Clic en Restore y Ok para confirmar la ejecución de la restauración. o Esperar que el nodo reinicie y validar las credenciales restauradas.

Notas Importantes:

La instancia de PAM se revierte a un estado anterior, incluyendo las contraseñas almacenadas en la bóveda de credenciales.

- El servidor sobre escribe todos los registros de sesiones. Sin embargo, antes de restaurar, se puede salvar y descargar los registros del nodo.
- La restauración no interfiere con las grabaciones de sesión. Las grabaciones de sesión son almacenadas externamente.
- El texto resaltado en rojo que indica una violación dentro de las grabaciones de sesión se pierde durante el intervalo posterior a la última vez que se respaldó la base de datos.

d. Bóveda Física

Es importante mantener un respaldo manual (bóveda física) ante incidentes / desastres que eviten recuperar el sistema con los procedimientos previamente descritos.

Que debe contener la bóveda física:

- 01 Credencial privilegiada de cada sistema que está custodiado por CA PAM.

En tal sentido, si ocurriera lo sgt. en conjunto:

- No disponibilidad del servicio de PAM en ninguno de los nodos.
- Respaldos de backup corruptos o no contiene información actualizada.
- Servicio de virtualización o *Datacenter* no disponible.
- Otro factor que no permita recuperar el servicio de PAM para el acceso automatizado a los dispositivos.

Se procede con el acceso convencional a los dispositivos que son custodiados por PAM, a través de las credenciales almacenadas en **Bóveda Física.**

Notas Importantes:

Este procedimiento, contempla la recuperación de Usuarios, Grupos, Políticas, Configuraciones, Credenciales Privilegiadas.

Después del establecimiento del ambiente productivo, se debe validar por lo menos: pruebas de acceso a los dispositivos por parte del administrador de la solución, validación de funcionalidades habilitadas, tales como: grabación de sesiones, acceso por SSH/RDP/Web nativo, acceso a aplicaciones via Jump Server.

El documento contiene, únicamente, procedimientos y conceptos relacionado a CA PAM. Procedimientos adicionales dentro de CA PAM como: salvar registros, reproducir grabaciones sesiones.

Anexo 5: Guía de Proveedor CA PAM

Acceso Seguro a CA PAM

Acceso a CA PAM

Requisito:

- El proveedor debe tener una cuenta de AD para que pueda autenticarse a CA PAM.

A continuación, se describe los pasos a realizar para iniciar sesión en CA PAM.

Actividad	Secuencia
Acceder a CA PAM	Ejecutar el cliente de CA PAM (ubicado en el escritorio del equipo Windows) y definir los siguientes datos: • Address: pam.cbp.pe • Connect Mode: WEB Y seleccionar “Connect”.
	Ingresar los siguientes datos: • Username: [Cuenta de AD] • Password: [Contraseña de AD] • Authentication type: LDAP Y seleccionar “Login”.

Acceso a Sistemas

Requisito:

- El administrador de CA PAM debe asignarle los accesos a los sistemas que requiera el proveedor.

A continuación, se describe los pasos a seguir para acceder a los dispositivos.

Actividad	Secuencia

Acceder a un Sistema desde CA PAM	Una vez autenticado a CA PAM, dentro de la sección “Access” tendrá las siguientes columnas:
	• Datos de los Dispositivos:
	  • Device Name: [Nombre del dispositivo]
	  • Address: [Dirección IP del dispositivo]
	  • Operating System: [Plataforma del dispositivo]
	• Formas de Acceso acorde a la App:
	  • Access Methods: [Tipo de acceso que utilizará para acceder al sistema operativo. Por ejm: SSH, RDP]
	  • Web Portal: [Tipo de acceso que utilizará para acceder a aplicaciones web]
	  • RDP Applications: [Tipo de acceso para aplicaciones de tipo C/S alojadas en el servidor terminal]

	Para acceder a un dispositivo, seleccionar el botón acorde a la aplicación que requiere acceder.

--- Fin del Documento ---

Anexo 6: Encuesta

Las siguientes encuestas son planteadas para los trabajadores de una empresa de RETAIL, con el objetivo de determinar el tiempo promedio que le tomaba a cada uno en acceder a los activos de TI.

1.- ¿A cuántos activos de TI tiene acceso?

A)	1 a 5
B)	6 a 10
C)	11 a 15
D)	16 a 20
E)	21 a más

2.- ¿A cuántos activos de TI accede al día?

A)	1 a 5
B)	6 a 10
C)	11 a 15
D)	16 a 20
E)	21 a más

3.- ¿Las credenciales que utilizaba es la misma para todos los activos de TI?

A)	Sí
B)	NO

4.- Si la respuesta de la pregunta anterior es NO, entonces ¿Cuántas credenciales en total utilizaba para autenticarse a todos los activos de TI?

A)	1 a 5
B)	6 a 10
C)	11 a 15
D)	16 a 20
E)	21 a más

5.- ¿Tenía registrado sus contraseñas en algún post-it, bloc de nota, celular o en algún otro lugar?

A)	Sí
B)	NO

6.- ¿Cuánto tiempo tardaba en acceder a un activo de TI?

Anterior	
A)	0 a 30 segundos
B)	31 a 59 segundos
C)	1 a 2 minutos
D)	2.01 a más

7.- ¿Cuánto tiempo tarda en acceder a un activo de TI con la solución CA PAM?

Ahora	
A)	0 a 30 segundos
B)	31 a 59 segundos
C)	1 a 2 minutos
D)	2.01 a más