Universidad de Buenos Aires
Facultades de Ciencias Económicas,
Cs. Exactas y Naturales e Ingeniería

Carrera de Especialización en Seguridad Informática

Trabajo Final

Control de Usuarios Privilegiados

Autor/a:
Ing. Arsenio Antonio Aguirre Ponce
Tutor/a del Trabajo Final:
Mg. Ing. Juan Devincenzi

Año de Presentación
2015

Cohorte del Cursante
2014

Declaración Jurada de origen de los contenidos

Por medio de la presente, el autor manifiesta conocer y aceptar el Reglamento de Trabajos Finales vigente y se hace responsable que la totalidad de los contenidos del presente documento son originales y de su creación exclusiva, o bien pertenecen a terceros u otras fuentes, que han sido adecuadamente referenciados y cuya inclusión no infringe la legislación Nacional e Internacional de Propiedad Intelectual.

RESUMEN

Este trabajo final de especialización propone compartir la experiencia profesional en la implementación de una plataforma de Seguridad Informática dedicada al control de usuarios privilegiados. El tema integra aprendizajes en áreas como: seguridad en sistemas operativos, seguridad en base de datos, control de accesos, estándares de contraseña, entre otros.

El trabajo final de especialización comienza analizando la problemática actual en las organizaciones sobre el control de los usuarios privilegiados en la infraestructura tecnológica, y así mismo como solución a la problemática se describe los requerimientos importantes debe cumplir una plataforma de control de usuarios privilegiados para ser considerada en una implementación.

Posteriormente con los requerimientos de la plataforma y arquitectura actual de la organización se diseña la nueva arquitectura a nivel de hardware y software garantizando la disponibilidad de la plataforma de control de usuarios privilegiados a los administradores de la infraestructura tecnológica. Luego se describen los pasos que se siguieron para la implementación de la plataforma control de usuarios privilegiados y se detalla los resultados de la implementación. En este punto el objetivo es compartir los resultados, facilidades y problemas que se encontraron al momento de la implementación.

Por último se mencionan las conclusiones y recomendaciones derivadas de la realización de la implementación de la plataforma y de este trabajo final de especialización.

CONTENIDO

CAPÍTULO 1

INTRODUCCIÓN [1]

El tema propuesto como trabajo de especialización fue escogido debido a la experiencia que he adquirido en el campo de Seguridad Informática y a la importancia que tuvo la implementación de una plataforma de control de usuarios privilegiados en una Institución bancaria. El análisis, diseño e implementación demando definir nuevos procesos de control, generó valor agregado y dio visibilidad al área de Seguridad Informática en temas de cumplimiento de normativas internas o externas.

La plataforma implementada en la Institución fue CA Control Minder que ofrece entre sus principales funciones: gestión de contraseñas de usuarios privilegiados, segregación de funciones, asegurar ambientes físicos y virtuales, reducir costos de administración de plataformas Linux/Unix, grabar la sesión de los usuarios, auditoria y reportes de actividad de usuarios, entre otros.

1.1 DEFINICIÓN DEL PROBLEMA [2]

La falta de control y monitoreo en la gestión de los usuarios privilegiados pueden representar una amenaza para la seguridad de la información de las empresas independientemente del rubro en que se desempeñan. En la mayoría de los casos, los usuarios privilegiados son los administradores de red, administradores de sistemas operativos, administradores de base de datos o de sistemas a los que se les concede unos derechos significativamente mayores que al resto de los usuarios de TI.

Se entiende por usuarios privilegiados a: (i): Los súper usuarios creados por defecto en la instalación de los componentes de la plataforma tecnológica, (ii): Los usuarios que realizan actividades de administración en los componentes tecnológicos con los máximos privilegios que requiere su función, (iii): Todos aquellas cuentas de usuario que requieren ser asignados

a funcionarios cuyo cargo está relacionado con la administración funcional y/o tecnológica de sistemas de información, y; (ix): Los usuarios administrador y root en plataformas Windows y Linux/Unix respectivamente. El usuario sa en plataformas de Base de Datos.

Si el acceso de los usuarios privilegiados no está apropiadamente controlado puede resultar difícil o imposible auditar, esto puede representar una grave amenaza de seguridad y riesgos contra la información de las organizaciones. Ante un incidente de seguridad no se puede determinar la responsabilidad de la persona que lo generó.

En este sentido se propuso en la Institución la implementación de una plataforma de control de usuarios privilegiados con el fin de garantizar un adecuado uso de los usuarios administrador de TI con máximos privilegios en componentes de la plataforma tecnológica de la empresa.

La implementación de una plataforma para el control de usuarios privilegiados permitirá tanto al personal técnico de la operación como al personal de control/auditoría aplicar los siguientes controles:

- Permitir que solamente los usuarios privilegiados autorizados puedan acceder a los datos sensibles.
- Fortalecer las políticas de control de acceso a la infraestructura de servidores de la empresa.
- Regular y auditar de manera permanente el acceso a los servidores, dispositivos y aplicaciones considerados críticos, en las diferentes plataformas.
- Cumplir con los requisitos normativos internos, externos y organismos de Control.
- Creación y presentación de informes de manera oportuna sobre las políticas de acceso a los servidores.
- Autenticar a los usuarios en los diferentes ambientes: Windows y Linux/Unix desde una única base de datos de usuarios.

- Reducir los costos administrativos en la gestión de cuentas de usuario con acceso privilegiado.
- Reducir los riesgos o vulnerabilidades en los procesos de control de acceso.

1.2 OBJETIVOS

El trabajo de especialización plantea los siguientes objetivos:

- Compartir la experiencia profesional sobre la implementación de una plataforma de control de usuarios privilegiados en la infraestructura de tecnologías de información de una Institución.
- Detallar las problemáticas encontradas en el área de Informática / Seguridad Informática sobre la gestión de los usuarios privilegiados sin la implementación de la plataforma.
- Identificar las tareas o actividades principales para la implementación de la plataforma en la infraestructura tecnológica de una Institución.
- Diseñar una arquitectura de hardware y software que permita tener una alta disponibilidad de la plataforma y pueda gestionar las cuentas privilegiadas de los dos Data Center uno principal y otro secundario que tiene la Institución.
- Definir en base a las mejores prácticas los procesos de solicitud de usuarios privilegiados hacia el personal de Informática y Seguridad Informática de una Institución.
- Detallar las problemáticas encontradas en el área de Informática / Seguridad Informática durante la implementación de la plataforma de control de usuarios privilegiados.
- Compartir los resultados obtenidos después de la implementación de la plataforma de control de usuarios privilegiados.

1.3 ALCANCE

El trabajo final de especialización analiza la problemática sobre la gestión de los usuarios privilegiados de los diferentes componentes de la plataforma tecnológica de una Institución y comparte la experiencia profesional sobre las diferentes etapas realizadas en un proyecto de implementación de una plataforma de control de usuarios privilegiados y cubrir una problemática en el área de Seguridad Informática.

CAPÍTULO 2

DESARROLLO DEL TRABAJO

En el presente capítulo se analiza la situación actual de la Institución en la gestión de los usuarios privilegiados, se definen los requerimientos importantes que deben considerarse para la implementación de una plataforma de control de usuarios privilegiados, con la plataforma seleccionada se muestra el diseño de la arquitectura en alta disponibilidad a fin de atender los dos Data Centers que posee la Institución y se finaliza con las actividades realizadas para la implementación de la plataforma.

2.1 ANÁLISIS DE LA SITUACIÓN ACTUAL

La Institución cuenta con diferentes tipos de infraestructura a nivel de servidores como: Windows y Linux/Unix; la administración del sistema operativo de los servidores es realizada por el área de Infraestructura de TI y la administración de las bases de datos y fuentes de los aplicativos, es realizada por el área de Producción y Control. El área de Infraestructura de TI y Producción y Control necesitan usuarios privilegiados o administradores para realizar las actividades.

La Institución posee como Directorio Activo corporativo la plataforma eDirectory de Novell, lo cual dificulta la integración y gestión de los usuarios con acceso privilegiado de los servidores de plataforma Windows mediante un dominio central. Esta dificultad permite que no se puedan aplicar políticas o directivas de seguridad en los servidores Windows. Debido a la falta de un dominio central los servidores Linux/Unix se encuentran en standalone y no integrados en un dominio.

Las problemáticas o riesgos con la gestión de los usuarios privilegiados que se detectaron en la Institución son los siguientes:

- Los funcionarios de las áreas de Producción y Control e Infraestructura de TI utilizaban el usuario administrador o root para la operación de los servidores.
- La contraseña de usuario administrador o root se encontraba compartida incumpliendo la política de seguridad de la información respecto a la confidencialidad de las contraseñas.
- La contraseña de los usuarios privilegiados en algunos servidores no cumplían con la política de contraseñas.
- La gestión de las políticas de contraseña se realiza por cada servidor y no de manera centralizada generando una carga operativa alta.
- Las contraseñas de usuarios privilegiados tienden a memorizarse o escribirlas en algún lugar no seguro.
- Las contraseñas de los usuarios privilegiados se encontraban en un archivo compartido de Excel protegido.
- Las actividades realizadas con los usuarios privilegiados no se estaban auditando.
- Las actividades realizadas con los usuarios privilegiados no se estaban monitoreando para reaccionar proactivamente ante un incidente.
- Las cuentas de los usuarios privilegiados se estaban usando para la ejecución de procesos en el servidor como: respaldos, servicios, etc.
- Ante un incidente de seguridad en los servidores, ocasionado por el uso de una cuenta privilegiada no se puede responsabilizar a un funcionario debido a que las cuentas se encuentran compartidas. Responsabilidades diluidas.

- Servidores vulnerables de accesos no autorizados debido a la falta de controles en el proceso de control de acceso a los servidores con las cuentas privilegiadas.

A continuación se muestra un diagrama de la situación actual del acceso de usuarios privilegiados. En el diagrama se muestra que un usuario o administrador de TI accede directamente a los servidores. Los servidores tienen múltiples cuentas de usuarios con acceso privilegiado. Los usuarios o administradores de TI tienen que recordar el número de contraseñas igual al número de servidores que tienen acceso.

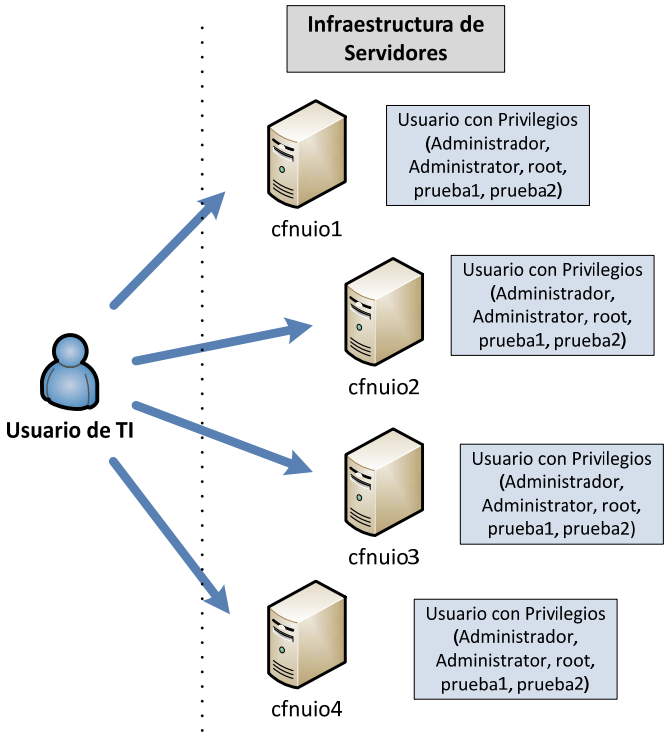


Figura 2.1 - Situación actual de un usuario de TI

2.2 DEFINICIÓN DE REQUERIMIENTOS

La plataforma de control de usuarios privilegiados independientemente del fabricante debe cumplir con diferentes requerimientos o necesidades establecidas en la Institución, estos

requerimientos deberán satisfacer y cumplir con la normativa interna y externa en temas de seguridad de la información.

A continuación se detallan los requerimientos más importantes para la implementación de la plataforma de control de usuarios privilegiados, los requerimientos son de tipo técnico y funcional de la herramienta.

No.	CARACTERÍSTICA	DESCRIPCIÓN	IMPORTANCIA DEL REQUERIMIENTO
1. CONTROL DE ACCESOS			
1.1	Soporte Multi Plataforma	La solución debe proteger los entornos de trabajo Solaris, Unix, Linux y Windows permitiendo la sincronización de políticas entre las tres plataformas a la vez.	La infraestructura cuenta con servidores de diferentes entornos.
1.2	Soporte de Entornos Virtuales	La solución debe soportar todos los entornos de servidores virtualizados siguientes: Solaris 10 Zones, Vmware ESX, Linux XEN, Oracle VM	La infraestructura cuenta con servidores virtualizados.
1.3	Ciclo de Vida de Políticas	La solución debe permitir una administración centralizada de políticas y usuarios a través de una consola web centralizada, única para todos los servidores Windows, Solaris, Unix e Linux, evitando la necesidad de ir máquina por máquina mediante el uso de herramientas locales para administrar usuarios y políticas.	La gestión de las políticas de contraseñas y usuarios privilegiados debe ser realizada de manera centralizada.
1.4	Ciclo de Vida de Políticas	La solución debe brindar capacidades de administración centralizada para	Identificar las cuentas de usuarios de los servidores para garantizar que los

		identificar y controlar las políticas aplicadas a cada servidor o conjunto de servidores.	usuarios privilegiados sean controlados.
1.5	Ciclo de Vida de Políticas	La solución debe brindar capacidades de administración centralizada para administrar, operar y revisar las políticas de acuerdo a roles predefinidos (Administrador, Operador, Auditor).	Segregación de funciones para el acceso la administración de cuentas privilegiadas.
1.6	Ciclo de Vida de Políticas (Versionamiento)	La solución debe brindar capacidades de manejar el ciclo de vida de las políticas de seguridad y tener la capacidad de versionar políticas de seguridad.	Para mantener el historial de los cambios de las políticas en caso de revisiones de auditoría.
1.7	Ciclo de Vida de Políticas (Versionamiento)	La solución debe tener la capacidad de hacer una vuelta atrás de políticas en forma individual y/o global	Para realizar proceso de roll back de políticas que hayan generado incidentes en la operación.
1.8	Soporte de cifrado	La solución debe soportar una estructura de criptografía para comunicación remota que soporte mecanismos avanzados tales como: AES, DES, 3DES, SSL, SHA-1 y certificados digitales.	La comunicación entre la plataforma y los servidores debe ser cifrada.
1.9	Arquitectura	Se requiere una descripción de arquitectura que identifique claramente las siguientes funcionalidades y características : Alta Disponibilidad Rendimiento	La plataforma debe soportar mecanismos de alta disponibilidad para soportar el acceso desde dos Datacenter.

1.10	Continuidad del control de seguridad	La solución de control de acceso debe seguir funcionando independientemente que la comunicación con el servidor central de políticas este interrumpida.	De esta manera se evita el riesgo que porque el servidor quedó aislado, un administrador pueda conectarse al servidor y acceder a información del mismo sin ningún control reforzado ni ninguna auditoría.
1.11	Autoprotección de Seguridad	La solución debe tener mecanismos de autoprotección que eviten la deshabilitación indebida del sistema de control de acceso a servidores.	Que los administradores no puedan deshabilitar el control de los usuarios privilegiados.
2. CONTROL DE CUENTAS PRIVILEGIADAS			
2.1	Control de acceso en línea	La solución debe proveer mecanismos que controlen el acceso en línea por terminal o consola a la función de subrogante (suid o sgid), controlando que los usuarios 'no root' asuman privilegios 'root'.	Cuando existe segregación de funciones en la administración de los servidores pueden existir casos que un administrador quiere usar su cuenta privilegiada para ver información no autorizada de directorios, de configuración o ejecutar comandos mediante la terminal. Con este requerimiento se garantiza que un usuario no pueda ejecutar comandos que no está autorizado o que no son de sus tareas mediante una terminal.
2.2	Control de Contraseñas de Cuentas Privilegiadas	La solución debe brindar un almacenamiento seguro para guardar	Las contraseñas que genere la plataforma deben ser guardadas de manera segura y

		las contraseñas de usuarios privilegiados para aplicaciones, sistemas operativos y bases de datos.	no puedan ser visibles por terceras personas.
2.3	Procedimiento de Emergencias para contraseñas de Cuentas Privilegiadas	La solución debe brindar facilidades de tener un procedimiento de emergencia para utilizar contraseñas de usuarios privilegiados.	En caso que falle la herramienta tener un mecanismo de emergencia para el acceso con una cuenta privilegiada.
2.4	Aprobación de Uso de Contraseñas de Cuentas Privilegiadas	La solución debe brindar un flujo de trabajo que permita solicitar y aprobar el uso de contraseñas de usuarios privilegiados.	Generación de workflow para la aprobación del uso de una cuenta privilegiada.
2.5	Cambio de Contraseñas de Cuentas Privilegiadas	La solución debe brindar mecanismos de control de cambio de contraseñas de cuentas privilegiadas basado en una frecuencia de tiempo determinada.	Periodicidad del cambio de contraseñas para cumplir con la política de seguridad.
3. ADMINISTRACIÓN DE USUARIOS Y REGLAS DE AUTORIZACIÓN			
3.1	Soporte de Modelo de Roles	La solución debe soportar el modelo de roles permitiendo definir usuarios y grupos de usuarios asociados a reglas específicas de control de acceso.	Definir segregación de funciones en la plataforma en base a usuarios y grupos.
3.2	Control de Usuario	La solución debe permitir expirar cuentas de usuario en las plataformas protegidas en una hora y fecha determinada, o suspender la cuenta por inactividad de la misma en período configurable de tiempo.	Establecer un horario de acceso a las cuentas privilegiadas por parte de los administradores.
3.3	Controles de Login	La solución debe permitir tener controles adicionales	Parámetros para cumplir con los

		sobre el login a nivel de :	estándares de la política de seguridad de la empresa.
		Bloqueo por login fallidos	
		Control de acceso por día y hora	
		Control de acceso por calendario	
		Control de expiración de contraseña	
		Configuración de ‘grace logins’ – se puede configurar la cantidad de veces que un usuario será avisado que debe cambiar su contraseña antes que expire	
		Controles de acceso por red – restringe a los usuarios a acceder desde una máquina/host/Terminal específica o terminales físicas conectadas como terminales bobas.	
3.4	Control de Sesiones	La solución debe ser capaz de limitar la cantidad de sesiones de login concurrentes de los usuarios.	Para contralar que una cuenta pueda ser accedida por una sola persona a la vez.
3.5	Control de Calidad de Contraseñas	La solución debe permitir establecer controles de calidad de contraseñas , tales como:	Parámetros para cumplir con los estándares de la política de seguridad de la empresa.
		Composición de contraseñas	
		Historia de contraseñas	
		Lista de contraseñas prohibidas	
		Envejecimiento de contraseñas	
4. AUDITORIA Y REPORTES DE CONTROL DE ACCESOS A SERVIDORES			

4.1	Registro de actividad	La solución debe ser capaz de registrar toda la actividad de control de acceso realizada por la solución. Debe permitir que el registro de la actividad del usuario en dicha sesión sea almacenada en forma de video. (Grabación de sesión). Esto debe incluir las plataformas de servidores Windows, Solaris, Unix y Linux	Guardar registros para revisión y monitoreo de usuarios privilegiados por el área de seguridad y auditoría. Grabar las sesiones de los usuarios privilegiados.
4.2	Correlación de Id original y usuario privilegiado	La solución debe tener la capacidad de registrar todas las acciones de un usuario relacionándola con la identidad original, aun cuando el usuario haya realizado un 'subrogante' a un usuario diferente, incluyendo 'root' o 'administrator'.	Permite asociar el usuario original o administrador y la cuenta privilegiada que utiliza.
4.3	Reportes del ciclo de vida de Políticas de seguridad	La solución debe brindar reportes del ciclo de vida de políticas de seguridad, tales como: Estado de la distribución de Políticas Cumplimiento de Políticas Desviaciones de las Políticas	Proceso de revisión y monitoreo de políticas de seguridad por el área de seguridad y auditoría.
4.4	Reportes de Estado de Contraseñas	La solución debe brindar reportes del estado de contraseñas, tales como: Contraseñas expiradas o inactivas Cumplimiento de políticas de	Proceso de revisión y monitoreo de políticas de seguridad por el área de seguridad y auditoría.

		contraseñas	
		Fechas de Expiración de contraseñas	
		Cambios de contraseñas por cuenta	
4.5	Reportes de permisos de acceso	La solución debe brindar reportes de permisos de acceso, tales como:	Proceso de revisión y monitoreo de usuarios por el área de seguridad y auditoría.
		Membresía de Grupos	
		Accesos por Recursos	
		Accesos por Usuario/Grupo	
4.6	Reportes de actividad de usuarios	La solución debe brindar reportes de la actividad de usuarios, tales como:	Proceso de revisión y monitoreo de usuarios por el área de seguridad y auditoría.
		Usuarios Inactivos	
		Actividad de usuarios privilegiados	
		Cumplimiento de Segregación de Funciones	
4.7	Reportes de Administración	La solución debe brindar reportes de Administración , tales como:	Proceso de revisión y monitoreo de usuarios por el área de seguridad y auditoría.
		Usuarios/grupos creados	
		Usuarios/grupos actualizados	
		Usuarios/grupos borrados	
		Usuarios suspendidos	
4.8	Reportes de Eventos de Seguridad	La solución debe poder brindar reportes de eventos de seguridad, tales como:	Proceso de revisión y monitoreo de usuarios por el área de seguridad y auditoría.
		Intentos de login exitosos / fallidos	
		Intentos de acceso a recursos exitosos / fallidos	
		Seguimiento de sesiones de usuarios privilegiados	

5. INTEGRACIÓN			
5.1	Directorio corporativo	La solución debe integrarse con directorios LDAP Novell eDirectory o Active Directory	Integración con el Directorio de Novell para el acceso a la plataforma.
5.2	Gestión de Identidad	La base de datos de usuarios y privilegios debe aprovisionar automáticamente a través del sistema actual de gestión de identidades Novell Identity Manager que dispone la CFN a través de un conector o desarrollo del mismo. Cualquier desarrollo de conector de integración debe ser provisto por el oferente.	Aprovisionamiento automático en la plataforma.

Tabla 2.1 – Definición de requerimientos de la plataforma

2.3 DISEÑO DE LA ARQUITECTURA DE LA PLATAFORMA

La plataforma de control de usuarios privilegiados debe brindar servicio a los dos Data Center uno principal y uno secundario que posee la Institución localizados geográficamente distantes.

La plataforma cuenta con 3 servidores para su funcionamiento:

- CA Access Control Enterprise Manager.- Servidor donde se instala y se realiza la configuración de la plataforma. (Necesario) (Critico)
- ObserveIT.- Servidor de base de datos y grabación de las sesiones remotas en los servidores gestionados. (Necesario) (Critico)
- CA Business Intelligence.- Servidor de reportes (Opcional) (No Critico)

- Adicional en los servidores gestionados se instala un agente de la plataforma y de ObserveIT para grabar la sesión.

El diseño de la arquitectura de la herramienta de control de accesos considera los 3 servidores indicados anteriormente en el Data Center principal. Los servidores que se encuentran en el Data Center principal y secundario serán gestionados centralizadamente desde la misma consola de administración. No existen inconvenientes en la plataforma para gestionar servidores que se encuentre física y lógicamente en otra ubicación.

Los servidores son gestionados por la plataforma mediante la instalación de un agente en el sistema operativo Windows y Linux/Unix. En este diseño los usuarios administradores ingresan al servidor de la plataforma para solicitar la contraseña del usuario privilegiado y luego acceder al servidor requerido.

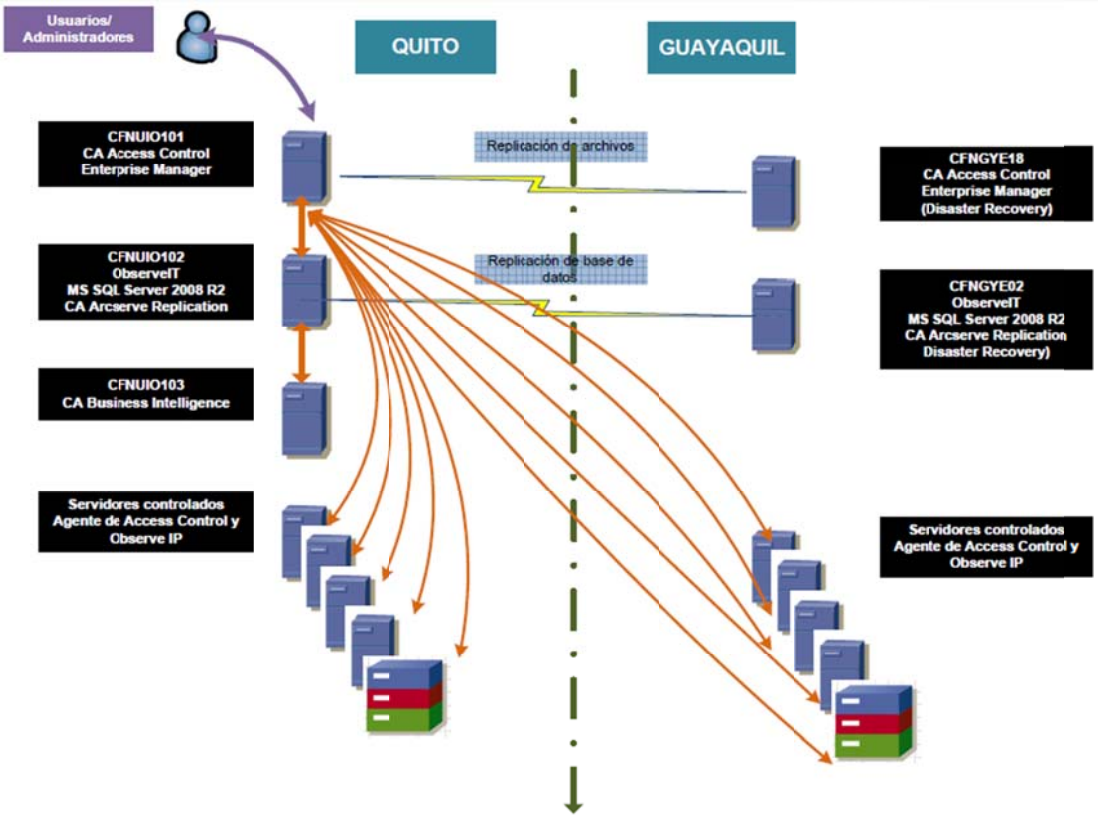


Figura 2.2 - Arquitectura de la plataforma de usuarios privilegiados

Un requerimiento importante de la implementación de la plataforma fue establecer un esquema de contingencia considerando que el Data Center principal queda fuera de servicio y las operaciones se realiza desde el Data Center secundario.

Se diseñó la contingencia en base a los dos servidores críticos de la plataforma: CA Access Control Enterprise Manager y ObserveIT. La contingencia de la plataforma funciona en base a la replicación de los archivos de configuración y la información de la base de datos del servidor principal al servidor secundario como se muestra en el diagrama. Los servidores secundarios siempre van a tener la información lista para el momento de asumir el rol de servidor principal.

Se descartó poner en contingencia el servidor CA Business Intelligence debido a que no es categorizado como crítico el servicio de reportes y la información se sigue guardando en la base de datos, solo se pierde la capa de visualización hasta recuperar el sitio principal.

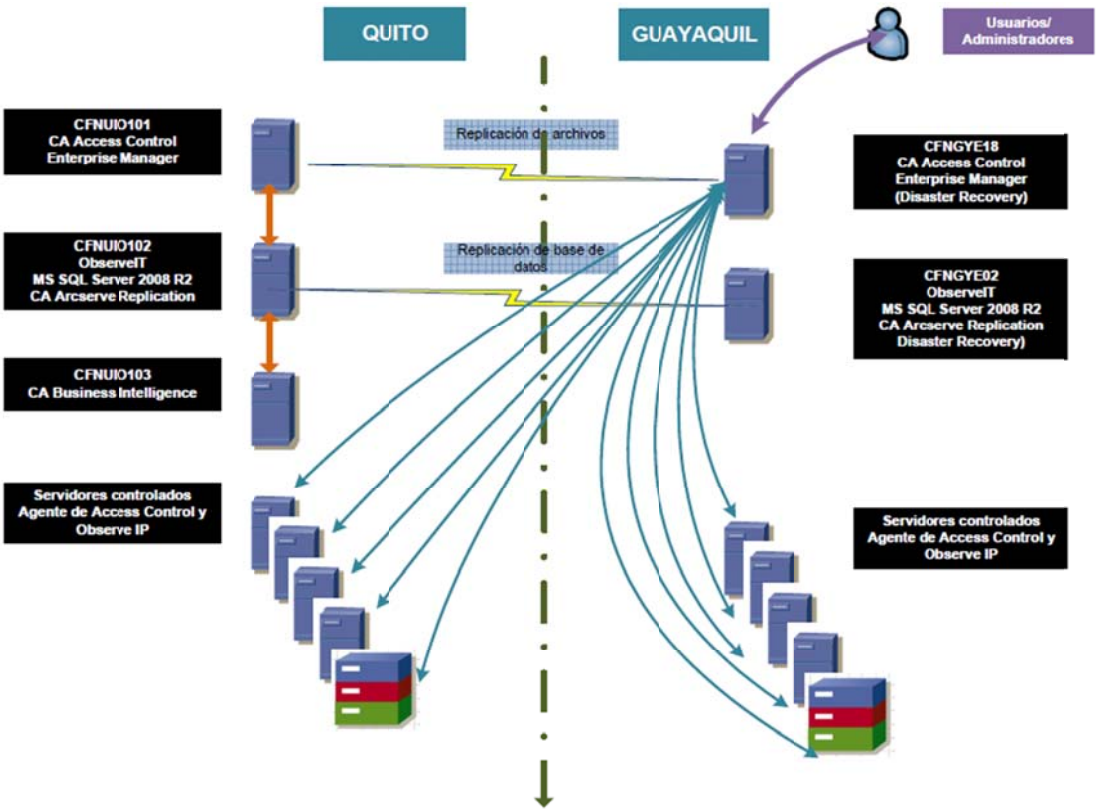


Figura 2.3 - Arquitectura en contingencia de la plataforma de usuarios privilegiados

2.4 IMPLEMENTACIÓN DE LA PLATAFORMA

La implementación de la plataforma se la realizó en diferentes etapas y conllevo a invertir mucho tiempo distribuido en las siguientes actividades:

Actividad #1

- Relevamiento de los servidores de producción sistema operativos: Windows y Linux/Unix. Se relevaron un total de 55 servidores a gestionar en la plataforma, 37 servidores del Data Center principal y 18 servidores del Data Center secundario. Adicional cada servidor deberá cumplir con 3 funcionalidades de la plataforma:
    - Control Minder - Password Vault (CMPV).- Funcionalidad para gestionar las contraseñas de los puntos finales (servidores).
    - Control Minder Session Recording (OIT).- Funcionalidad para grabar las sesiones que se realizan en los servidores con los usuarios privilegiados mediante la herramienta por parte de los administradores. Los programas compatibles para grabar las sesiones son: Remote Desktop para servidores Windows y una terminal SSH (Putty) para Windows y Linux. Existen otros programas que son compatibles pero no fueron parte de la implementación.
    - Audit and Recording (CA User Activity Reporting Module).- Funcionalidad para guardar los registros de auditoria, sesiones, accesos a cuentas privilegiadas, etc y enviarlos al servidor de Reporting de la plataforma.

  A continuación se muestra la matriz del relevamiento de los servidores.

Cantidad	Sistema Operativo dispositivo	Tipo de servidor		Requerimiento		
		Físico	Virtual	Control Minder - Password Vault (CMPV)	Control Minder Session Recording (OIT)	Audit and Recording (CA User Activity Reporting Module)
	Quito					
8	Windows Server 2008 R2 Standard x64 ES		8	X	X	X
7	Windows Server 2003 R2 Standard x64 ES	1	6	X	X	X
1	Windows Server 2003 Enterprise ES	1		X	X	X
4	Windows Server 2003 Standard ES	1	3	X	X	X
9	SuSE Linux Enterprise Server 10 x64	2	7	X	X	X
1	SuSE Linux Enterprise Server 10		1	X	X	X
1	SuSE Linux Enterprise Server 11 x64		1	X	X	X
1	Windows 2000 Server		1	X	X	X
1	Sun Solaris 10	1		X	X	X
4	Unix (por definir: Sun Solaris o IBM AIX)	4		X	X	X
	Total Quito	**10**	**27**			
	Guayaquil					
5	Windows Server 2008 R2 Standard x64 ES	1	4	X	X	X
1	Windows Server 2008 Enterprise EN		1	X	X	X
1	Windows Server 2003 R2 Standard x64 ES		1	X	X	X
2	Windows Server 2008	2		X	X	X
2	Windows Server 2003 Enterprise ES	1	1	X	X	X
2	Windows Server 2003 Standard ES		2	X	X	X
3	SuSE Linux Enterprise Server 10 x64	2	1	X	X	X
1	Windows 2000 Server		1	X	X	X
1	Sun Solaris 10	1		X	X	X
	Total Guayaquil	**7**	**11**			
	Total Servidores	**17**	**38**			
	Total a integrar	**55**				

Tabla 2.2 – Relevamiento de servidores a integrar en la plataforma

Actividad #2

- Relevamiento de los servidores de producción base de datos: SQL Server y Sybase. Se detectaron 17 servidores de base de datos.

Actividad #3

- Relevamiento de las cuentas con acceso privilegiado a nivel de sistema operativo y base de datos que se encuentran creadas en los servidores. Se detectaron alrededor de 250 usuarios creados en los servidores de los cuales 91 son usuarios con acceso privilegiado y que se deben controlar mediante la plataforma.

    - En esta actividad se identificó que en la mayoría de servidores no existen cuentas personales para los administradores del sistema operativo y de base de datos. Los funcionarios comparten las credenciales (usuario y contraseña) de acceso incumpliendo la política de seguridad de la información.

A continuación se muestra un ejemplo de la matriz del relevamiento de las cuentas privilegiadas. Las cuentas con (*) presentan inconvenientes con el cambio de clave y no pueden ser integradas a la plataforma sin realizar un análisis previo.

SISTEMA OPERATIVO					Cuentas privilegiadas
No.	**Aplicativo**	**Nombre**	**Dirección IP**	**Sistema Operativo**	
1	BI	CFNUIO8	172.16.1.2	Windows Server 2008 R2 Standard x64 ES	Administrador, tguevara, whinostroza, qlikview
2	COBIS Prod	CFNUIO33	157.100.100.119	Windows Server 2008 R2 Standard x64 ES	Administrador (*)
3	COBIS Prod	CFNUIO54	172.16.1.4	Windows Server 2003 R2 Standard x64 EN	Administrador
4	COBIS Prod	CFNUIO58	157.100.103.164	Windows Server 2008 R2 Standard x64 ES	Administrador (*)
5	COBIS Prod	CFNUIO77	172.16.1.6	Windows Server 2003 R2 Standard x64 EN	Administrador
6	DETECTART	CFNUIO48	157.100.101.235	Windows Server 2003 R2 Standard x64 ES	Administrador (*)
7	LOTUS	CFNTRAVELER	10.20.22.20	Windows Server 2008 Standard ES	Administrador
8	NOVELL	CFNUIO41	157.100.103.141	SuSE Linux Enterprise Server 10 x64, OES2	root (*)

				SP3	
9	NOVELL	CFNUIO65	157.100.103.152	SuSE Linux Enterprise Server 11 x64	root
10	NOVELL	CFNUIO81	157.100.103.22	SuSE Linux Enterprise Server 10 x64	root (*)

Tabla 2.3 – Relevamiento de usuarios en los servidores.

Actividad #4

- Identificar si las cuentas con acceso privilegiado se encuentran configuradas en un proceso, aplicación, servicio, base de datos, etc que no permita realizar una gestión adecuada de la cuenta. En esta actividad se encontraron las siguientes novedades:
    - Las cuentas con acceso privilegiado estaban hardcodeadas para levantar los servicios del sistema operativo cuando reinicia el servidor.
    - Las cuentas con acceso privilegiado estaban asociadas a los procesos de obtención de respaldos de archivos del sistema operativo de los servidores.
    - Las cuentas con acceso privilegiado estaban asociadas a los procesos de obtención de respaldos de las bases de datos de los servidores.
    - Las cuentas con acceso privilegiado estaban hardcodeadas en la programación de la aplicación core del negocio para realizar los procesos batch.
- Instalar los agentes de la plataforma en los servidores Windows y Linux/Unix que van a ser gestionados por la plataforma de usuarios privilegiados. Esta actividad se realizó sin problemas en los servidores Windows, Linux y en los servidores Unix se generó el siguiente incidente:
    - El proceso del ObserveIT consumía muchos recursos en los servidores Unix y generaba indisponibilidad en los servicios

que estaban corriendo. Este incidente se escaló al proveedor CA Technologies para la revisión y solución del mismo.

Actividad #5 [3]

- Definir los roles de acceso o matriz RACI (Responsible, Accountable, Consulted, Informed) de la plataforma de usuarios privilegiados. La matriz RACI es un modelo útil para la asignación de responsabilidades en la ejecución de tareas o actividades a un área específica de una empresa, en este caso se lo aplica a la plataforma de control de usuarios privilegiados. Algunas de las responsabilidades que fueron asignadas son las siguientes:
    - Administración de la plataforma. **Responsible/Accounted** es el área de Seguridad de la Información**.**
    - Proceso de ABM de usuarios de la plataforma. **Responsible/Accounted.** es el área de Operaciones de Seguridad de TI. **Informed** es el área de Seguridad de la Información**.**
    - Proceso de integración de nuevos puntos finales (servidores) en la plataforma. **Responsible** es el área de Operaciones de Seguridad de TI. **Accounted** es el área de Infraestructura de TI**. Consulted/Informed** es el área de Seguridad de la Información**.**
    - Configurar políticas de contraseña a un nuevo usuario privilegiado. **Responsible/Accounted.** es el área de Seguridad de la Información. **Informed** es el área de Infraestructura de TI**.**
    - Creación de nuevas políticas de contraseña a los usuarios privilegiados. **Responsible/Accounted.** es el área de Seguridad de la Información. **Consulted/Informed** es el área de Infraestructura de TI**.**

- Monitoreo de la disponibilidad de la plataforma de usuarios privilegiados. **Responsible/Accounted.** es el área de Infraestructura de TI. **Informed** es el área de Seguridad de la Información y Operaciones de Seguridad de TI.

- Revisión de log de la plataforma de usuarios privilegiados. **Responsible/Accounted.** es el área de Seguridad de la Información. **Informed** es el área de Seguridad de TI.

- Existen dos tipos de roles en la plataforma: roles de administración y roles de acceso privilegiado.

  - Los roles de administración están enfocados al uso o gestión de la plataforma en general, están relacionados a la parte operativa: ABM de usuarios, creación de políticas, configuración de logs, configuración de dispositivos finales, etc.

  - Los roles de acceso privilegiado están enfocadas a la gestión de las cuentas privilegiadas, es decir a la funcionalidad principal de la plataforma.

- A continuación se muestra un cuadro con los roles que tiene la plataforma de usuarios privilegiados y que área de la empresa es asignada. Adicional se realiza una descripción de los roles de la plataforma.

Rol a Solicitar funcionario	**Roles del sistema**		**Asignación**
	Roles de administración	**Roles de acceso privilegiado**	
Administrador del Sistema	System Manager	PUPM Target System Manager	Seguridad de la Información
	CA Access Control Policy Deployer		
	CA Access Control Policy	PUPM Policy Manager	

	Manager		
Acceso a Cuentas con Privilegio	Self Manager	Break Glass	Infraestructura de TI
		Endpoint Privileged Access Role	Producción y Control
		Privileged Account Request	Atención a Usuarios
		PUPM Approver	Responsables de Áreas de TI
		PUPM User	Operaciones de Seguridad IT
Administrador de Usuarios	CA Access Control User Manager	PUPM User Manager	Operaciones de Seguridad IT
Administrador de Infraestructura	CA Access Control Host Manager		Infraestructura de TI
	UNAB Administrator		
	CA Enterprise Log Manager Admin		
Operador Producción		Endpoint Privileged Access Role	Producción y Control
Auditoría		PUPM Audit Manager	Auditoria Interna

Tabla 2.4 – Asignación de roles de administración de la plataforma.

Descripción de roles de administración

System manager.- Un usuario con este rol de administración puede realizar, crear y gestionar todas las funciones en la plataforma de usuarios privilegiados.

CA Access Control Policy Deployer.- Este rol permite a los usuarios asignar políticas a los hosts y grupos de hosts.

CA Access Control Policy Manager.- Este rol permite a los usuarios crear, modificar ver y eliminar políticas.

Self Manager.- Un usuario con este rol puede realizar tareas administrativas sobre su propia cuenta como: cambio de la contraseña, modificar su perfil de usuario, ver los roles asignados, entre otros.

CA Access Control User Manager.- Crea y administra usuarios y grupos para el acceso a la plataforma de usuarios privilegiados. Asigna roles de acceso privilegiado a los usuarios.

CA Access Control Host Manager.- Este rol permite a los usuarios crear hosts y grupos de host, asigna host a los grupos y los modifica.

UNAB (Unix Administrator Broker) Administrator.- Un usuario con este rol puede configurar host Unix y grupos de hosts, administra políticas de autorización de acceso.

CA Log Enterprise Manager.- Responsable de ver los reportes de la plataforma de control de usuarios privilegiados.

Descripción de los roles de acceso privilegiado

Break Glass.- Un usuario con este rol puede iniciar una extracción de una cuenta privilegiada de manera emergente sin pasar por los niveles de aprobación implementados. Un usuario gana acceso inmediato a cualquier dispositivo que no tiene acceso.

Endpoint Privileged Access Role.- Un usuario con este rol puede realizar tareas sobre los usuarios privilegiados de un tipo específico de punto final (servidor).

PUPM (Privileged User Password Management) Approver.- Un usuario con este rol puede aprobar o denegar las solicitudes para utilizar un usuario privilegiado. Este rol es asignado a los Jefes para aprobar las solicitudes de acuerdo al workflow establecido.

PUPM Audit Manager.- Un usuario con este rol puede auditar la actividad de los usuarios privilegiados.

PUPM Policy Manager.- Un usuario con este rol puede gestionar los miembros de los roles y políticas, crea y elimina los roles.

PUPM Target System Manager.- Un usuario con este rol puede administrar las políticas de contraseñas y cuentas privilegiadas, y puede ejecutar el asistente para descubrir cuentas de usuarios privilegiados en los dispositivos finales (servidores).

PUPM User.- Un usuario con este rol puede realizar tomar posesión y entrega de las credenciales de un usuario privilegiado que está permitido usar.

PUPM User Manager.- Un usuario con este rol puede administrar los usuarios y grupos y políticas de contraseñas del acceso a la plataforma.

A continuación se muestra un matriz sobre las principales tareas que poseen los roles de acceso privilegiado.

Rol	Tareas	Asignación
System Manager	Cuentas con privilegios	Seguridad de la Información
	Gestión de Políticas	
	Informes	
	Página Principal	
	Sistema	
	Usuarios y Grupos	
	Vista Global	
Aprobador de PUPM (Privileged User Password Management)	Aprobar cuenta con privilegios	Infraestructura de TI Producción y Control Atención a Usuarios Seguridad de la Información Operaciones de Seguridad de IT
	Aprobar cuenta con privilegios de emergencia	
	Aprobar solicitud de cuenta con privilegios	
Endpoint Privileged Access Role	Extraer cuentas con privilegios	
	Mis cuentas	
	Mis cuentas con privilegios	
	Registrar cuenta con privilegios	
De emergencia	De emergencia	

	WF de emergencia	
Usuario PUPM	Esperando mi aprobación...	
	Extraer cuenta con privilegios	
	Mis cuentas	
	Mis cuentas con privilegios	
	Obtener contraseña de cuenta	
	Registrar cuenta con privilegio	
Gestor de auditorías de PUPM	Auditar cuentas con privilegios	Auditoría interna
	Crear recopilador de auditorías	
	Modificar recopilador de auditorias	
	Suprimir recopilador de auditorias	

Tabla 2.5 – Asignación de roles de acceso privilegiado

Actividad #6

- Definir el proceso para el uso de los usuarios con acceso privilegiado. En este punto se definió un workflow para la aprobación de las solicitudes de las cuentas con accesos privilegiado de tal manera de tener dos niveles de control y aprobación. Los niveles de control y aprobación permiten tener un conocimiento de los usuarios privilegiados que son utilizados.

- La herramienta permite asignar un rol de emergencia a los usuarios, este rol permite obtener una cuenta privilegiada sin pasar por los niveles de control y aprobación pero queda registrada en los logs la utilización de la misma. En la implementación no se asignó este rol.

  Se definieron 4 tipos de workflow de acuerdo al solicitante:

  - Cuando el solicitante es un usuario normal de un área de TI el primer punto de control y aprobación es el jefe del usuario y el segundo punto de control y aprobación es Seguridad de la Información.

  - Cuando el solicitante es un usuario tipo jefe de un área de TI el único punto de control y aprobación es Seguridad de la

Información. A continuación se muestra un diagrama de los dos primeros workflow indicados.

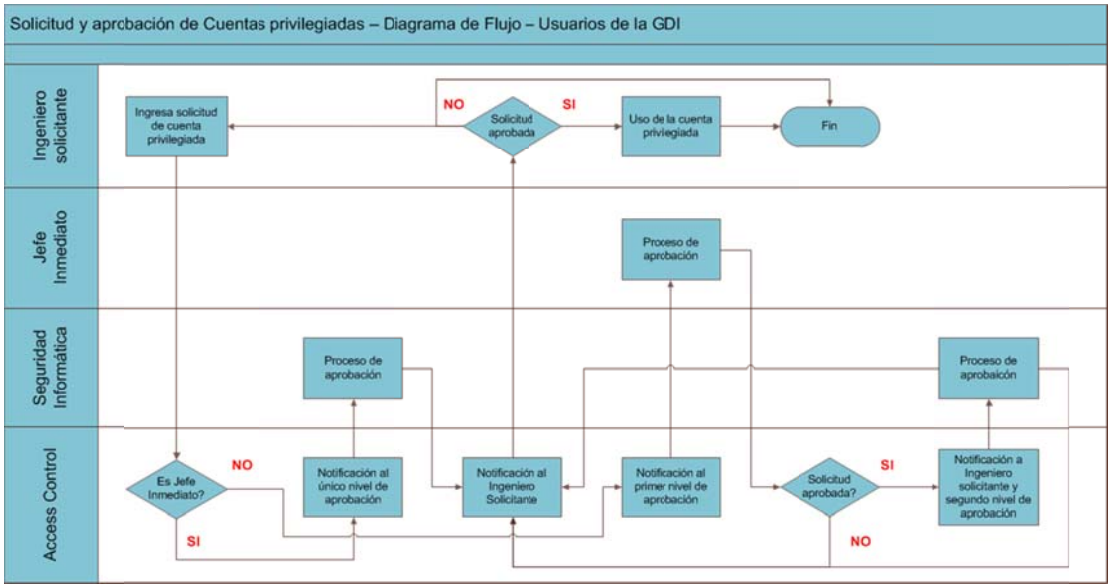


Figura 2.4 – Workflow para usuarios de Informática

- Cuando el solicitante es un usuario normal de Seguridad de la Información el primer punto de control y aprobación es el jefe de Seguridad Informática y el segundo punto de control y aprobación es el jefe de Infraestructura de TI.
- Cuando el solicitante es el jefe de Seguridad de la Información el único punto de control y aprobación es el jefe de Infraestructura de TI. A continuación se muestra un diagrama de los dos segundos workflow indicados.

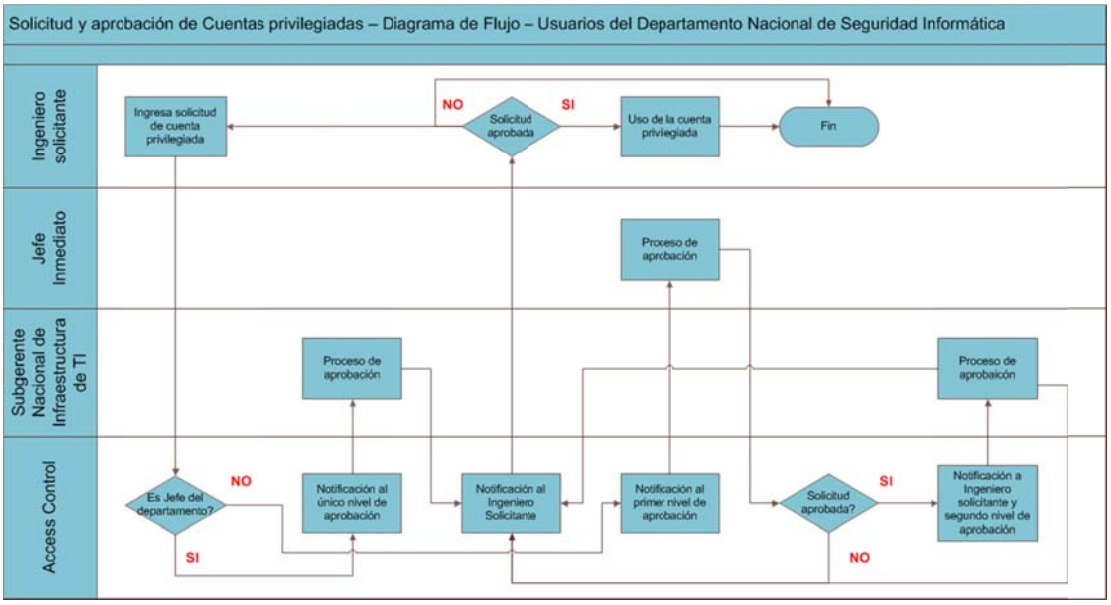


Figura 2.5 – Workflow para usuarios de Seguridad de la Información

Actividad #7

- Definir la política de contraseña que se van a aplicar a los usuarios privilegiados. En este punto se analizó la oportunidad de integrar los dispositivos de networking a la plataforma con un usuario privilegiado para la gestión de incidentes. Debido a la granularidad de la plataforma para la asignación de políticas de contraseña se crearon las siguientes políticas:
    - Política para usuarios de sistema operativos: Aplicado a ambientes Windows, Linux/Unix.
    - Política para usuarios de base de datos: Aplicado a ambientes SQL Server y Sybase.
    - Política para usuarios de networking: Aplicado a dispositivos de networking.
- Cada política tenía parámetros diferentes de acuerdo al siguiente análisis interno:

- Política para usuarios de sistema operativos: El cambio de contraseña no genera una carga operativa en los servidores y se la puede cambiar con mayor frecuencia. Mayor complejidad en la generación de la contraseña.
- Política para usuarios de base de datos: El cambio de contraseña genera una alta carga operativa en los servidores debido a configuraciones manuales establecidas y el cambio tiene baja frecuencia. Complejidad media en la generación de la contraseña.
- Política para usuarios de networking: El cambio de contraseña no genera una carga operativa en los dispositivos de networking y se la puede cambiar con mayor frecuencia. Baja complejidad en la generación de la contraseña debido a la ios de los dispositivos.

Configuración de la plataforma de control de usuarios privilegiados.

En esta sección se listan las actividades principales para configurar la plataforma y quede lista para controlar y gestionar los usuarios privilegiados. No es parte de esta sección la instalación de la plataforma.

Actividad #1 – Gestión de usuarios de la plataforma web

- Como requerimiento de la gestión de accesos de los usuarios la plataforma debería ser integrada con la herramienta de Gestión de Identidades de la empresa. En este punto se desarrollaron los conectores entre las plataformas de gestión de accesos y de identidades para aprovisionar a los usuarios mediante el usuario del Directorio Activo. Con esta integración el usuario accede a la plataforma con las credenciales (usuario y contraseña) del Directorio.
- Una vez finalizada la integración se listo los usuarios que van a acceder a la plataforma y se realizó el proceso de

aprovisionamiento mediante la plataforma de Gestión de Identidades. Como actividad adicional al aprovisionamiento del usuario se le debe asignar el superior Jerárquico que será quien apruebe el workflow de solicitud de la cuenta de un usuario privilegiado y agregar al grupo de acuerdo el área organizacional.

Actividad #2 – Gestión de roles de acceso a la plataforma web

- Como actividad adicional al aprovisionamiento de los usuarios se les debe asignar los roles para el acceso a la plataforma y los roles para la gestión de los usuarios privilegiados. Los roles son asignados de acuerdo a la matriz indicada anteriormente.

- A continuación se muestran los roles que son asignados a los usuarios. Un usuario puede tener uno o más roles. El administrador de usuarios es el encargado de verificar que no exista conflicto de funciones.

Seleccionar	* Nombre	Descripción
◉	Access Control for PUPM Privileged Access Role	Role created by discover accounts wizard
○	Access Control for PUPM Rol de acceso con privilegios	Rol creado por el asistente de detección de cuentas
○	Aprobador de SAM	
○	Emergencia	
○	Gestor de auditorías de SAM	
○	Gestor del sistema de destino de SAM	
○	Gestor de políticas de SAM	
○	Gestor de usuarios de SAM	
○	MS SQL Server Rol de acceso con privilegios	Rol creado por el asistente de detección de cuentas
○	Network Device Rol de acceso con privilegios	Rol creado por el asistente de detección de cuentas
○	SAM Account Owner	A user with this role can administer the privileged accounts that the user is the account owner
○	Solicitud de cuenta con privilegios	
○	Solicitud de cuenta con privilegios SI	
○	Sybase Server Rol de acceso con privilegios	
○	Usuario de SAM	

Figura 2.6 – Roles de administración de la plataforma.

Actividad #3 – Configuración de los workflows para aprobar el uso de una cuenta privilegiada

- El acceso a la infraestructura con una cuenta privilegiada debe ser auditada, monitoreada y autorizada. En este contexto la plataforma implementada permite establecer diferentes workflows para la aprobación del uso de una cuenta privilegiada.

- Los workflows fueron diseñadas en base al diagrama indicado anteriormente. Con la finalidad de fortalecer el control sobre un

usuario privilegiado se consideran dos aprobaciones de manera secuencial que se genera cuando un usuario final realiza una solicitud.

- Los usuarios aprobadores serán notificados mediante un correo electrónico cuando tienen una solicitud para su aprobación del acceso con cuenta privilegiada. Con esta opción los aprobadores se mantienen informados y no se generan demoras en los procesos de gestión de usuarios privilegiados.

- A continuación se muestra una captura de pantalla mostrando los diferentes niveles de aprobación que permite configurar la plataforma.

Figura 2.7 – Configuración de workflow

Actividad #4 – Implementación de las políticas de contraseña.

- La Institución cuenta con una política de contraseña para aplicar a los usuarios finales pero en este proyecto se vio la necesidad de definir una política de contraseña para usuarios privilegiados y considerar los diferentes impactos en las aplicaciones, sistema operativo, base de datos, etc.

- Después del análisis realizado se vio la necesidad de crear 3 diferentes políticas de contraseña para usuarios privilegiados:

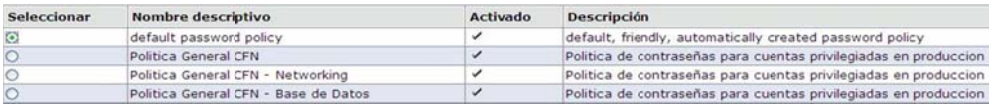
    - Política General.- Política de contraseña estándar para usuarios privilegiados del sistema operativo.

    - Política General – Networking.- Política de contraseña para usuarios privilegiados de los dispositivos de red como: switches, routers, etc.

    - Política General – Base de datos.- Política de contraseña para usuarios privilegiados de las bases de datos. Esta política se caracteriza por contemplar el cambio de contraseña de manera semestral de los usuarios privilegiados en las bases de datos y los operadores deben de correr procesos manuales donde la contraseña se encuentre hardcodeada.

- A continuación se muestran las siguientes imágenes:

    - Listado de políticas de contraseña incluida la política por defecto de la plataforma que no puede ser desactivada.



Seleccionar	Nombre descriptivo	Activado	Descripción
◉	default password policy	✔	default, friendly, automatically created password policy
○	Politica General CFN	✔	Politica de contraseñas para cuentas privilegiadas en produccion
○	Politica General CFN - Networking	✔	Politica de contraseñas para cuentas privilegiadas en produccion
○	Politica General CFN - Base de Datos	✔	Politica de contraseñas para cuentas privilegiadas en produccion

Figura 2.8 – Implementación de políticas de contraseña

    - Parámetros para establecer una política de contraseña en la plataforma.

Figura 2.9 – Parámetros de política de contraseña

Opciones adicionales para gestionar la contraseña

- La plataforma provee la funcionalidad de establecer una contraseña manual para una cuenta privilegiada. Esta opción puede ser usada por los administradores de la plataforma cuando se requiera asignar una contraseña de manera temporal. El uso de una contraseña temporal debe ser autorizada por el área de Seguridad de la Información como excepción al proceso de gestión de cuentas privilegiadas. Esta funcionalidad es importante

en especial en los proyectos donde participan administradores de diferentes áreas y necesiten conectarse con el mismo usuario para la instalación de alguna nueva herramienta en la infraestructura.

- El uso de esta opción se considera muy delicada y por eso la responsabilidad es de los administradores de la plataforma. Si alguien no autorizado ingresa una contraseña manual se pueden generar acceso mal intencionados en la infraestructura y el control sería reactivo.

- A continuación se muestra la opción para ingresar una contraseña manual donde se indica el servidor y el usuario que afecta.

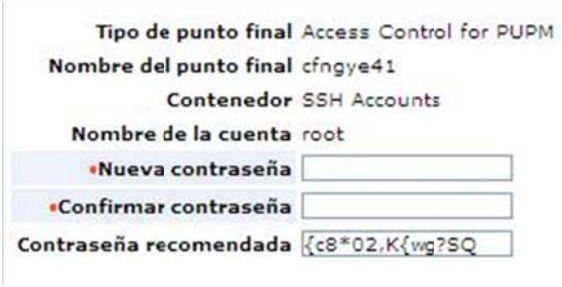


Figura 2.9 – Asignación manual de una contraseña.

- Toda actividad que se realiza con las cuentas privilegiadas es registrada y auditada en la plataforma, en caso de realizar una auditoría sobre la asignación manual de contraseña se puede revisar el historial con la fecha de asignación de la contraseña y que contraseña fue asignada.

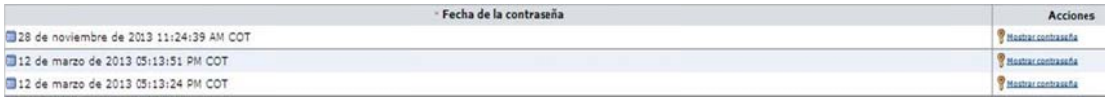


Figura 2.10 – Historial de asignación de contraseñas

Actividad #5 – Integrar servidores en la plataforma

- En esta actividad se comienzan a integrar la siguiente infraestructura a la plataforma:
    - Servidores Windows, Linux, Solaris (Sistema Operativo y Base de Datos)
    - Dispositivos de red
- El proceso de integración se realiza mediante la instalación de un agente para los servidores y la ejecución de un script para los dispositivos de red.
- En el proceso de instalación el agente solicitará la información del servidor de la plataforma que gestionara las cuentas privilegiadas. Una vez instalado el agente se debe reiniciar el servidor por lo cual se debe generar una ventana de mantenimiento para esta actividad y no afectar el horario productivo.
- Cuando el servidor ha sido reiniciado la plataforma de usuarios privilegiados va a detectar automáticamente un nuevo endpoint o dispositivo integrado.
- Este proceso debe ser realizado en todos los endpoints a gestionar los usuarios privilegiados.

Actividad #6 – Registro de cuentas privilegiadas en la plataforma

- Finalizada la actividad de integrar los dispositivos a la plataforma se debe registrar las cuentas de usuarios privilegiados, para esta actividad la plataforma ofrece un asistente para detectar cuentas privilegiadas en los diferentes servidores, simplemente realizas una búsqueda por servidor o por cuenta privilegiada y la plataforma te devuelve los resultados.
- En esta actividad se le asigna la política de contraseña que debe cumplir la cuenta privilegiada, por lo cual es importante tener en

mente el tipo de cuenta que estamos registrando para no generar incidentes.

- Todas las cuentas que han sido registradas pueden ser vistas por los usuarios finales que van a solicitarlas. Si se requiere tener más segregación sobre los usuarios y servidores a los que pueden realizar la solicitud de una cuenta privilegiada la plataforma permite manejar esa granularidad en la configuración pero no fue el alcance de la implementación. El control sobre los usuarios y servidores se realiza mediante el workflow donde los aprobadores deben estar conscientes de la responsabilidad asignada.

Actividad #7 – Configuración de herramientas de acceso a los servidores

- La plataforma brinda la funcionalidad de configurar ciertas herramientas para generar acceso a los servidores, entre las herramientas configuradas fueron: RDP o SSH, también para base de datos. Es importante conocer que estas herramientas deben estar instaladas en la maquina local desde donde el usuario quiere acceder a los servidores.

- Esta funcionalidad desde el punto de vista de seguridad es importante porque permite ejecutar un acceso remoto directo al servidor sin ingresar las credenciales, la autenticación la realiza la plataforma en un proceso donde envía las credenciales de acceso al servidor y el resultado es transparente para el usuario. El usuario con esta funcionalidad no necesita conocer, memorizar, escribir, etc, la contraseña.

Actividad #8 – Revisión registros de auditoria sobre las cuentas privilegiadas

- La plataforma genera registros sobre todas las actividades o acciones realizadas por los usuarios sobre una cuenta privilegiada como por ejemplo: cuando un usuario pide una cuenta

privilegiada, cuando se genera la contraseña para la cuenta privilegiada, cuando se devuelve la contraseña de la cuenta privilegiada, etc. Estos registros son almacenados en la plataforma y se pueden generar informes o reportes para validar el monitoreo y uso de una cuenta privilegiada

- En la siguiente imagen se muestra eventos que fueron capturados.

Figura 2.11 – Registro de eventos sobre usuarios privilegiados

- A continuación se muestra en la figura las solicitudes actuales de un usuario sobre las cuentas privilegiadas, se muestra información como: la cuenta privilegiada solicitada, el servidor donde reside el usuario, el tipo de servidor, el estado de la cuenta (Extraído.- la cuenta está siendo usada por un usuario) y las acciones que se pueden realizar con la cuenta.

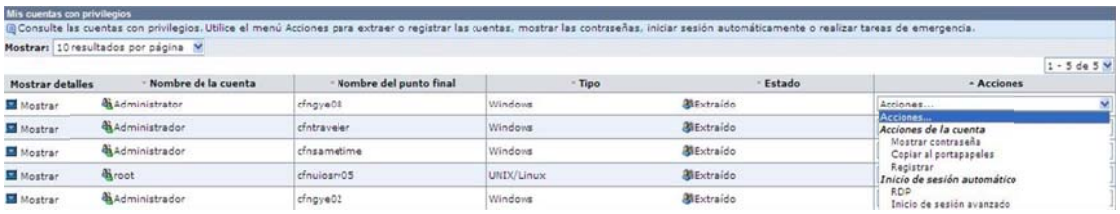


Figura 2.12 – Tablero de usuarios privilegiados solicitados.

La plataforma adicionalmente cuentas con las siguientes funcionalidades que fueron implementadas:

- Grabación de sesiones a través de plataforma CA ObserveIT.
    - Cuando los usuarios realizan accesos mediante RDP, Putty o alguna herramienta de acceso configurada en la actividad #7 automáticamente en la estación local se comienza a grabar la sesión y es almacenada en el servidor para revisión de monitoreo y auditoría.
    - Es importante considerar y generar una alerta que si se realizan accesos directamente por el Putty, RDP, etc sin pasar por la plataforma no se va a generar una grabación de la sesión.
- Reportes gerenciales sobre el uso de las cuentas privilegiadas.
    - Los reportes gerenciales son basados en los registros de las cuentas privilegiadas, estos reportes sirven para validar el uso de las cuentas privilegiadas por parte de los usuarios.
    - Los reportes permiten detectar actividades inusuales sobre la infraestructura y de ser el caso se puede comenzar una investigación en conjunto con otras plataformas de monitoreo como el SIEM (System Information and Event Management).

CAPÍTULO 3

RECOMENDACIONES

En este capítulo se describen las recomendaciones derivadas de la implementación de la plataforma de seguridad informática:

- Establecer estándares de seguridad con respecto al uso de los usuarios privilegiados y las condiciones que deben de cumplir antes de poner un servidor en ambiente productivo.

- Definir dos tipos de cuentas para los usuarios administradores: una cuenta para el acceso normal al dominio y otra cuenta con acceso privilegiados para la administración de los servidores del dominio. Esto minimiza el riesgo de comprometer la cuenta con mayores privilegios. Aplica para servidores Windows.

- Si un administrador no entrega la cuenta privilegiada a la plataforma, la plataforma no va a cambiar la contraseña y puede ser conocida por el administrador, el administrador puede generar accesos digitando la contraseña manualmente, en este punto se recomienda normar que los accesos con un usuario privilegiado sean realizados mediante la plataforma, así se garantiza que todos los accesos serán auditados y grabados para tener evidencia ante cualquier incidente.

- Implementar otros controles que en conjunto con el control de usuarios privilegiados minimizan el nivel de riesgo de accesos no autorizados a los servidores. El control de usuarios privilegiados ayuda a minimizar el riesgo pero no es la única solución. Los controles adicionales pueden ser:

    - Plataforma de gestión de eventos de seguridad para monitorear los accesos a la plataforma de TI.

    - Tener una correcta segmentación en la red interna y aislar los servidores en una red monitoreada.

    - Establecer listas de control de acceso para el acceso a la plataforma de TI.

- Involucrar al área de Auditoria en el proyecto debido a que es un área de control interno de las organizaciones.

- Seguir una metodología de proyectos estableciendo como mínimo: periodicidad de reuniones de avance, tareas programadas y responsables, riesgos asociados al proyecto, tiempos, entregables del proyecto, etc, para llevar una adecuada gestión del proyecto y cumplir con los objetivos planteados.

CAPÍTULO 4

CONCLUSIONES

En este capítulo se describen las conclusiones derivadas de la implementación de la plataforma de seguridad informática:

- Antes de implementar un proyecto de control de usuarios privilegiados se debe realizar un inventario de cuentas para establecer el alcance y los tiempos estimados de implementación.

- Es necesario revisar si los usuarios privilegiados están comprometidos en alguna tarea del sistema operativo o proceso de negocio que impida el control de la cuenta de manera inmediata.

- Se pudo implementar la herramienta en la mayoría de las cuentas privilegiadas de los servidores productivos de sistemas operativos, base de datos y dispositivos de networking.

- Concientizar a los administradores de TI sobre los riesgos que existen sin el control de las cuentas privilegiadas y el incumplimiento de controles de seguridad de la información de la Institución sobre la normativa interna y externa. Se confirma que los administradores de servidores o bases de datos se oponen a la implementación de una herramienta que controle las actividades de administración que realizan.

- Fue importante poder crear diferentes políticas de contraseña de acuerdo al tipo de cuenta privilegiada porque las cuentas de las bases de datos generaban una carga operativa muy alta si se cambiaban mensualmente las contraseñas de acuerdo a la política.

- La herramienta pudo facilitar una correcta separación de funciones entre el personal de TI y el personal de Seguridad de la Información que es un principio importante de la seguridad.

- Es importante establecer sinergia entre los diferentes equipos o áreas impactadas en el proyecto para que se tenga el éxito esperado.

BIBLIOGRAFÍA ESPECÍFICA

[1] CA Privileged Identity Manager – CA Technologies (Descripción de la solución)
http://www.ca.com/ar/~/media/Files/DataSheets/ca-priviledged-identity-manager-LAS.PDF (Consultada el 15/01/2015)

[2] CA fortalece la seguridad TI asegurando el acceso de usuarios privilegiados | Innovación | ComputerWorld
http://www.computerworld.es/innovacion/ca-fortalece-la-seguridad-ti-asegurando-el-acceso-de-usuarios-privilegiados (Consultada el 15/01/2015)

[3] Puesta en marcha > RACI [Curso ITIL Foundation > Diseño de los Servicios TI]
http://itilv3.osiatis.es/diseno_servicios_TI/modelo_RACI.php (Consultada el 30/01/2015)

[4] CA, CA Control Minder - Enterprise Administration Guide 12.7, CA Technologies, (2012), pp. 19-23.

BIBLIOGRAFÍA GENERAL

CA Privileged Identity Manager – CA Technologies (anteriormente CA ControlMinder)
http://www.ca.com/ar/securecenter/ca-privileged-identity-manager.aspx (Consultada el 07/01/2015)

Requirements for Next-Generation Privileged Identity Management | @CloudExpo Blog
http://cloudcomputing.sys-con.com/node/2834980/ (Consultada el 7/3/2015)

Monitoring Privileged User Actions for Security and Compliance
http://www.sans.org/reading-room/whitepapers/analyst/keys-kingdom monitoring-privileged-user-actions-security-compliance-34890 (Consultada el 07/01/2015)

Privileged user management - It’s time to take control | quocirca.com
http://quocirca.com/content/privileged-user-management-it%E2%80%99s-time-take-control (Consultada el 10/01/2015)