ESCUELA SUPERIOR POLITÉCNICA DEL LITORAL

Facultad de Ingeniería en Electricidad y Computación

Maestría en Seguridad Informática Aplicada

"IMPLEMENTACIÓN DE UNA SOLUCIÓN DE BÓVEDA DE SEGURIDAD PARA ADMINISTRAR CREDENCIALES PRIVILEGIADAS DE LOS ACTIVOS INFORMÁTICOS DE UNA EMPRESA DE TELECOMUNICACIONES"

EXAMEN DE GRADO (COMPLEXIVO)

PREVIO A LA OBTENCIÓN DEL TITULO DE GRADO:

MAGISTER EN SEGURIDAD INFORMÁTICA APLICADA

DIEGO ARMANDO JIMÉNEZ PLUAS

GUAYAQUIL – ECUADOR

AÑO: 2015

AGRADECIMIENTO

A Dios por darme la oportunidad de poder cumplir una meta más en mi vida profesional.

A mis compañeros de clase y profesores que me apoyaron directa o indirectamente durante el desarrollo de la maestría.

A mi amigo, y socio de negocios Daniel Salcedo por su constante apoyo lo cual me ha dado la confianza de creer en mis habilidades profesionales y como persona.

DEDICATORIA

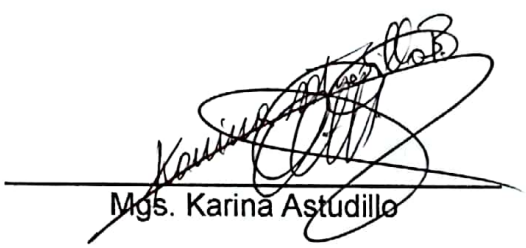
A mi madre Betty y mi hermano Christian por el apoyo constante durante mi vida profesional y durante el desarrollo de la maestría, dándome aliento en los momentos más difíciles y alentándome a seguir siempre hacia adelante.

A todos mis hermanos y familiares que me han apoyado directa o indirectamente a poder culminar una meta más.

TRIBUNAL DE SUSTENTACIÓN

Ing. Lenin Freire

DIRECTOR MSIA



Mgs. Karina Astudillo

PROFESOR DELEGADO

POR LA UNIDAD ACADÉMICA

RESUMEN

El presente documento reúne las diferentes fases que se manejaron durante un proyecto de Implementación de Bóveda de Seguridad de Credenciales Privilegiadas de Activos Informáticos. El proyecto dio inicio a mediados del año 2014 en una compañía de telecomunicaciones del país, con el objetivo de integrar una solución de seguridad en la compañía que ayude a administrar de forma centralizada las credenciales privilegiadas de los activos o plataformas tecnológicas, manejando así registros de uso y controles de acceso para prevenir posibles incidentes de seguridad sobre las mismas.

La solución de Bóveda de Seguridad implementada cuenta con mecanismos de seguridad que le permite almacenar y administrar de forma centralizada las credenciales privilegiadas y poder manejar controles, perfiles de accesos y esquemas de registro. Para el efecto se dispone de las siguientes clasificaciones asociadas a las credenciales privilegiadas:

- Credenciales Privilegiadas: llámese a éstas los usuarios y claves con permisos de acceso total sobre una plataforma las cuales se dividen en las siguientes:

- Usuarios Built-in: usuarios nativos de un sistema o plataforma con privilegios de super-usuario, sean estos “root”, “admin”, “administrador”, “sys”, y todo aquel usuario que venga creado por defecto y que tenga privilegios elevados para ejecución de tareas administrativas.
- Usuarios Administradores: usuarios personalizados creados con el fin de ayudar a delegar la administración de una plataforma o activo tecnológico.
- Usuarios de Aplicativos o Procesos: usuarios personalizados con privilegios que ayudan a ejecutar tareas automáticas sin la necesidad de que un administrador intervenga en dicho proceso.

ÍNDICE GENERAL

AGRADECIMIENTO ii

DEDICATORIA iii

RESUMEN v

ÍNDICE GENERAL vii

ABREVIATURAS Y SIMBOLOGÍA x

ÍNDICE DE FIGURAS xii

ÍNDICE DE TABLAS xiii

INTRODUCCIÓN xiv

Capítulo 1 1

GENERALIDADES 1

1.1 Antecedentes 1

1.2 Objetivo General 2

1.3 Descripción del Problema 3

1.4 Solución Propuesta 4

Capítulo 2 7

METODOLOGÍA DE DESARROLLO DE LA SOLUCIÓN 7

2.1 Planteamiento 7

2.1.1 Fase 1: Presentación del proyecto al Directorio Ejecutivo de la empresa 8

2.1.2 Fase 2: Levantamiento de información 8

2.1.3 Fase 3: Definición de activos y credenciales privilegiadas 9

2.1.4 Fase 4: Definición de perfiles de acceso 9
2.1.5 Fase 5: Esquemas de contingencia 10
2.1.6 Fase 6: Definición de políticas y procedimientos internos 10
2.2 Desafíos del Proyecto 11
2.3 Evaluación de soluciones de Bóveda de Seguridad 12
2.4 Hitos del Proyecto 15
2.4.1 Hito 1: Definición y Alcance 16
2.4.2 Hito 2: Requerimientos Técnicos 17
2.4.3 Hito 3: Requerimientos Generales 27
2.4.4 Hito 4: Evaluación de las soluciones de Bóveda de Seguridad 34
2.4.5 Hito 5: Implementación de la solución de Bóveda de Seguridad 35
2.4.6 Hito 6: Traspaso de Conocimiento 38
2.4.7 Hito 7: Puesta en Marcha de la solución 38
Capítulo 3 40
RESULTADOS OBTENIDOS 40
3.1 Análisis de la solución de Bóveda de Seguridad 41
3.1.1 Identificación de activos integrados 41
3.1.2 Identificación de credenciales privilegiadas 42
3.2 Mejoras en los procedimientos de administración de las credenciales privilegiadas..... 43
3.3 Análisis de problemática resuelta por la Bóveda de Seguridad 49
3.4 Limitaciones de la solución 54

CONCLUSIONES Y RECOMENDACIONES 56

BIBLIOGRAFÍA.....60

ABREVIATURAS Y SIMBOLOGÍA

ACCOUNTING	Auditoria o registros de actividades en ámbito IT
ACTIVE DIRECTORY	Servicio de directorio de Windows.
AES	Algoritmo de cifrado.
ANTISPAM	Sistema de prevención de correo basura.
AUTENTICACION	Procedimiento informático que asegura un servicio.
AUTORIZACION	Procedimiento informático que asegura un servicio.
APIs	Interfaz de programación de aplicaciones informáticas.
C++	Lenguaje de desarrollo.
CHECK-IN	Proceso de solicitud de clave privilegiada.
CHECK-OUT	Proceso de devolución de clave privilegiada.
CHECKLIST	Lista de comprobación.
DC	Servicio de controlador de dominio de Windows.
DES	Algoritmo de cifrado.
FW	Cortafuegos de red de datos.
GARTNERT	Empresa consultora y de investigación de TI
HARDENING	Proceso de aseguramiento de un sistema.
HARDWARE	Componentes físicos de un computador.
IN-HOUSE	Interno de la empresa.
IP	Etiqueta numérica única que identifica un computador.
IPS	Sistema informático de prevención de intrusos.

ISO 27000	Estándar de Seguridad de la Información.
JAVA	Lenguaje de desarrollo.
LDAP	Servicio de directorio Linux.
LOG	Archivo de registro de sistema.
OTP	Contraseña de un solo uso.
PC	Computador personal.
PCI-DSS	Estándar de Seguridad de la Información.
PERL	Lenguaje de desarrollo.
POC	Prueba de concepto.
POSTGRES	Sistema de gestión de bases de datos.
SHA	Algoritmo de autenticación.
SMS	Servicio de mensajes cortos.
SOX	Estándar de Seguridad de la Información.
SSL	Protocolo criptográfico de comunicaciones seguras.
TACACS	Sistema de control de acceso a terminales.
WEBSERVICE	Servicio web de intercambio de datos entre aplicaciones.
WORKFLOW	Flujo de trabajo.

ÍNDICE DE FIGURAS

FIGURA 1. 1 MÓDULOS PRINCIPALES DE LA BÓVEDA DE SEGURIDAD. 6

FIGURA 2. 1 GARTNER - LISTA DE FABRICANTES REPRESENTATIVOS Y CARACTERÍSTICAS PRINCIPALES (AÑO 2014). 13

FIGURA 2. 2 DIAGRAMA LÓGICO DE LA SOLUCIÓN DE BÓVEDA DE SEGURIDAD. 30

FIGURA 2. 3 RESULTADO DE EVALUACIÓN DE SOLUCIONES DE BÓVEDA DE SEGURIDAD. 35

FIGURA 3. 1 FLUJO DE APROBACIÓN DE ACCESO A USUARIOS INTERNOS. 44

FIGURA 3. 2 FLUJO DE APROBACIÓN DE ACCESO A USUARIOS EXTERNOS. 45

FIGURA 3. 3 FLUJO DE APROBACIÓN DE INTEGRACIÓN DE ACTIVOS TECNOLÓGICOS. 46

FIGURA 3. 4 FLUJO DE APROBACIÓN DE ELIMINACIÓN DE ACTIVOS. 47

FIGURA 3. 5 FLUJO DE APROBACIÓN DE INTEGRACIÓN DE CREDENCIALES PRIVILEGIADAS. 48

FIGURA 3. 6 FLUJO DE APROBACIÓN DE INTEGRACIÓN DE CREDENCIALES PRIVILEGIADAS. 48

FIGURA 3. 7 PORTAL DE ACCESO DE USUARIOS DE BÓVEDA DE SEGURIDAD. 50

FIGURA 3. 8 SOLICITUDES DE ACCESO PENDIENTES DE APROBACIÓN. 50

FIGURA 3. 9 PORTAL DE CONFIGURACIÓN DE ACTIVO/SISTEMA Y CONFIGURACIÓN DE TEMPORALIDAD DE CREDENCIAL…… 51

FIGURA 3. 10 PORTAL DE SOLICITUD DE ACCESO A CREDENCIALES. 51

FIGURA 3. 11 SOLICITUD DE ACCESO A UN ACTIVO MEDIANTE SESIÓN AUTOMÁTICA (INYECCIÓN AUTOMÁTICA DE CREDENCIALES) 52

FIGURA 3. 12 LISTADO DE REPORTES 53

FIGURA 3. 13 REPORTE DE ACTIVIDAD DE USUARIOS. 53

FIGURA 3. 14 REPORTE DE USO DE CREDENCIALES. 53

FIGURA 3. 15 CONFIGURACIÓN DE REINICIO AUTOMÁTICO DE CLAVES. 54

ÍNDICE DE TABLAS

TABLA 1 SOLUCIONES DE BÓVEDA DE SEGURIDAD EVALUADAS..... 13

TABLA 2 CANTIDAD DE ACTIVOS TECNOLÓGICOS INTEGRADOS. 42

TABLA 3 CANTIDAD DE CREDENCIALES PRIVILEGIADAS INTEGRADAS. 43

INTRODUCCIÓN

Actualmente en el país, la compañías de telecomunicaciones están siendo observadas y reguladas por los entes gubernamentales que exigen que se manejen rigurosos estándares y niveles de disponibilidad de los servicios que prestan y la confidencialidad de la información sensible de los clientes a los cuales brindan dichos servicios. [1]

Entre las principales está la Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos, la cual indica que los clientes tienen derecho a la confidencialidad sobre los datos proporcionados en cualquier relación con un tercero, a la no circulación de los datos personales y a no recibir mensajes de datos no solicitados que puedan ser transmitidos por la red de comunicaciones. [2]

Debido a la gran cantidad de clientes y servicios que prestan, las empresas de telecomunicaciones han sido en los últimos años focos de cyber ataques los cuales son estructurados con fines lucrativos, competitivos del mercado o

simplemente la divulgación de información. Estos incidentes han ido en aumento en los últimos años, lo cual ha causado que las empresas afectadas sufran pérdidas y no solo a nivel monetario sino también ha causado que el nivel de confianza de los clientes disminuya e incluso se han visto sujetos a sanciones por parte del ente regulador. [3]

Debido a todos estos controles y demás leyes regulatorias, las empresas de telecomunicaciones han estado trabajando fuertemente en la reducción de las brechas de seguridad a través de la implementación de firewalls, sistemas de detecciones y prevenciones de intrusos, servicios de antispam, controles de accesos, entre otros.

Sin embargo, a nivel interno los controles, en algunos casos, no han sido lo suficientemente efectivos puesto que la administración de los incontables sistemas y plataformas que componen la infraestructura de servicios y las credenciales de acceso de éstas son almacenadas de manera insegura, muchas veces guardadas en hojas de cálculo, de texto e incluso en documentos físicos (impresos o escritos), poniendo en riesgo los servicios y

por consiguiente la operativa de la compañía debido que aumentan las probabilidades de que éstas credenciales sean filtradas y lleguen a manos de personal no autorizado o externo a la compañía.

En base a las necesidades de las operaciones que el negocio demanda, las empresas se están encaminando en la implementación de **Soluciones de Bóvedas de Seguridad de Credenciales Privilegiadas** que les permitan cubrir los siguientes macro objetivos:

- Almacenar de forma segura y centralizada las credenciales privilegiadas de los sistemas y plataformas tecnológicas.
- Administrar de forma centralizada y controlada dichas credenciales.
- Manejar un registro del uso de las credenciales privilegiadas tanto por personal administrativo, operativo e incluso externo o de soporte.

El lector encontrará en el desarrollo del presente documento las diferentes fases que se llevaron a cabo para la implementación del Proyecto de Bóveda de Seguridad, los alcances del proyecto y limitaciones de la solución de Bóveda de Seguridad implementada.

CAPÍTULO 1

GENERALIDADES

1.1 Antecedentes

En el ámbito de la seguridad informática, el objetivo principal es identificar las brechas de seguridad de un sistema, plataforma y/o proceso y evitar que éstas afecten la disponibilidad, la integridad y confidencialidad de los servicios y de la información que en estos contienen. [4]

Es de conocimiento público que empresas ecuatorianas han sido afectadas al día de hoy por algún tipo de ataque informático, sufriendo

graves violaciones en relación a la integridad de sus datos y la disponibilidad de los servicios que proveen, lo que lleva a preguntarse si las organizaciones están llevando los controles de seguridad de manera adecuada cumpliendo con los estándares establecidos en el mundo de la seguridad informática. [5]

Existen mecanismos actualmente que ayudan a proteger los activos informáticos y el almacenamiento de las credenciales privilegiadas, pero estas soluciones son muy limitadas y requieren de componentes adicionales para poder implementar la solución como tal, lo que implica en el aumento de tareas administrativas, dependencia de personal capacitado y el mantenimiento de dichas soluciones, lo que implica un aumento considerable del costo del proyecto y desmotivando así a las empresas a adquirir una solución de administración centralizada de credenciales privilegiadas.

1.2 Objetivo General

Implementar una solución de Bóveda de Seguridad que permita administrar de forma centralizada y segura las credenciales privilegiadas de las plataformas tecnológicas de la empresa de telecomunicaciones.

1.3 Descripción del Problema

El activo más importante de toda empresa es la información y mucho más cuando se trata de una empresa de Telecomunicaciones debido que existen leyes regulatorias que exigen mantener niveles altos de protección sobre la información sensible de los clientes a los cuales presta un servicio. [2]

Debido al sin número de sistemas, servidores, equipos de comunicación y plataformas en general que ayudan a mantener la red de servicios activos y disponibles 24x7, existe una gran cantidad de credenciales privilegiadas que deben ser recordadas por los administradores y que en su mayoría las almacenan de forma insegura en archivos de texto planos, hojas de cálculo e incluso en documentos físicos que son compartidos por un grupo de administradores.

La administración de estas credenciales carece también de esquemas adecuados de registro de uso y niveles de acceso basados en perfiles y privilegios tanto así que no se lleva un control sobre el uso de éstas tanto por personal interno como por personal externo que brinda soporte.

En caso de presentarse un incidente de seguridad en alguno de los sistemas, servidores y/o equipos de comunicación, la empresa de Telecomunicaciones no podrá identificar los responsables de manera oportuna puesto que deberá recurrir a revisiones de logs de forma manual y en solo en cuyos casos donde existan dichos registros, pudiendo así no identificar de manera oportuna los responsables, afectando la disponibilidad de los servicios que brindan y verse sujeto a sanciones por parte de los entes reguladores.

1.4 Solución Propuesta

Dado que en su mayoría las empresas de telecomunicaciones son un foco de atracción para los hackers, éstas deben contar con sistemas de seguridad que permitan identificar de manera ágil y oportuna incidentes de seguridad que se presenten debido al mal uso o uso no autorizado de las credenciales privilegiadas.

La compañía consciente del riesgo actual en cuanto a las limitaciones y consciente de la necesidad de una solución de administración de claves privilegiadas tomó la decisión de implementar una solución que le permita almacenar y administrar de forma centralizada, segura y eficiente dichas credenciales, la cual es conocida como Bóveda de Seguridad de Credenciales Privilegiadas.

Esta solución permite registrar toda actividad que se realice con una credencial privilegiada de un sistema, servidor y/o equipos de comunicación con el fin de conocer si fue utilizada por personal interno o externo en determinado tiempo, garantiza el acceso a las credenciales mediante perfiles y roles, registra en video las sesiones establecidas pudiendo acudir a las grabaciones en caso de presentarse algún incidente, permite integrar un sin número de activos informáticos ya sean sistemas, servidores, sistemas operativos, equipos de comunicación, equipos de seguridad, bases de datos e incluso aplicativos desarrollados in-house.

Esta solución inyecta de forma automática las credenciales evitando así que los administradores conozcan la clave lo cual evita que se filtre hacia personal no autorizado y por último puede entregar una clave temporal que luego de finalizado su uso o tiempo de expiración, la cambia automáticamente en el activo. Permite también cambiar de forma automática y programada las credenciales ahorrando tiempo considerable a los administradores.

Estos esquemas de seguridad ayudarán a la empresa de Telecomunicaciones a identificar de forma ágil los incidentes de seguridad que se presenten con las credenciales.

Con la implementación de una solución de Bóveda de Seguridad de Credenciales se obtienen los siguientes beneficios:

- Repositorio central de contraseñas.
- Restablecimiento automático de contraseñas.
- Flujos de aprobación y alertas en tiempo real de acceso a credenciales.
- Integración con servicios de directorio tales como Active Directory y LDAP. Descubrimiento automático de sistemas, usuarios y cuentas.
- Controles de acceso basados en roles.
- Control de visibilidad de usuarios hacia los recursos que solo le son permitido ver por las políticas implementadas.
- Trazabilidad, auditorias de acceso e informes de permisos. Arquitectura de alta disponibilidad.
- Automatización del uso de contraseñas entre aplicaciones y cuentas de procesos.

Figura 1. 1 Módulos Principales de la Bóveda de Seguridad.

CAPÍTULO 2

METODOLOGÍA DE DESARROLLO DE LA SOLUCIÓN

2.1 Planteamiento

Para el correcto desenvolvimiento del proyecto y considerando todos los elementos necesarios se definieron las siguientes 6 Fases:

- Fase 1: Presentación del proyecto al Directorio Ejecutivo de la empresa.
- Fase 2: Levantamiento de información.
- Fase 3: Definición de activos y credenciales privilegiadas.
- Fase 4: Definición de perfiles de acceso.
- Fase 5: Esquemas de contingencia.
- Fase 6: Definición de políticas y reglamentos internos.

2.1.1 Fase 1: Presentación del proyecto al Directorio Ejecutivo de la empresa

En esta fase del proyecto se busca presentar al Directorio Ejecutivo de la empresa las necesidades actuales por las cuales se debe incluir en la infraestructura una solución de Bóveda de Seguridad y exponer los beneficios que traerá a la empresa y los riesgos que se corren. En esta reunión se definen los responsables de cada área/departamento como apoyo al proyecto y el cronograma de trabajo para las siguientes reuniones de avances del proyecto.

2.1.2 Fase 2: Levantamiento de información

En esta fase del proyecto se busca reconocer todas y cada una de las plataformas, sistemas, servidores, servicios web, y cualquier otro servicio que de manera directa o indirecta soportan la operativa de la empresa y de los servicios que ofrecen al cliente. Esto con el fin de identificar cada uno de los activos tecnológicos donde puedan existir una o más de una credencial privilegiada y poder armar un inventario detallado de cada uno, lo cual ayudó a dimensionar el alcance del proyecto en cuanto a licenciamiento e infraestructura de la solución de Bóveda de Seguridad escogida. También se busca reconocer cada una de las áreas/departamentos que tienen acceso sobre estos activos con el fin de definir las necesidades que tienen de acceso y poder identificar

en el camino privilegios excesivos o accesos innecesarios por parte de personal no autorizado.

2.1.3 Fase 3: Definición de activos y credenciales privilegiadas

En esta fase del proyecto se eligen a los activos más importantes que soportan la operativa de la empresa y que en caso de verse afectado por algún incidente de seguridad pondrían en riesgo los servicios críticos y/o información de los clientes. También se busca identificar cada una de las credenciales privilegiadas con acceso a estos activos las cuales serán ingresadas a la Bóveda de Seguridad para su administración. El costo de licenciamiento del proyecto dependerá de la eficacia del trabajo de identificación realizado en esta fase con el apoyo de todas las áreas/departamento que participan en el proyecto.

2.1.4 Fase 4: Definición de perfiles de acceso

En esta fase del proyecto se definen los perfiles de accesos basados en las tareas administrativas que se realizarían cada uno de los administradores sobre los activos identificados. Esto con el fin de poder generar una matriz de acceso basado en cargos vs perfiles vs roles.

2.1.5 Fase 5: Esquemas de contingencia

En esta fase del proyecto se definen los esquemas de contingencia que tendrá la solución de Bóveda de Seguridad puesto que esta administraría las credenciales privilegiadas de cada uno de los activos integrados y en caso de indisponibilidad de la misma, se podría ver afectada la administración de cada uno de estos activos tecnológicos.

2.1.6 Fase 6: Definición de políticas y procedimientos internos

En esta fase del proyecto se definen cada uno de los procedimientos que conlleva la inclusión de una plataforma de Bóveda de Seguridad puesto que la integración de nuevos activos y de credenciales requiere de nuevos procedimientos a diferencia de los llevados actualmente. Se deberán definir procedimientos para inclusión, bloqueo o eliminación de nuevos activos y/o credenciales privilegiadas. Se deberán definir los responsables de llevar a cabo cada una de estas tareas y procedimientos de seguridad que se deberán tomar para evitar incidentes de seguridad. Y en caso de que se materialice alguna amenaza, los procedimientos de contingencia que se deberán ejecutar para velar que la operativa de la empresa no se vea afectada.

2.2 Desafíos del Proyecto

- Saber comunicar de manera entendible y precisa al Directorio Ejecutivo las necesidades de esta tecnología y obtener el apoyo de los mismos con recursos económicos para el proyecto.

- Poca colaboración de las áreas/departamentos de la empresa ya sea por desconocimiento, indisponibilidad o desacuerdos.

- Identificación limitada de plataformas y credenciales privilegiadas debido a la poca documentación que se lleva sobre los activos tecnológicos de la empresa.

- Desacuerdos sobre responsabilidades a adquirir por las áreas/departamentos.

- Definir claramente lo que está permitido como uso personal dentro de los activos tecnológicos y lo que no.

- Definición no precisa de los activos y credenciales debido al criterio de las áreas responsables de los mismos, lo cual afecta los costos de implementación y licenciamiento de la solución.

- Incompatibilidad de plataformas con la solución de Bóveda de Seguridad.

- Definición de políticas y procedimientos debido al modo de trabajo individual de cada área.

2.3 Evaluación de soluciones de Bóveda de Seguridad

La fase de evaluación comenzó con la identificación de los fabricantes más representativos del mercado y las diferentes soluciones que estos poseían de acuerdo a las evaluaciones realizadas por la empresa consultora y de investigación de TI, Gartner. [6] Influyó en gran parte de la selección de las soluciones el hecho de que estos fabricantes tengan representantes locales en el país:

Figura 2. 1 Gartner - Lista de fabricantes representativos y características principales (Año 2014).

En la siguiente tabla se observa el listado de las soluciones de Bóveda de Seguridad evaluadas:

Tabla 1 Soluciones de Bóveda de Seguridad evaluadas.

Fabricante	Producto	Resumen de las características del producto
ManageEngine Powering IT ahead		Password Manager Pro es una bóveda de seguridad para el almacenamiento y gestión de información sensible compartida como contraseñas, documentos e identidades digitales de las empresas. Los beneficios de la implementación de Password Manager Pro incluyen: • Despliegue de una bóveda segura, centralizada para almacenamiento de contraseñas y acceso. • Mejora de la productividad de TI muchas veces

	Password Manager Pro	mediante la automatización de los cambios de contraseña con frecuencia requeridas en los sistemas críticos. • Proporciona controles de seguridad a través de flujos de trabajo de aprobación y alertas en tiempo real sobre la contraseña de acceso. • Cumple con normativas de seguridad como SOX, HIPAA y PCI. Está compuesta de tres módulos que ayudan a que el servicio sea seguro y eficiente: • PMP: aplicativo de bóveda. • Video Recording: grabador de sesiones. • Auto Logon Helper scripts: uso de aplicativos de escritorio para el logeo automático de sesiones. [7]
IBM	IBM Security Privileged Identity Manager	IBM® Security Privileged Identity Manager permite que las organizaciones gestionen, automaticen y realicen un seguimiento del uso de identidades con privilegio compartidas. La solución proporciona las características siguientes: • Administración centralizada, acceso seguro y almacenamiento de credenciales compartidas. • Control de acceso para credenciales compartidas. • Gestión del ciclo de vida de contraseñas de credencial compartida. • Inicio de sesión único con extracción e incorporación automatizada de las credenciales compartidas. • Auditoría del uso de credenciales compartidas • Grabación de sesión y reproducción. • Integración con la cartera de Identity and Access Management Governance más amplia. • Gestión de identidades de aplicaciones. [8]
ca technologies	**CA Shared Account Management**	Esta solución ofrece un enfoque unificado para administrar las identidades de usuarios durante todo el ciclo de vida, y para brindarles acceso oportuno y apropiado a aplicaciones y datos. La solución de aprovisionamiento de usuarios y autoservicio del usuario de CA ofrece la capacidad de automatizar la integración, modificación y desvinculación de usuarios para permitir solicitudes de autoservicio y automatizar los procesos proactivos de cumplimiento de identidad, desde la empresa hasta la nube. Entre las funcionalidades de esta solución se encuentran: • Aprovisionamiento y des aprovisionamiento de usuarios.

		• Flujo de trabajo de aprobación personalizable. • Autoservicio de usuarios. • App móvil. • Soporte amplio para apps on-premise y servicios en la nube. [9]
	**Total Privilege Access Management**	La solución de Privileged Appliance and Modules (TPAM) permite manejar esquemas de seguridad de acuerdo a las necesidades que mejor se acomoden a una empresa. Permite registrar toda actividad que se realice con una credencial privilegiada de un sistema, servidor y/o equipos de comunicación con el fin de conocer si fue utilizada por personal interno o externo en determinado tiempo, garantiza el acceso a las credenciales mediante perfiles y roles, registra en video las sesiones establecidas pudiendo acudir a las grabaciones en caso de presentarse algún incidente, permite integrar un sin número de activos informáticos ya sean sistemas, servidores, sistemas operativos, equipos de comunicación, equipos de seguridad, bases de datos e incluso aplicativos desarrollados in-house. Consta de 3 módulos: • Privileged Password Manager (PPM) - Permite el almacenamiento seguro y control de cambio de contraseñas privilegiadas. • Privileged Session Manager (PSM) - Ofrece Control, auditoría y grabación de las sesiones de los usuarios de alto riesgo, incluyendo los administradores y proveedores remotos. • Privileged Command Manager (PCM) - Le permite controlar de forma granular el acceso de los usuarios a programas específicos, tareas y comandos que tienen permitido ejecutar. [10]

2.4 Hitos del Proyecto

Con el fin de llevar un control y dar un seguimiento constante de los avances del proyecto se procedió a dividirlo en 7 hitos:

1. Definición y Alcance
2. Requerimientos Técnicos
3. Requerimientos Generales

4. Evaluación de las soluciones de Bóveda de Seguridad
5. Implementación de la solución de Bóveda de Seguridad
6. Traspaso de Conocimiento
7. Puesta en Producción de la solución

2.4.1 Hito 1: Definición y Alcance

Como alcance del proyecto se requiere una solución que disponga de un sistema de almacenamiento seguro de cuentas privilegiadas (root, admin, SYS, sa, administrator y otras) a los sistemas y plataformas de la empresa que cumpla con los estándares:

- SOX
- PCI-DSS.

En base al levantamiento de información realizado en la Fase 2 del proyecto se requiere que la solución de Bóveda cubra las siguientes necesidades:

- 100 personas (administradores de los sistemas administrados)
- 1500 cuentas de usuario (al menos).
- 200 servidores/plataformas (Servidores, Bases de Datos, equipos de comunicación, equipos de seguridad, aplicaciones).
- Integración con al menos 70 activos tecnológicos/plataformas.

- Implementar/configurar 15 perfiles (roles) en la bóveda de seguridad.
- 13 reportes personalizados.

2.4.2 Hito 2: Requerimientos Técnicos

Los requerimientos técnicos para cada proveedor que participe se segmentaron en función de cada una de las necesidades identificadas:

Requerimientos en base a **Aseguramiento**:

- La solución debe tener capacidad de almacenar las contraseñas en un repositorio seguro y cifrado (bóveda de contraseñas). Indique los mecanismos de protección de que dispone la solución.
- Los cambios de contraseña deben ser realizados automáticamente en la bóveda de contraseñas una vez que se realiza el proceso de check-out.
- En caso de que la solución almacene las contraseñas en una base de datos, de preferencia deberá usarse Oracle 11g.

Requerimientos en base a **Control de Acceso e Integración con Servicios de Directorio (Active Directory / LDAP / TACACs)**:

- Tener la capacidad para autenticar a los usuarios contra el Active Directory / LDAP / TACACs.

- Tener capacidad para gestionar la autorización (perfil de acceso), ligados a al Active Directory / LDAP / TACACs.
- Disponer de su propio esquema de autenticación/autorización (a más de la integración con AD, LDAP o TACACs)

Requerimientos en base a **Control de Acceso**:

- La solución permite el ingreso automático a los sistemas gestionados directamente desde su interface de usuario sin tener que copiar y pegar las contraseñas.
- La solución debe permitir/denegar conexiones así como acceso a cuentas privilegiadas basado en criterios tales como: dirección de IP, usuario de dominio, usuario expirado, usuario bloqueado.
- La solución debe permitir configurar los siguientes controles de inicio de sesión:
    - Bloqueo por intentos fallidos de conexión (número de intentos parametrizable)
    - Control de acceso por día y hora
    - Control de acceso por calendario
    - Control de expiración de contraseñas
    - Configuración de ‘grace logins’ – se puede configurar la cantidad de veces que un usuario será notificado que debe cambiar su contraseña antes que expire.

Requerimientos en base a **Esquemas y Políticas de autorización**:

- La solución debe tener la capacidad de establecer Políticas de Autorización de usuario basado en día y hora.
- La solución debe permitir asignar accesos temporales (personal de desarrollo) o permanentes (administradores).
- Check-In/Check-Out: "Reinicios automáticos de Contraseñas
  - La solución permite reiniciar las contraseñas asociadas a las plataformas integradas desde la interface web bajo demanda o automáticamente a través de tareas programadas."
  - La contraseña se restablece automáticamente una vez finalizado el tiempo para el cual fue solicitada.
  - Si no se actualiza una contraseña en un sistema integrado no debe dar lugar a que la nueva contraseña sea almacenada en la bóveda de credenciales.
- El sistema debe mantener sincronizadas las credenciales (de activos tecnológicos…, almacenadas en la bóveda) con las credenciales de los activos tecnológicos. Si la bóveda envía a actualizar una credencial en un activo tecnológico y en esa transacción se presenta un problema (con la actualización/cambio de la contraseña), la bóveda debe registrar el nuevo estado (contraseña fallida). Lo anterior se puede presentar para casos de reseteo automático (propio de la bóveda) o manual (realizada por

un administrador). La solución debe poder validar que los cambios fueron realizados en el activo primero antes de almacenarla en su base de contraseñas, caso contrario deberá guardar con estado de fallido.

Requerimientos en base a **Flujos de Trabajo**:

- La solución debe contar con un workflow para solicitar/autorizar la entrega de contraseñas.
- La concesión de los accesos podrá ser limitada al tiempo requerido para la actividad.
    - Nota: Si el usuario no realiza el proceso de check-out (devolución de la credencial) y su tiempo de vigencia ha finalizado, el sistema debería enviar alertas ya sea por correo o SMS a los administradores.
- Dispone de Reglas a nivel de workflows para controlar peticiones inusuales de acceso, para garantizar que todas las solicitudes son autenticados, validados y autorizados antes de conceder el acceso
    - Nota: Se considerarán como peticiones inusuales las siguientes:
        - Usuarios que están próximos a expirar y que solicitan accesos.

    - Usuarios que no realizan procesos de check-out pasado del tiempo solicitado y solicitan acceso a otra contraseña.
- El workflow deberá advertir a los aprobadores de estos escenarios para que los considere al momento de aceptar o denegar una petición.

Requerimientos en base a **Integración con aplicaciones desarrolladas in-house**:

- La solución debe permitir que cualquier aplicación o script pueda solicitar una contraseña a la bóveda central para conectarse con otras aplicaciones o bases de datos, eliminando las contraseñas quemadas en el código.
- El código a incluir dentro de la aplicación o script no debe ser complejo.
- La solución debe disponer de APIs/WebServices para la gestión de contraseñas.
- El API debe estar disponible para cualquier programa cliente, en cualquier plataforma.
- La solución debe tener la facultad de generar contraseñas de tipo OTP (One Time Password). Describir el mecanismo que emplea para la generación de este tipo de contraseñas.

- Como medida de seguridad complementaria, la solución, comprueba la dirección IP de la aplicación cliente que realiza la llamada al momento de intentar el inicio de sesión.
- La solución debe contar con un workflow para solicitar/autorizar la entrega de contraseñas.

Requerimientos en base a **Reportes**:

- Reportes de tipo administrativo (Sobre Usuarios Bóveda):
  - Cambios de contraseñas por cuenta
  - Usuarios/grupos creados
  - Usuarios/grupos borrados
  - Usuarios suspendidos
- Reportes de tipo Operativo (Sobre Usuarios Bóveda):
  - Cuentas expiradas o inactivas
  - Fechas de Expiración de contraseñas
  - Intentos fallidos de conexión
  - Identidades, cuentas y perfiles asociados
  - Cuentas y usuarios que no han realizado el check-out
  - Cuentas y usuarios que hacen el check out más allá de x horas
  - Reporte de usuarios que no cumplen políticas de contraseñas (usuarios de Bóveda)

- Reportes de Credenciales guardadas en la Bóveda (contraseñas de administradores de activos tecnológicos)
  - Reporte de Cuentas almacenadas en la bóveda
  - Detalle de perfiles y servidores asociados
  - Reportes de Cumplimiento
- Reportes de las violaciones con respecto al uso y administración de contraseñas privilegiadas basándose en los requerimientos de PCI DSS, SOX, ISO 27000
- Formatos de reporte
  - Los reportes deben ser generados en diferentes formatos (xls, doc, pdf, csv, xml, html o txt).
  - Los reportes deben ser programables y enviados por mail.

Requerimientos en base a **Plataformas Soportadas**:

- La solución debe tener capacidad para administrar cuentas privilegiadas de los siguientes sistemas:
  - Unix AIX, HP-UX, Solaris
  - Linux Red Hat, SUSE, CentOS, Ubuntu, FreeBSD
  - Windows 2003, 2008, 2012
  - Oracle, SQL, Postgres, MySQL
  - Equipos de comunicación (Cisco, Huawei, Genband (Safari), Oracle SBC)

- Equipos de Seguridad (Checkpoint, Stonesoft, Fortinet, TippingPoint, McAfee, Websense, IronPort, ASA, Radware)

Requerimientos en base a **Ambientes Virtualizados**:

- La solución debe soportar la administración de cuentas privilegiadas de las plataformas señaladas en el ítem anterior, aun cuando estas se encuentren alojadas en los siguientes ambientes virtualizados:
  - Citrix XenServer
  - VMWare ESX
  - LINUX XEN
  - Ms Hypervisor
  - HP-UX VPARS

Requerimientos en base a **Aplicaciones de escritorio soportadas**:

- La solución debe tener compatibilidad al menos con las siguientes aplicaciones de escritorio:
- Para cada aplicación, el Proveedor debe confirmar si la contraseña se inyecta automáticamente.
  - Putty
  - WinSCP
  - Secure CRT

- mRemote
- PLSQL Developer
- TortoiseSVN
- IBM Infosphere Datastage Client
- Netezza (browser)
- IPCLI - Incognito
- IMC – Incognito
- Entre otros.

Requerimientos en base a **Autenticación Robusta**:

- Debe soportar un segundo factor de autenticación para acceder a la bóveda (El proveedor debe describir los esquemas de segundo factor que soporta la solución propuesta).

Requerimientos en base a **Alta Disponibilidad y respaldo**:

- La solución debe incluir un mecanismo de alta disponibilidad del servicio que permita su recuperación automática ante fallos eventuales (para autenticación, autorización y accounting).
- El proveedor debe implementar redundancia a través del despliegue de servidores redundantes locales.
- La solución debe soportar redundancia geográfica.

- La solución debe soportar redundancia a nivel de las instancias de bases de datos.
- La solución debe disponer de esquemas de respaldo. La solución debe conectarse a los sistemas de respaldo de la empresa.
- El proveedor debe realizar el plan de respaldo y restauración (documentar el proceso) y deberá realizar el primer respaldo de todo el sistema (sistema base. Configuraciones y datos).
- El proveedor deberá ejecutar el plan de restauración (prueba del backup obtenido)

Requerimientos en base a **Procedimiento de Contingencia**:

- El proveedor debe garantizar que los administradores tendrán acceso a los sistemas administrados aun cuando la solución deje de operar.
- Debe presentar el procedimiento de contingencia y confirmar si las políticas de seguridad en los sistemas administrados seguirán activas (ej. usando agente).
- De producirse daños en la bóveda de contraseñas o en caso de darse una pérdida de acceso a la base de datos, se deberá disponer un mecanismo para que los administradores puedan acceder a los sistemas administrados.
- Nota: no deberá permitirse la existencia de un único punto de falla.

2.4.3 Hito 3: Requerimientos Generales

Los requerimientos generales para cada proveedor que participe se segmentaron en función de cada una de las necesidades identificadas:

Requerimientos en base a **Temas Generales**:

- Confidencialidad:
  - El proveedor deberá garantizar que no tomará (ni almacenará) información confidencial/sensible de la empresa ni de nuestros clientes (por ejemplo usuarios/contraseñas, información personal u otros)
- Endurecimiento de la solución:
  - El proveedor al finalizar su implementación, deberá garantizar que la misma está libre de vulnerabilidades
  - El proveedor deberá generar un informe al inicio de la prestación del servicio:
    - Una Evaluación de Vulnerabilidades (checklist de seguridad para dar cumplimiento a los lineamientos de seguridad).
    - Realizar un Hardening del sistema (pruebas de penetración interna/externa), es decir, corregir las vulnerabilidades y tomar las medidas necesarias para garantizar que el sistema está libre de riesgos de seguridad.
    - Deberá generar reporte de las acciones tomadas.

- Nota: Se debe aplicar las buenas prácticas de la industria para endurecer el sistema, esto es, identificar las vulnerabilidades y corregirlas (en base a las buenas prácticas).

Requerimientos en base a **Arquitectura de la solución**:

- La solución debe contemplar todos los elementos tecnológicos para su implementación, entre ellos: servidores, sistemas operativos, licenciamiento, elementos de red pasivos y activos, etc.
- La solución debe brindar un almacenamiento seguro para guardar las contraseñas de los usuarios privilegiados de las aplicaciones, sistemas operativos y bases de datos gestionados.
- Garantiza alta disponibilidad a nivel de hardware/Software, al menos 4 nueves de disponibilidad:
  - 4 nueves --> 99,99% --> 53 minutos
- La plataforma debe considerar redundancia geográfica.
- En caso de requerirse hardware para la implementación de la solución deberá montarse preferiblemente es servidores tipo blade.
- Los logs de la aplicación, registros de auditoría de la actividad de los usuarios, entre otros, deberán poder almacenados en la propia solución.

- Nota: Se requiere que la data almacenada en línea deberá ser accedida por un período de hasta 6 meses.
- Todo equipo debe venir con fuente redundante DC.
- La plataforma no debe impactar el rendimiento de los sistemas o aplicaciones.
- Se debe especificar el impacto de los agentes desplegados en los sistemas a monitorear a nivel del rendimiento del servidor.
- La plataforma no debe ser intrusiva. En caso de serlo, el Proveedor deberá especificarlo.
- En caso que se necesite un agente instalado en la PC del administrador, especificar los requerimientos técnicos mínimos de la PC para un correcto funcionamiento.
- El proveedor deberá garantizar que la solución no afectará el desempeño de nuestra red/aplicaciones/servicios.
- La solución debe soportar esquemas de comunicación segura que soporten cualquiera de los algoritmos/mecanismos: AES 256bits, Triple DES, SSL, SHA-1, certificados digitales.
- Debe proveer soporte para los protocolos IPv4 e IPv6.
- La solución debe tener mecanismos de autoprotección que eviten que el sistema de control de acceso al servidor pueda ser deshabilitado localmente de forma indebida por un usuario privilegiado.

Arquitectura

El diagrama lógico de la solución de Bóveda de Seguridad implementada se lo muestra a continuación:

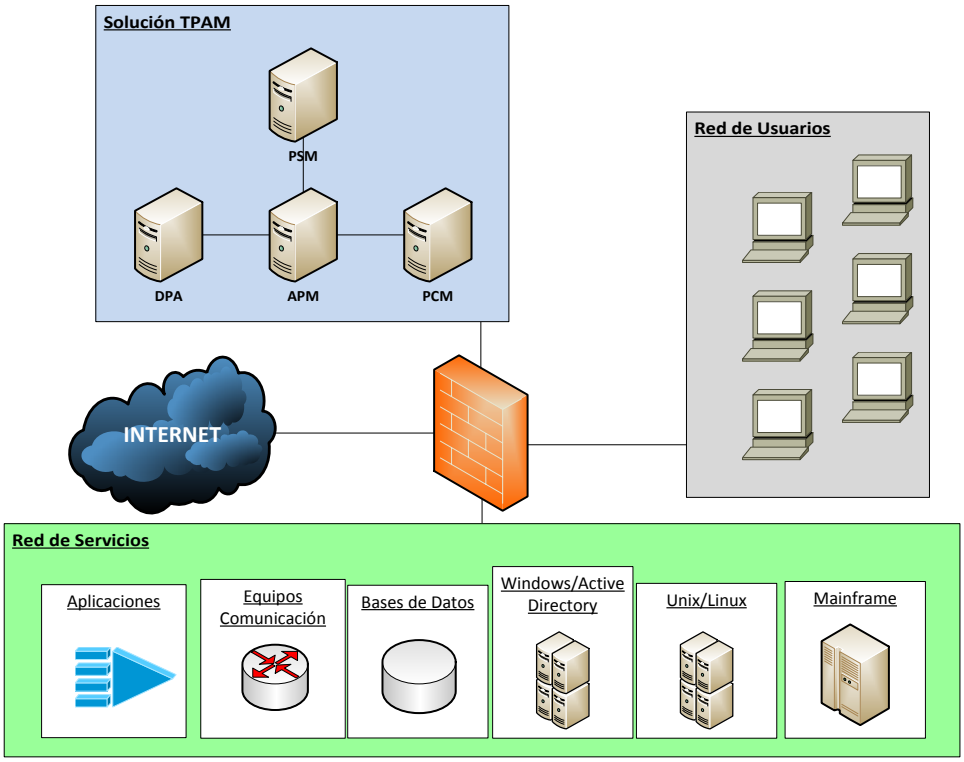


Figura 2. 2 Diagrama Lógico de la Solución de Bóveda de Seguridad.

Requerimientos en base a **Soporte y Mantenimiento**:

- El soporte y mantenimiento de la solución debe incluir:
  - Soporte telefónico:
    - nivel 1 local 7x8
    - nivel 2 remoto 7x24
  - Soporte en sitio:
    - nivel 1 local 7x24 (a las 2 horas de notificado)

- Actualizaciones de versión.
- El proveedor debe incluir en su propuesta:
  - Soporte y mantenimiento del sistema por 12 meses (a partir de la firma del Acta de Entrega Recepción definitiva de la solución).
  - Tempos mínimos de respuesta en caso fallas del producto.
  - Tiempos de reparación de hardware.
  - Instalación de actualizaciones (service packs o similares, releáse, upgrades, etc.).
  - Mecanismos de personalización o afinamiento.
  - Derechos del cliente para obtener las actualizaciones de cualquiera de los componentes del producto (componentes, conectores, herramientas de apoyo, etc.).
- El Proveedor debe incluir como parte del mantenimiento y soporte lo siguiente:
  - La solución de problemas técnicos.
  - Atención a consultas de cualquiera de los componentes de la solución.
  - Revisión periódica de buen funcionamiento de la plataforma (incluyendo componentes de la solución.
  - Reportes de solución de eventos.

- El Proveedor debe tener un Plan de Contingencia para garantizar la continuidad de los servicios del sistema (acciones a tomar antes, durante y después del evento).
- El Proveedor debe ofrecer operación asistida por un período de 30 días a partir de la fecha de cierre del proyecto.
- El proveedor garantiza como mínimo 5 años la permanencia del producto/servicio y sus componentes en el mercado (generar carta de garantía del fabricante).
- El Proveedor debe incluir los costos de mantenimiento y soporte como un rubro independiente, claramente identificable en su propuesta económica (El primer año debe estar incluido en la propuesta de manera obligatoria).
- El proveedor deberá confirmar que los costos por concepto de licencias/servicios/soporte mantenimiento de un año a otro no deben ser superiores al 5% de lo pactado en el contrato inicial.
- El proveedor deberá presentar en su propuesta económica los costos de soporte y mantenimiento a partir del segundo año y se compromete en respetar tales valores en caso de que la empresa opte por la renovación.

Requerimientos en base a **Licenciamiento**:

- El proveedor debe asegurar que en su propuesta técnica y económica ha incluido todos los costos relacionados a Licencias de software (componentes, conectores, APIs, webservices, Generadores de Reportes, Visualizadores gráficos que emplee la solución, etc.).
- El Proveedor debe describir claramente el esquema de licenciamiento, es decir debe confirmar si el esquema de licenciamiento es:
  - Por servidor.
  - Por usuario (supe usuario, usuarios administradores, usuarios aplicación/proceso).
  - Por identidad.
  - Ilimitado.
  - Un solo licenciamiento por toda la solución? o varías por componente? Si es así deberá describirlo en su propuesta.
  - Esta descripción debe ser presentada para cada componente de la solución.
- Para todos los desarrollos que realice el proveedor para la integración de su solución con las aplicaciones y plataformas de la empresa deberá entregar el código fuente de las mismas (jar, xml, prc, prg o cualquier otro procedimiento o función). Esta información deberá ser entregada a la empresa previo a la firma

del acta de entrega-recepción (este código pasa a ser propiedad intelectual de la empresa).

2.4.4 Hito 4: Evaluación de las soluciones de Bóveda de Seguridad

Con el fin de poder identificar una solución que cumpla con las necesidades requeridas por la empresa, se realizó un plan de pruebas de concepto (POC) con los proveedores que presentaron sus soluciones y para su calificación fueron considerados los siguientes aspectos claves:

- Almacenamiento Cifrado y centralizado
- Alta disponibilidad y respaldo
- Integración con el Directorio Activo
- Flujos de trabajo
- Controles de acceso
- Accounting o registro de actividades
- Arquitectura de la solución
- Plataformas soportadas
- Reportes
- Integración con plataformas no soportadas por default
- Soporte y mantenimiento
- Licenciamiento

Se llevaron a cabo pruebas de concepto para cada una de las soluciones de Bóveda de Seguridad evaluadas por un lapso de no más de 20 días por cada solución, realizándose con cuatro de ellas las pruebas con datos en tiempo real.

El resultado de las pruebas ayudó a visualizar las fortalezas y debilidades de cada solución, así como las ventajas y desventajas desde el punto de vista técnico y operativo.

El resultado de la evaluación de las pruebas de concepto se muestran a continuación:

Sección	SOLUCION 1	SOLUCION 2	SOLUCION 3	SOLUCION 4
1. Aseguramiento de las cuentas privilegiadas	0,44	0,45	0,50	0,33
2. Integración con Servicios de Directorio (Active Directory / LDAP /	2,70	2,70	2,10	2,70
3. Control de Acceso	1,99	1,99	1,99	1,99
4. Esquemas y Políticas de autorización	1,20	4,00	1,60	1,60
5. Flujo de Trabajo	3,00	3,00	3,00	3,00
6. Integración con aplicaciones desarrolladas in-house	2,40	2,13	2,60	2,13
7. Reportes	1,54	1,29	0,79	1,29
8. Plataformas Soportadas	2,00	1,33	1,47	1,33
9. Ambientes Virtualizados	1,00	1,00	0,20	1,00
10. Aplicaciones de escritorio soportadas	0,08	1,00	0,31	1,00
11. Autenticación Robusta	1,00	0,00	1,00	0,00
12. Alta Disponibilidad y respaldo	4,00	4,00	3,43	4,00
13. Procedimiento de Contingencia	1,50	1,49	2,00	1,49
14. Administración de la plataforma	0,00	1,00	1,00	1,00
15. Adicionales	0,18	0,38	0,00	0,38
SUBTOTAL 1 - Requerimientos Técnicos (30 puntos)	23,03	25,75	21,98	23,23
SUBTOTAL 2 - Servicios Profes, Calificaciones del Staff y de la Empresa, Propuesta detallada (20 puntos)	13,31	15,81	16,01	14,11
SUBTOTAL 3 - Puntos importantes revisados en conjunto con FIN, SIS, TEC y AIC (50 puntos,)	29,15	28,38	40,75	48,85
TOTAL	65,49	69,95	78,73	86,19

Figura 2. 3 Resultado de evaluación de soluciones de Bóveda de Seguridad.

2.4.5 Hito 5: Implementación de la solución de Bóveda de Seguridad

Para el desarrollo del proyecto de Bóveda de Seguridad se consideraron las siguientes actividades:

a. Elaboración del plan de trabajo del Proyecto
    - La duración del proyecto en total fue de 7 meses.
b. Reunión de lanzamiento del Proyecto
c. Adquisición de la solución de Bóveda de Seguridad:
    - Hardware
    - Software
    - Licenciamiento
    - Soportes y mantenimiento
    - Requerimientos adicionales
d. Preparación de la arquitectura de la solución:
    - Instalación del Hardware.
    - Configuración de accesos y políticas de firewall.
    - Diagramas lógicos y físicos, parametrizaciones de configuraciones.
e. Instalación y configuración:
    - El proveedor realizará la instalación inicial de la solución de Bóveda de Seguridad.
    - Incluye creación de usuarios administradores y parametrizaciones propias de la solución base.

- Configuración de la integración con el sistema de Servicio de Directorio para la identificación automática de cuentas privilegiadas.
- Pruebas de comunicación entre los equipos que componen la arquitectura de la solución.

f. Integración de activos tecnológicos y cuentas privilegiadas:

- Configuración de los accesos hacía cada uno de los activos a integrar.
- Integración de las credenciales privilegiadas a la solución.
- Creación de cuentas de usuario de la solución para los administradores de los activos.
- Configuración de workflows basados en roles y cargos previamente definidos y de las acciones que se tomarán frente a un incidente de seguridad.

g. Perfiles, accesos y procedimientos

- Configuración del flujo de trabajo definido en conjunto con las áreas responsables.
- Configuración de perfiles basados en roles y privilegios de acceso a los activos tecnológicos.
- Creación de procedimientos internos con el fin de definir esquemas de creación, bloqueo, eliminación de activos y cuentas privilegiadas dentro de la solución.

h. Pruebas

- Las pruebas incluirán cada una de las soluciones definidas en el alcance del proyecto.
- Participarán todas las áreas tecnológicas responsables de los diferentes activos.

2.4.6 Hito 6: Traspaso de Conocimiento

- El proveedor deberá incorporar en su propuesta los costos de servicios profesionales para capacitación del personal de la empresa:
- Capacitación formal (incluyendo manuales) en el uso del producto, su configuración, administración y mantenimiento.
- La capacitación será tanto para administradores y para usuarios del sistema.
- Las sesiones de capacitación no deben ser mayores a 4 horas por día.
- Proveedor debe describir su programa de entrenamiento.
- La capacitación deberá ser realizada por personal certificado y con amplia experiencia en la herramienta.
- La capacitación será impartida para 10 personas.

2.4.7 Hito 7: Puesta en Marcha de la solución

- Se declarará al sistema en operativo y en marcha una vez que todos los activos tecnológicos y cuentas privilegiadas hayan sido integradas en la solución de Bóveda de Seguridad.
- Acta de finalización de proyecto (Entrega/Recepción).

CAPÍTULO 3

RESULTADOS OBTENIDOS

Este capítulo se orienta al análisis de los resultados obtenidos luego de haber implementado la solución de Bóveda de Seguridad de Credenciales Privilegiadas.

3.1 Análisis de la solución de Bóveda de Seguridad

La Bóveda de Seguridad luego de su implementación ha proporcionado a la empresa una plataforma de seguridad que le permite controlar de manera centralizada los accesos a los activos críticos de la empresa y dando visibilidad de quienes acceden y las actividades que realizan dentro de dichos activos.

Como información adicional, la solución se licencia en base a usuarios administradores de los activos tecnológicos, los cuales pueden tener integrados cuantos servidores y credenciales privilegiadas deseen.

3.1.1 Identificación de activos integrados

Luego de haber integrado a la Bóveda de Seguridad las diferentes plataformas y activos tecnológicos se identificó que entre las Bases de Datos, Equipos de Comunicación, Sistemas de Detección de Intrusos, Firewalls, entre otros, en total se integraron más de 500 activos los cuales se distribuyen a continuación:

Tabla 2 Cantidad de activos tecnológicos integrados.

Ítem	Plataforma	Cant. Activos Integrados
1	Linux	75
2	Windows 2003	15
3	Windows 2008	55
4	Windows 2012	20
5	FreeBSD	5
6	RedHat	45
7	Solaris	30
8	Suse	10
9	CentOS	65
10	Unix AIX	11
11	Cisco	150
12	Fortinet	4
13	StoneSoft	4
14	BD Oracle	15
15	BD SQL	10
16	AD	6
17	LDAP	2
		522

3.1.2 Identificación de credenciales privilegiadas

Luego de haber integrado a la Bóveda de Seguridad las diferentes plataformas y activos tecnológicos y las credenciales privilegiadas se identificó que en total se integraron más de 1300 credenciales las cuales se distribuyen a continuación:

Tabla 3 Cantidad de credenciales privilegiadas integradas.

Ítem	Plataforma	Cant. Activos Integrados	Credenciales Integradas
1	Linux	75	150
2	Windows 2003	15	20
3	Windows 2008	55	120
4	Windows 2012	20	40
5	FreeBSD	5	10
6	RedHat	45	90
7	Solaris	30	60
8	Suse	10	20
9	CentOS	65	120
10	Unix AIX	11	20
11	Cisco	150	450
12	Fortinet	4	8
13	StoneSoft	4	8
14	BD Oracle	15	35
15	BD SQL	10	22
16	AD	6	12
17	LDAP	2	130
		522	1315

3.2 Mejoras en los procedimientos de administración de las credenciales privilegiadas

Debido a la implementación de la Bóveda de Seguridad, la empresa tenía la necesidad de definir procedimientos para la administración de estas credenciales, accesos a los activos tecnológicos y definir los responsables de gestionar estos requerimientos, por lo que en conjunto con las áreas participantes del proyecto y el departamento encargado de levantar e implementar las políticas y procedimientos de la empresa, desarrollaron una política en donde se establecían procedimientos para:

Requerimiento de acceso a **Usuarios Internos**:

- Se establecieron procedimientos para los casos en que un usuario interno de la empresa requiera acceso a una de las credenciales privilegiadas. Este deberá ingresar una solicitud de acceso y deberá ser aprobado por el jefe inmediato y por el gerente del área de acuerdo al workflow establecido. Luego de haber pasado por el proceso de aprobación el área que atiendo estos requerimientos tendrá un tiempo de atención no máximo a 24 horas laborables. Si el requerimiento es permanente, este será solo por un año y luego serán revalidados los accesos. Si el requerimiento es temporal, el acceso será habilitado solo por el tiempo requerido.

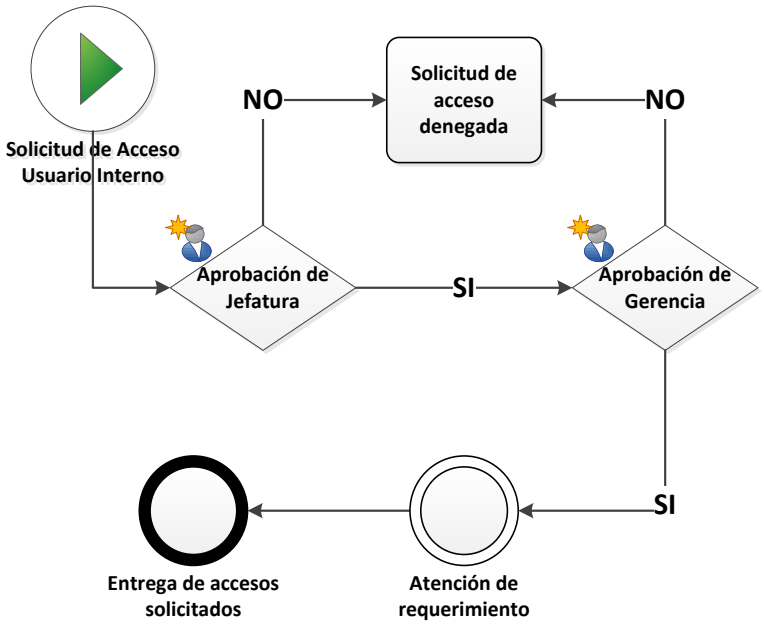


Figura 3. 1 Flujo de aprobación de acceso a Usuarios Internos.

Requerimiento de acceso a **Usuarios Externos**:

- Se establecieron procedimientos para los casos en que un usuario externo de la empresa requiera acceso a una de las credenciales privilegiadas. Este deberá enviar un correo con copia al administrador del contrato de la empresa externa, y este último deberá ingresar una solicitud de acceso y deberá ser aprobado por el jefe inmediato y por el gerente del área de acuerdo al workflow establecido. Luego de haber pasado por el proceso de aprobación el área que atiendo estos requerimientos tendrá un tiempo de atención no máximo a 24 horas laborables. No existirán requerimientos permanentes para usuarios externos. Si el requerimiento es temporal, el acceso será habilitado solo por el tiempo requerido.

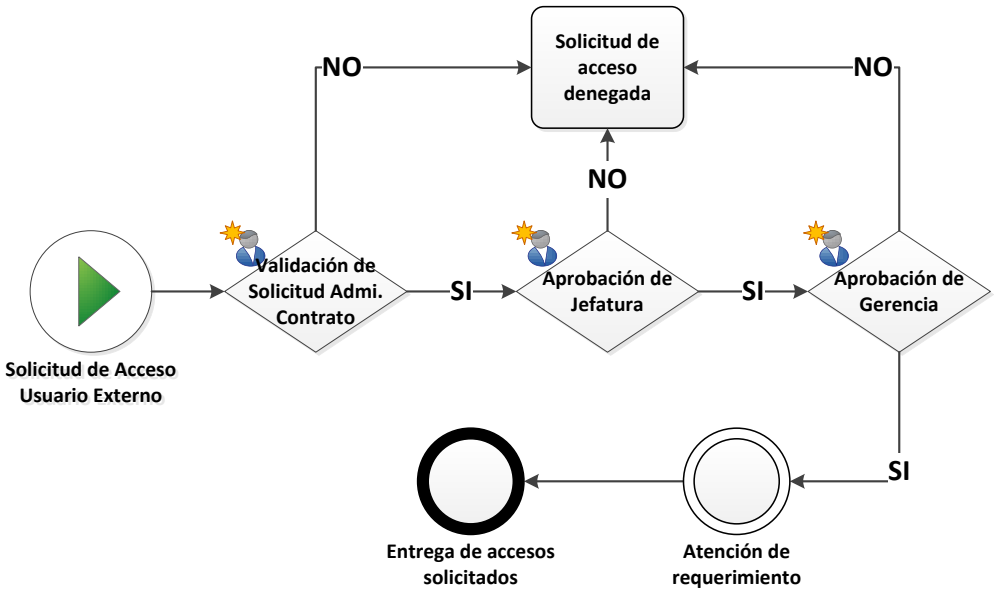


Figura 3. 2 Flujo de aprobación de acceso a Usuarios Externos.

Requerimiento de **integración o eliminación de Sistemas o Activos Tecnológicos**:

- Se establecieron procedimientos para los casos en que un área requiera que se integren de nuevos sistemas o activos tecnológicos a la Bóveda de Seguridad, definiendo pasos a seguir, aprobadores, responsabilidades y tiempos de atención para los encargados de gestionar estos requerimientos.

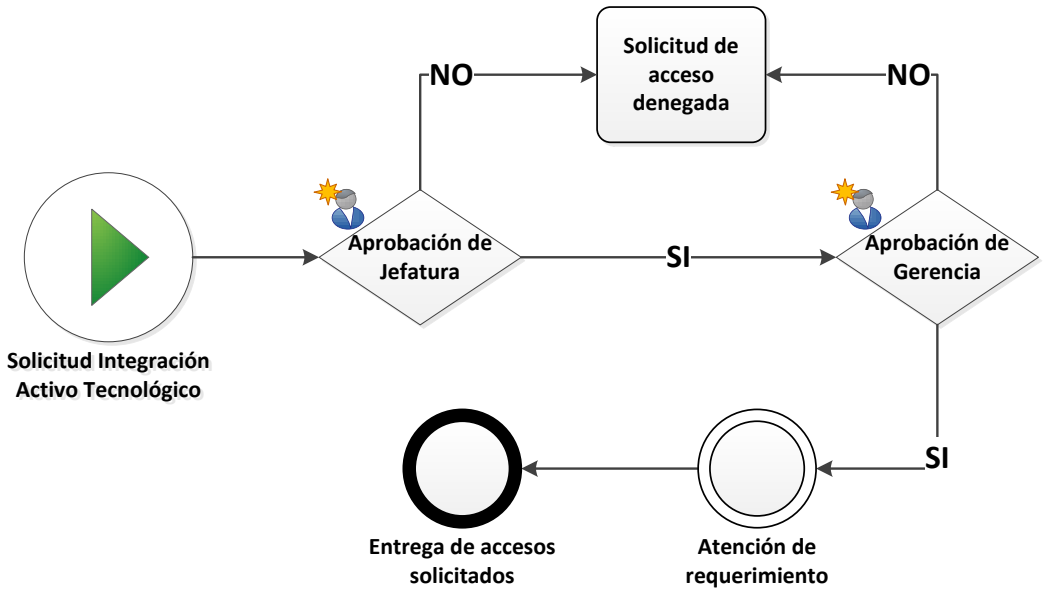


Figura 3. 3 Flujo de aprobación de integración de Activos Tecnológicos.

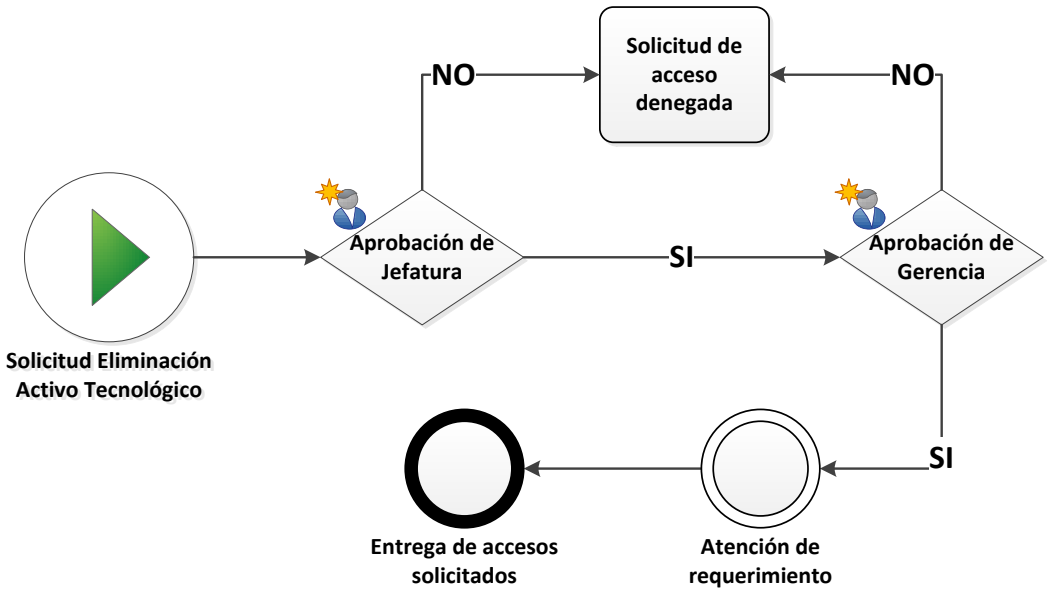


Figura 3. 4 Flujo de aprobación de eliminación de Activos.

Requerimiento de **integración o eliminación de Credenciales Privilegiadas**:

- Se establecieron procedimientos para los casos en que un área requiera que se integren de nuevos sistemas o activos tecnológicos a la Bóveda de Seguridad y por ende se integren las credenciales privilegiadas de estos activos, definiendo pasos a seguir, aprobadores, responsabilidades y tiempos de atención para los encargados de gestionar estos requerimientos.

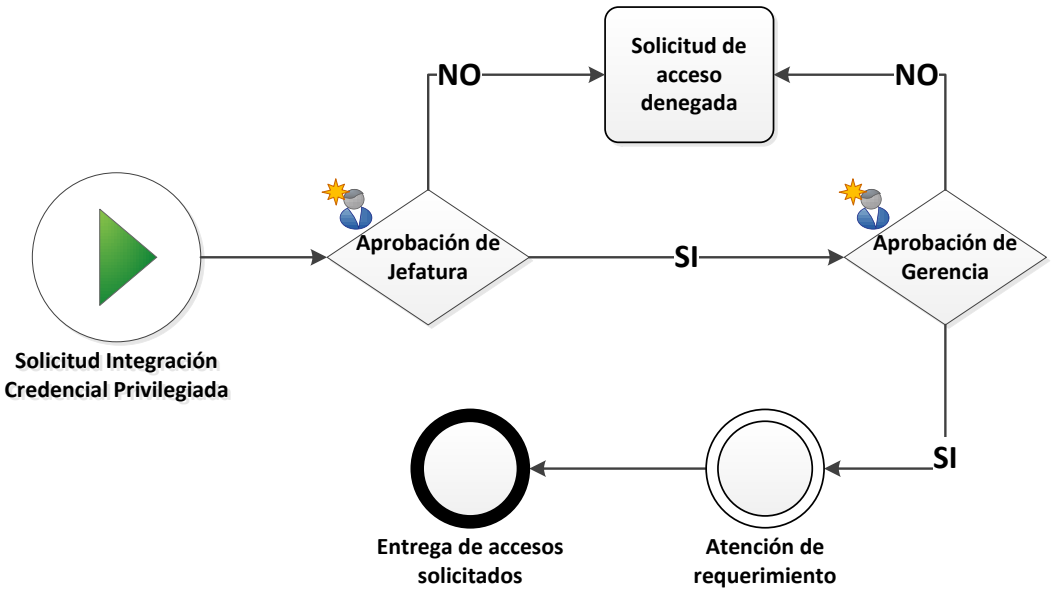


Figura 3. 5 Flujo de aprobación de integración de Credenciales Privilegiadas.

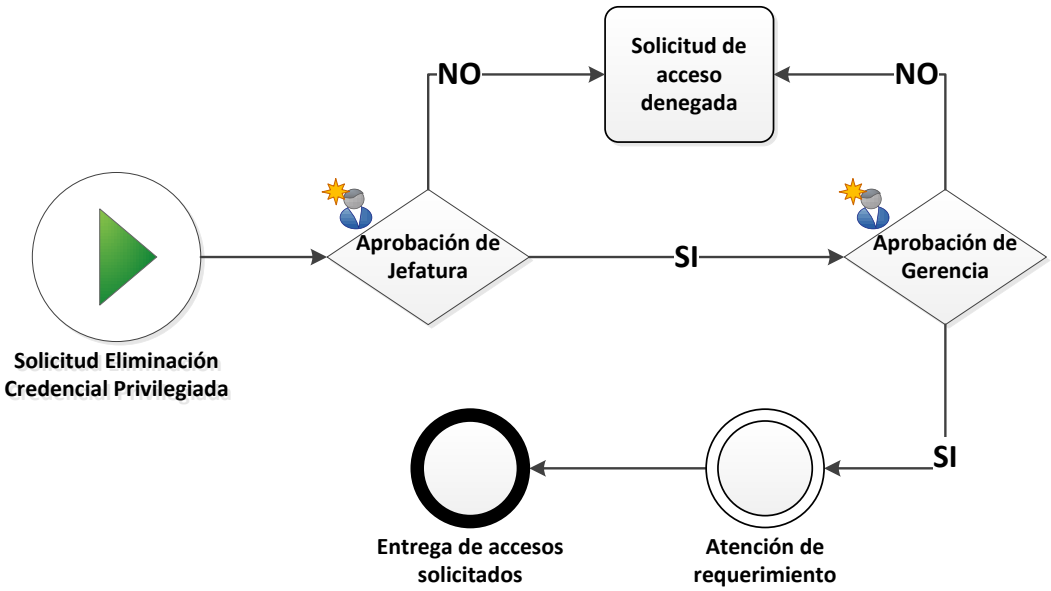


Figura 3. 6 Flujo de aprobación de integración de Credenciales Privilegiadas.

Procedimientos en caso de **fallas/contingencia**:

- Se establecieron procedimientos para casos de emergencia en donde se definió que si se presentaba algún inconveniente con la Bóveda de Seguridad, el sistema de backup deberá levantarse inmediatamente. En caso de presentarse una falla con la red donde está conectada la Bóveda de Seguridad, se dejará un usuario con privilegios de administrador que no será integrado en la Bóveda de Seguridad pero que estará bajo sobre sellado y guardado en un lugar restringido de acceso solo para el gerente del área o al recurso que el mismo disponga de dicha autorización, en caso de que se presente esta emergencia.

3.3 Análisis de problemática resuelta por la Bóveda de Seguridad

- Luego de haber puesto en producción la solución, se pudo identificar que existían administradores que dejaban las sesiones abiertas y sin bloqueo del entorno de trabajo lo cual podía ocasionar incidentes de seguridad por manipulación de personal no autorizado o externo a la empresa. Se pudo corregir a tiempo esto no solo concientizando a los administradores sino también con la ayuda de la Bóveda de Seguridad estableciendo tiempos de expiración a las sesiones, para los casos en los que la clave es inyectada automáticamente. Para los casos en los que la clave es dada al administrador, la clave caducaba luego del

tiempo solicitado, evitando así que la clave sea filtrada a otros usuarios no autorizados.

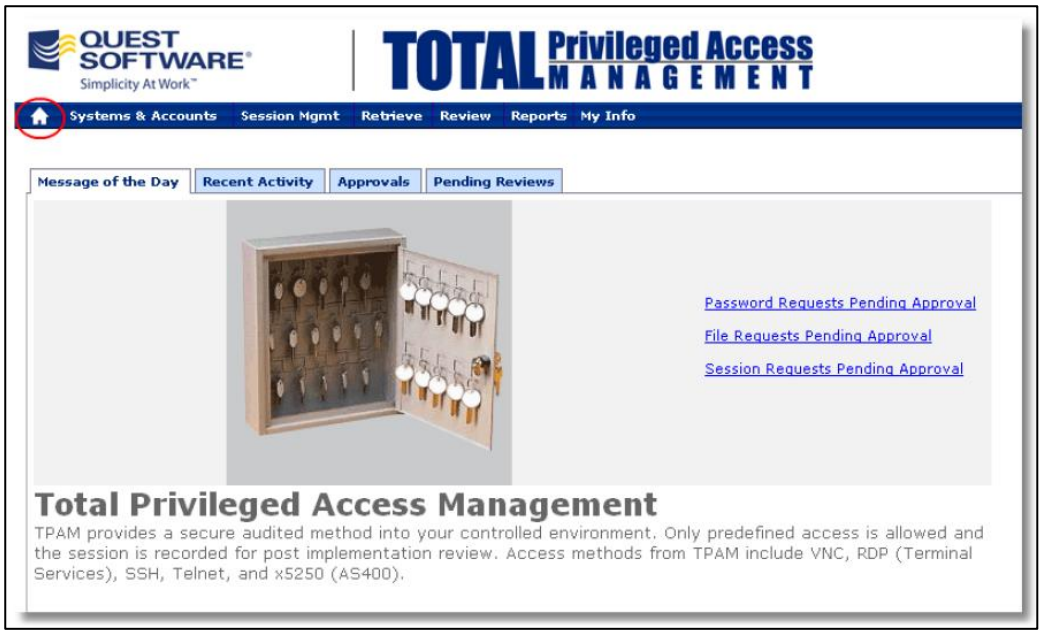


Figura 3. 7 Portal de acceso de usuarios de Bóveda de Seguridad.

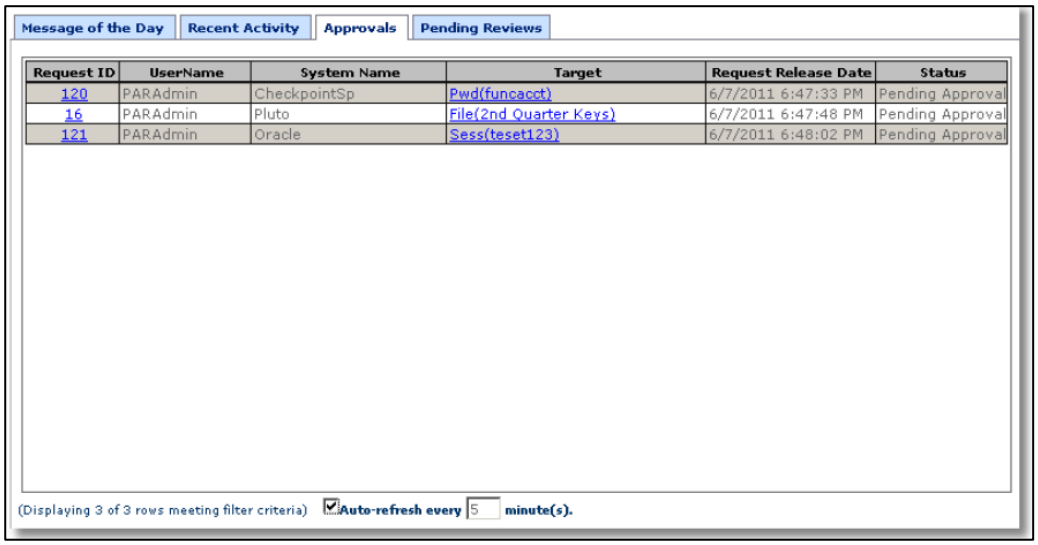


Figura 3. 8 Solicitudes de acceso pendientes de aprobación.

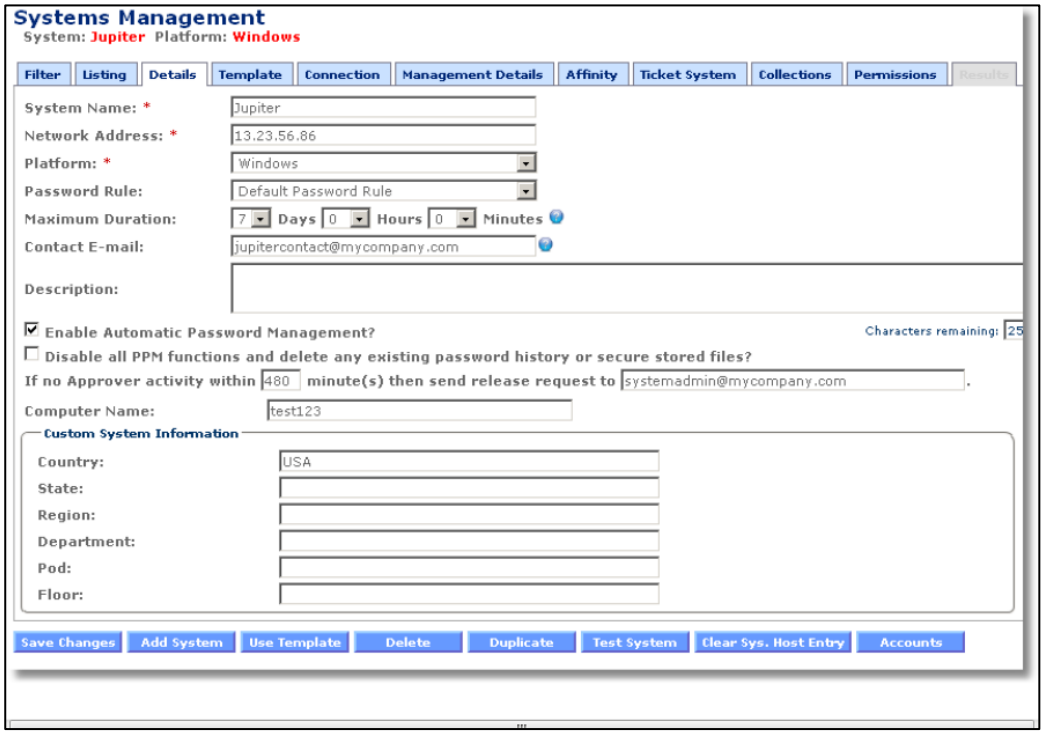


Figura 3. 9 Portal de configuración de activo/sistema y configuración de temporalidad de credencial.

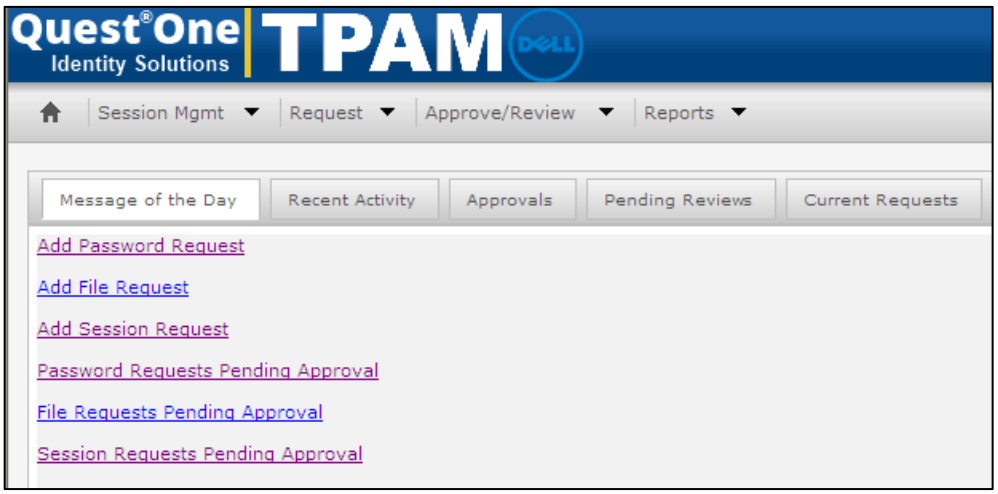


Figura 3. 10 Portal de solicitud de acceso a credenciales.

- Se identificó también que los administradores no controlaban las acciones que realizaba el personal externo, por lo cual se corría el riesgo de sufrir alguna indisponibilidad de servicio debido a una mala manipulación o configuración de los sistemas o incluso sustracción de información confidencial. Esto se pudo controlar con la ayuda de la grabación de las sesiones que establecían los usuarios.

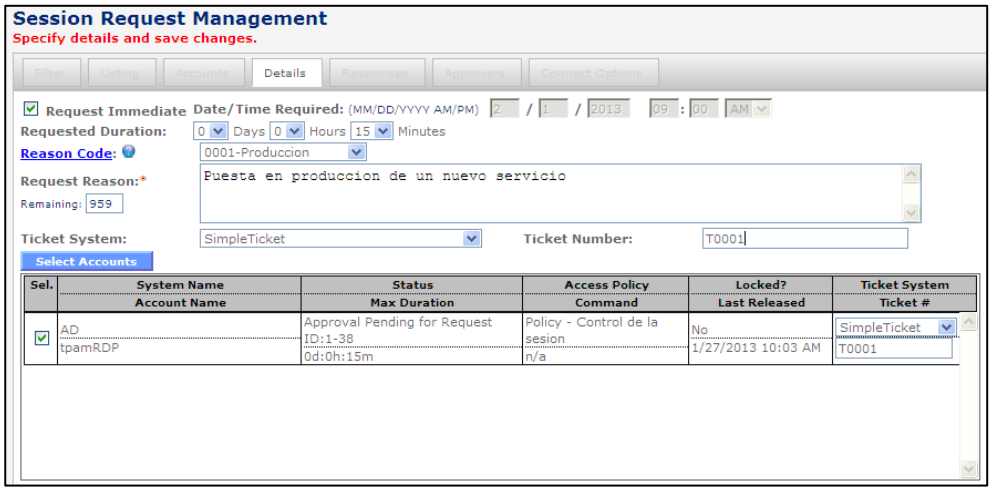


Figura 3. 11 Solicitud de acceso a un activo mediante sesión automática (inyección automática de credenciales)

- Se identificó que los administradores no podían proveer información inmediata a cerca de los accesos realizados a los activos tecnológicos en determinado momento lo cual podría ocasionar que en caso de incidentes de seguridad se dé con los responsables tardíamente. Con la ayuda de la solución de Bóveda, se pueden generar reportes de

accesos, uso de credenciales, solicitudes aprobadas y denegadas de acceso, entre otros.

Figura 3. 12 Listado de reportes

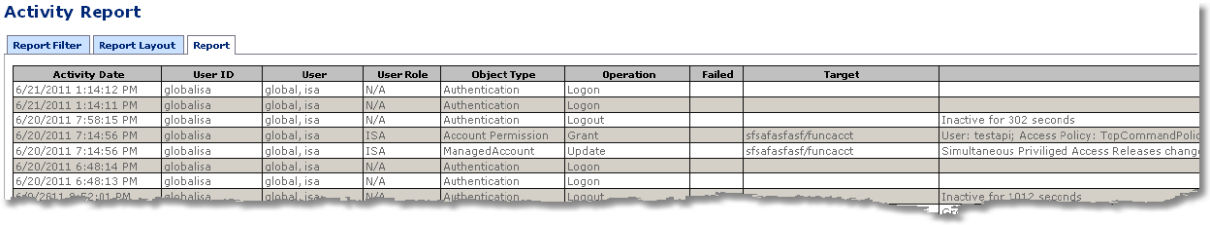


Figura 3. 13 Reporte de actividad de usuarios.

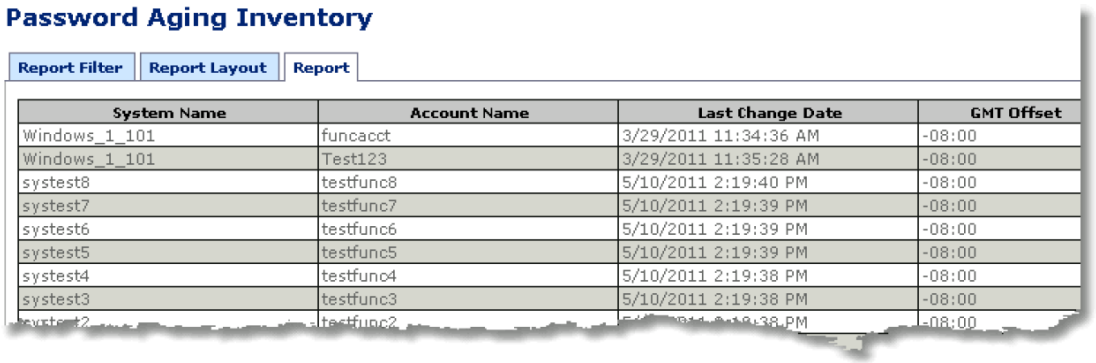


Figura 3. 14 Reporte de uso de credenciales.

- Por último se identificó que las áreas separaban un tiempo considerable para el reinicio de forma programada y manual de las credenciales privilegiadas de todos y cada uno de los activos tecnológicos, esto debido a la criticidad de las mismas. Con la Bóveda de Seguridad se logró reducir los tiempos que antes tomaban de 2 a 3 semanas en cuestión de minutos puesto que la Bóveda lo hacía de forma automática y programada de acuerdo a la necesidad del usuario.

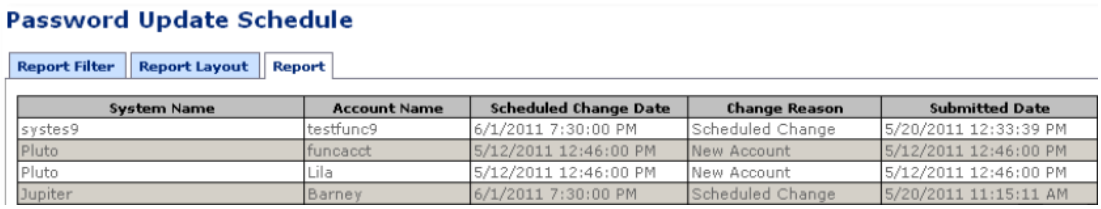


Figura 3. 15 Configuración de reinicio automático de claves.

3.4 Limitaciones de la solución

Se identificó que existían limitaciones con relación a plataformas que no son soportadas por defecto por la solución de Bóveda de Seguridad.

- Por ejemplo la infraestructura de equipos de red Huawei, debido que sus equipos son cerrados y no se obtuvo el apoyo necesario por parte del fabricante para poder hacer una integración personalizada, quedaron por fuera del proyecto.

- No se pudo integrar los equipos que estaban centralizados con un TACACs+ debido a que no existía compatibilidad de la misma pero se logró integrar los equipos Cisco de manera individual.

- Existían sistemas cuyo desarrollo era in-house los cuales no pudieron ser integrados debido que el lenguaje que utilizaba la bóveda no era compatible con el mismo. La bóveda soporta desarrollos en Java, Perl, C++ y .Net. Estos no pudieron ser identificados al inicio del levantamiento de información debido que las áreas responsables no lo consideraban como un sistema crítico al principio del desarrollo del proyecto.

- Las plataformas que no pudieron ser integrados se los lista a continuación:
    - TACACs
    - APPs desarrolladas en Postgres
    - Radware IPS
    - Checkpoint FW

CONCLUSIONES Y RECOMENDACIONES

1. El mantener un sistema centralizado que administre las Credenciales Privilegiadas ayuda a la empresa a tener un control y un registro de los accesos con el fin de evitar incidentes de seguridad con los activos críticos de la empresa y que operan los servicios que la empresa ofrece.

2. La solución de Bóveda de Seguridad ayudó a identificar escenarios tales como:

    a. Usuarios administradores desprevenidos que no mantenían esquemas de seguridad.
    b. Usuarios externos no controlados.

c. Identificación de credenciales privilegiadas y de los usuarios que administraban estas credenciales, pudiendo así revocar permisos innecesarios.
d. Disminución de tiempos en reinicios programados de claves privilegiadas.

3. A pesar de que la solución de Bóveda de Seguridad tiene el carácter preventivo y de controlar los accesos a los activos tecnológicos críticos, esto no siempre podrá ser cubierto por completo si los administradores no realizan configuraciones de seguridad y mantenimientos respectivos, puesto que de existir una brecha de seguridad sería una puerta de entrada trasera para los hackers, por lo que es necesario que se tomen medidas continuas de seguridad con el fin de disminuir las amenazas y las afectaciones a la operativa de la empresa.

Recomendaciones:

1. Definir en conjunto con todas las áreas que participarán del proyecto el alcance que abarque la solución a adquirir. Priorice entre los activos más críticos que el negocio requiere proteger; conforme los servicios que mantienen operativa la empresa.

2. Defina los siguientes elementos indispensables para el desarrollo del proyecto:
    - Responsables de cada área que participe en el proyecto. Solicitar el apoyo a las gerencias y directorio ejecutivo de la empresa.
    - Levantar un inventario de todos los activos tecnológicos clasificados por criticidad para le empresa. Esto ayudará de forma rápida poder identificar durante el proyecto los activos que deberían ser considerados en el alcance.

3. Diseñe planes de capacitación y concientización dirigido a:
    - Todos los administradores de la empresa que tengan bajo su responsabilidad un activo tecnológico.
    - Los administradores de la Bóveda de Seguridad, que serán quienes se encarguen de atender los requerimientos que soliciten las áreas.

4. En caso de no disponer, definir políticas que ayuden con el cumplimiento de los nuevos procedimientos que se establezcan en relación al uso y responsabilidades de cada usuario sobre los activos y credenciales integradas en la Bóveda de Seguridad.
5. Al implementar una solución de Bóveda de Seguridad, se deberá considerar los siguientes factores: compatibilidad con las plataformas con

las que cuenta la empresa, compatibilidad con estaciones de trabajo, portátiles y dispositivos móviles; licenciamiento, arquitectura, esquemas de contingencia, soporte técnico, niveles de servicio y capacitación completa para el personal que dará soporte a la Bóveda de Seguridad.

BIBLIOGRAFÍA

[1] El Telegrafo, «Ecuador tiene nueva Ley de Telecomunicaciones,» 17 12 2015. [En línea]. Available: http://www.telegrafo.com.ec/economia/item/ecuador-tiene-nueva-ley-de-telecomunicaciones.html. [Último acceso: 15 09 2015].

[2] Agencia de Regulación y Control de las Telecomunicaciones, «LEY DE COMERCIO ELECTRÓNICO, FIRMAS ELECTRÓNICAS Y MENSAJES DE DATOS,» 11 04 2002. [En línea]. Available: http://www.arcotel.gob.ec/wp-content/uploads/downloads/2015/04/LEY-COMERCIO-ELECTRONICO-FIRMAS-ELECTRONICAS-Y-MENSAJE-DE-DATOS.pdf. [Último acceso: 15 09 2015].

[3] El Telégrafo, «Ataques hacker a redes de Ecuador,» 10 07 2011. [En línea]. Available: http://www.telegrafo.com.ec/noticias/tecnologia/item/mas-paginas-web-oficiales-hackeadas.html. [Último acceso: 15 09 2015].

[4] Information security management systems (2006), «Análisis de riesgo informático,» 27 03 2015. [En línea]. Available: https://es.wikipedia.org/wiki/An%C3%A1lisis_de_riesgo_inform%C3%A1tico. [Último acceso: 20 09 2015].

[5] J. Ortega, «Cibermafias atacaron a 17 empresas ecuatorianas,» 24 01 2015. [En línea]. Available: http://www.elcomercio.com/actualidad/cibermafias-ciberataque-17empresas-ecuador-seguridadinformatica.html. [Último acceso: 17 09 2015].

[6] A. S. Felix Gaehtgens, «Market Guide for Privileged Account,» 17 06 2014. [En línea]. Available: http://www.meritalk.com/uploads_resources/000224_3320.pdf. [Último acceso: 17 09 2015].

[7] Manage Engine, «Password Manager Pro,» 09 2014. [En línea]. Available: https://www.manageengine.com/es/passwordmanagerpro/. [Último acceso: 18 09 2015].

[8] IBM, «IBM Security Privileged Identity Manager: Gestión Automatizada de ID,» 23 07 2013. [En línea]. Available: http://www.ibm.com/developerworks/ssa/security/library/ibmspi/. [Último acceso: 19 09 2015].

[9] CA Technologies, «CA Shared Account Manager,» 08 2014. [En línea]. Available: http://www.ca.com/us/securecenter/ca-shared-account-manager/details.aspx. [Último acceso: 19 09 2015].

[10] DELL, «Identity and Access Management,» 25 01 2014. [En línea]. Available: http://software.dell.com/solutions/privileged-management/. [Último acceso: 20 09 2015].