Protección y Optimización de la Plataforma ISDP: Un Enfoque en Gestión de Identidad y Acceso

DIEGO ARMANDO MAYORGA HERNANDEZ

UNIVERSIDAD SANTO TOMAS
INGENIERIA DE TELECOMUNICACIONES
BOGOTA
2024

Protección y Optimización de la Plataforma ISDP: Un Enfoque en Gestión de Identidad y Acceso

DIEGO ARMANDO MAYORGA HERNANDEZ

Protección y Optimización de la Plataforma ISDP: Un Enfoque en Gestión de Identidad y Acceso

Director: Ing. Ernesto Cadena Muños, PhD

UNIVERSIDAD SANTO TOMAS
INGENIERIA DE TELECOMUNICACIONES
BOGOTA
2024

RECTOR GENERAL
Fray. Alvaro José ARANGO RESTREPO, O.P.

VICERRECTOR ADMINISTRATIVO Y FINANCIERO GENERAL
Fray, Hender Alveiro RODRÍGUEZ PÉREZ, O.P.

VICERRECTOR ACADEMICO GENERAL
Fray, Mauricio Antonio CORTÉS GALLEGO, O.P.

SECRETARIA GENERAL
Lucero Galvis Cano

SECRETARIA DE DIVISION
Luz Patricia Rocha Caicedo

DECANO FACULTAD DE INGENIERIA DE TELECOMUNICACIONES
Ingeniero Gustavo Alonso Chica Pedraza

CONTENIDO

Pág.

LISTA DE TABLAS

Pág

LISTA DE FIGURAS

Pág

RESUMEN

Este documento aborda los desafíos de ciberseguridad relacionados con la gestión de identidad y acceso (IAM) en la plataforma ISDP (Integrated Service Delivery Platform) de Huawei, utilizada por la división de telecomunicaciones de SERDAN. Los problemas actuales incluyen el uso compartido de cuentas de usuario, la falta de mecanismos de autenticación robustos y las deficiencias en trazabilidad y control, lo que expone a la organización a riesgos significativos de seguridad y posibles sanciones legales.

El objetivo principal de este estudio es analizar los riesgos de ciberseguridad asociados al uso compartido de usuarios en la plataforma ISDP, mediante el estudio de las prácticas de uso actuales, el comportamiento de los usuarios y la identificación de vulnerabilidades. A partir de este análisis, se desarrollará un plan detallado para la adopción e implementación de tecnologías y estrategias IAM que fortalezcan la seguridad de la plataforma y protejan la integridad de los datos.

El Proyecto se estructura en varias fases clave, comenzando con una evaluación y planificación inicial, seguida de la selección y adquisición de herramientas, el diseño e integración del sistema, pruebas y validación, y finalmente, el despliegue y capacitación. Además, se incluye un sistema de monitoreo y evaluación continua para asegurar la sostenibilidad y adaptabilidad de las soluciones implementadas.

Los resultados de la implementación de estas soluciones incluyen una mejora significativa en la seguridad de los datos, aumento de la eficiencia operativa, cumplimiento normativo mejorado, y una mayor trazabilidad y control. Estas mejoras no solo mitigarán los riesgos actuales, sino que también prepararán a SERDAN para enfrentar futuros desafíos en ciberseguridad, asegurando un entorno digital seguro y eficiente.

1 INTRODUCCION

En un entorno empresarial cada vez más digitalizado y vulnerable a amenazas cibernéticas, la seguridad de la información se ha convertido en una prioridad fundamental. La gestión de identidad y acceso (IAM) es un componente crítico para proteger la integridad y confidencialidad de los datos [1], [2]. En este contexto, la plataforma ISDP (Integrated Service Delivery Platform) de Huawei, utilizada por la división de telecomunicaciones de SERDAN, enfrenta serios desafíos debido a la gestión inadecuada de identidades y accesos [20].

Actualmente, los principales problemas en la plataforma ISDP incluyen el uso compartido de cuentas de usuario, la falta de mecanismos de autenticación robustos y problemas de trazabilidad y control. Estos desafíos no solo comprometen la seguridad de la información, sino que también pueden resultar en sanciones legales y afectar la reputación de la empresa [5], [6].

Se tiene como objetivo analizar los riesgos de ciberseguridad asociados al uso compartido de usuarios en la plataforma ISDP, mediante el estudio de las prácticas de uso actuales, el comportamiento de los usuarios y la identificación de vulnerabilidades. Además, se desarrollará un plan detallado para la adopción e implementación de tecnologías y estrategias de gestión de identidad y acceso, con el fin de fortalecer la seguridad de la plataforma y proteger la integridad de los datos [1], [2].

A lo largo de este documento, se explorarán las soluciones existentes en la industria, se evaluarán sus ventajas y desafíos, y se propondrán mejoras específicas para SERDAN. La implementación de estas soluciones no solo resolverá los problemas actuales, sino que también preparará a la organización para enfrentar futuros desafíos en ciberseguridad, asegurando un entorno digital seguro y eficiente [3], [4].

2 OBJETIVOS

2.1 OBJETIVO GENERAL

Analizar los riesgos de ciberseguridad en la plataforma ISDP, propiedad de Huawei y utilizada por SERDAN, identificando vulnerabilidades y desarrollando un plan para implementar tecnologías y estrategias de gestión de identidad y acceso que fortalezcan la seguridad y protejan la integridad de los datos de SERDAN.

2.2 OBJETIVOS ESPECIFICOS

- Identificar los riesgos de ciberseguridad en la plataforma ISDP utilizada por SERDAN, analizando amenazas y vulnerabilidades que comprometen la integridad y confidencialidad de los datos, con el fin de desarrollar estrategias que protejan los activos digitales de la empresa y aseguren su continuidad operativa.
- Evaluar el impacto del uso compartido de cuentas en la autenticación, autorización y control de accesos en la plataforma ISDP de SERDAN, para determinar las debilidades en la gestión de identidad y acceso, y proponer mejoras que reduzcan el riesgo de accesos no autorizados y protejan la información sensible de la organización.
- Diseñar e implementar estrategias de gestión de identidad y acceso en la plataforma ISDP de SERDAN, con el fin de mitigar los riesgos del uso compartido de cuentas y garantizar la integridad de los datos, asegurando así el cumplimiento de las regulaciones de seguridad y protección de datos aplicables a la organización.

3 PLANTEAMIENTO DEL PROBLEMA

3.1 DEFINICION DEL PROBLEMA

La plataforma ISDP (Integrated Service Delivery Platform) de Huawei es un sistema integral destinado a optimizar la entrega de proyectos, particularmente en el ámbito de las telecomunicaciones. Este sistema facilita la gestión eficiente de proyectos a través de la planificación, ejecución y monitoreo, integrando herramientas avanzadas para la gestión de recursos, control de calidad y automatización de flujos de trabajo. Además, ofrece capacidades para la gestión centralizada de documentos, herramientas de comunicación para mejorar la colaboración y funciones de informes y análisis para proporcionar insights detallados sobre el desempeño del proyecto, lo que permite a las organizaciones mantener el cumplimiento de los estándares y optimizar tanto costos como tiempos de entrega [20].

Figura 1. logotipo ISDP [20]

El principal desafío que enfrenta la división de telecomunicaciones de SERDAN en la plataforma ISDP de Huawei es la inadecuada gestión de identidad y acceso [20]. El problema se manifiesta en dos escenarios: primero, el personal del área documental, que necesita realizar revisiones, se ve obligado a utilizar las credenciales de técnicos en campo. Este procedimiento puede dar lugar a usos incorrectos o inapropiados de estas cuentas. En segundo lugar, algunos técnicos, al carecer de un usuario propio o de los permisos necesarios, deben acceder a la plataforma utilizando las credenciales de otros. Esto puede resultar en el acceso no autorizado a información que no corresponde a sus asignaciones, comprometiendo la seguridad de los datos [18].

La ausencia de una autenticación segura más allá de la contraseña para el ingreso a la plataforma ISDP deja a la empresa vulnerable ante posibles ataques cibernéticos y accesos no autorizados por parte de terceros [17]. Además, el uso de cuentas de técnicos antiguos o inexistentes amplía el riesgo de seguridad al aumentar la complejidad en la gestión de cuentas de usuario y la inconsistencia en el acceso a la información [2]. Esta falta de trazabilidad y control sobre quién accede y modifica los datos almacenados en la plataforma podría resultar en la pérdida de integridad de los datos y posibles violaciones de la confidencialidad de la información sensible [16].

Otro riesgo asociado con este problema es la falta de cumplimiento con las regulaciones de seguridad y privacidad de datos. Al no contar con un sistema adecuado de gestión de identidad y acceso que garantice la autenticación segura y el control de acceso a la información, la empresa podría enfrentar sanciones legales y financieras significativas por incumplimiento de normativas como el Reglamento General de Protección de Datos (GDPR) [5] o regulaciones específicas del sector de las telecomunicaciones [24].

En conclusión, el problema fundamental que debe resolver SERDAN es establecer un sistema robusto de gestión de identidad y acceso dentro de la plataforma ISDP de Huawei, para asegurar la autenticación segura y la adecuada autorización de usuarios, mitigando así los riesgos de seguridad cibernética y cumpliendo con las regulaciones de protección de datos [1], [6].

En este contexto, surge una pregunta central que guiará el presente trabajo y buscará resolver el problema identificado:

¿Cómo puede SERDAN implementar un sistema de gestión de identidad y acceso (IAM) robusto y seguro en la plataforma ISDP de Huawei que permita reducir los riesgos asociados al uso compartido de cuentas y mejorar la trazabilidad y cumplimiento normativo, asegurando la integridad y confidencialidad de los datos?

3.2 JUSTIFICACION

Resolver los problemas relacionados con la gestión inadecuada de identidades y accesos en la plataforma ISDP es crucial para la seguridad operativa de SERDAN. En un entorno digital altamente vulnerable a amenazas cibernéticas, un sistema de gestión de identidad y acceso (IAM) eficiente es esencial para proteger la integridad, confidencialidad y disponibilidad de los datos, pilares de la triada de la seguridad de la información. La falta de un sistema robusto expone a la organización a riesgos importantes, como el acceso no autorizado a información crítica y la pérdida de control sobre las acciones dentro de la plataforma.

El mal manejo de identidades no solo compromete la seguridad de los datos, sino que también puede tener repercusiones legales graves y dañar la reputación de la empresa. En SERDAN, el uso compartido de cuentas y la falta de trazabilidad afectan negativamente la capacidad de auditar y monitorear los accesos a la información, aumentando el riesgo de actividades maliciosas o negligentes. Dado que la plataforma ISDP maneja información sensible vinculada a proyectos de telecomunicaciones, la criticidad de dicha información es alta, y tanto los propietarios (los responsables de los datos) como los custodios (quienes gestionan

su seguridad) deben garantizar el cumplimiento de normativas como GDPR y CCPA para evitar sanciones.

Si SERDAN no aborda este problema de manera proactiva, podría enfrentar ataques cibernéticos que comprometan la integridad, confidencialidad y disponibilidad de los datos, afectando tanto la operatividad de la empresa como la confianza de los clientes. Además, el incumplimiento de las normativas internacionales de protección de datos podría llevar a multas financieras significativas y comprometer el acceso continuo a los servicios críticos. El impacto negativo en la reputación de la empresa podría ser devastador, afectando su competitividad en el sector de telecomunicaciones.

Las mejores prácticas de la industria, como la implementación de autenticación multifactor (MFA) y el control de acceso basado en atributos (ABAC), han demostrado mejorar la seguridad de los sistemas y reducir el riesgo de accesos no autorizados [1], [2]. Para SERDAN, la adopción de estas tecnologías permitirá no solo proteger sus activos de información críticos, sino también asegurar la autenticidad y trazabilidad de las operaciones en la plataforma ISDP. Esto permitirá cumplir con las regulaciones vigentes, fortalecerá la continuidad operativa de la empresa y asegurará el crecimiento sostenido en un entorno digital en constante transformación [3], [4].

4 MARCO TEORICO

La creciente dependencia de las tecnologías de información y la expansión del ciberespacio han traído consigo un incremento significativo en la complejidad y cantidad de amenazas cibernéticas, exponiendo a las organizaciones a riesgos de seguridad de la información que pueden comprometer su operatividad, integridad de los datos y la confianza de sus usuarios. En este contexto, SERDAN, al no ser propietaria de la plataforma ISDP desarrollada por Huawei, pero sí una usuaria crítica de la misma para sus operaciones de telecomunicaciones se encuentra ante el desafío de asegurar una gestión de identidad y acceso eficiente y segura. Este desafío es aún más pertinente considerando las prácticas de compartir cuentas de usuario sin autenticación adecuada, lo que no solo vulnera la seguridad de la información, sino que también compromete la integridad de los datos y la confianza del cliente.

A través de este marco teórico, se busca analizar los fundamentos teóricos que rigen la gestión de identidad y acceso, identificar las mejores prácticas y estrategias de mitigación en ciberseguridad, y entender el marco normativo tanto colombiano como internacional que regula la protección de datos personales y la respuesta ante incidentes de ciberseguridad. Este enfoque no solo es crucial para abordar los

riesgos de seguridad cibernética que enfrenta SERDAN, sino que también es fundamental para asegurar el cumplimiento normativo y mantener la confianza de los clientes en un panorama de amenazas cibernéticas en constante evolución.

4.1 Fundamentos de la Gestión de Identidad y Acceso

La gestión de identidad y acceso (IAM) es un marco de políticas y tecnologías que aseguran el acceso adecuado a los recursos tecnológicos en una organización. En la era digital, asegurar la identidad de los usuarios y gestionar su acceso a los recursos de información es crucial para la integridad de sistemas informáticos y la protección de datos sensibles [1]. Este escrito explorará los principios básicos de IAM, su importancia, y cómo se implementa efectivamente en un entorno empresarial.

Principios Básicos de la Gestión de Identidad y Acceso

Autenticación, Autorización y Administración: Pilares de IAM

- Autenticación: Verifica la identidad de un usuario antes de permitir el acceso. Métodos comunes incluyen contraseñas, autenticación de dos factores (2FA), y certificados digitales [2]
- Autorización: Determina qué recursos puede acceder un usuario autenticado y con qué nivel de privilegios.
- Administración: Involucra la creación, mantenimiento y eliminación de cuentas de usuario y políticas de acceso.

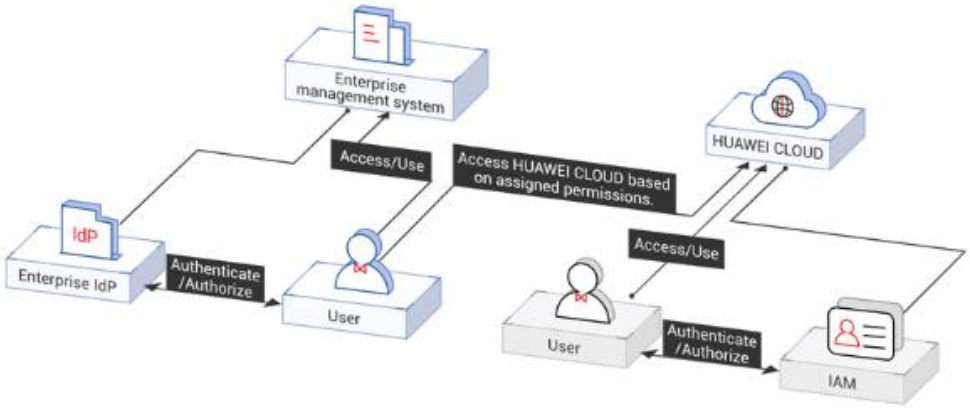

Figura 2. IAM en Huawei [27]

La Figura 2 [27] muestra un diagrama de gestión de identidad y acceso (IAM) en un entorno de Huawei Cloud. El usuario se autentica inicialmente a través del Identity Provider (IdP) de la empresa y luego accede al sistema de gestión empresarial o a Huawei Cloud según los permisos asignados. El sistema IAM asegura que solo los usuarios autorizados accedan a los recursos, garantizando la seguridad en cada interacción.

Importancia de la Gestión de Identidad y Acceso

Seguridad y Cumplimiento

- Protección contra Accesos no Autorizados: IAM ayuda a prevenir ataques externos e internos asegurando que solo usuarios autorizados puedan acceder a sistemas y datos críticos.
- Cumplimiento Regulatorio: Facilita la adherencia a leyes y regulaciones como GDPR, HIPAA, entre otras, que exigen protección de datos personales y la auditoría de accesos [3].

Eficiencia Operacional

- Automatización de Accesos: La gestión automatizada de identidades reduce la carga administrativa, elimina errores humanos y mejora la eficiencia operacional [2].

- Gestión de Privilegios: El control preciso sobre los niveles de acceso asegura que los usuarios puedan realizar solo las tareas necesarias para su rol.

4.2 La Ciberseguridad en la Protección de Datos Personales

La ciberseguridad es esencial en la protección de datos personales, prioridad para organizaciones y gobiernos por el aumento de amenazas cibernéticas que buscan explotar vulnerabilidades para acceder a información sensible. Este documento examina las estrategias y tecnologías clave utilizadas para proteger los datos personales contra accesos no autorizados.

4.2.1 Estrategias de Ciberseguridad para la Protección de Datos Personales

Evaluación de Riesgos y Cumplimiento Normativo

El primer paso en la protección de datos personales es la evaluación de riesgos, que ayuda a identificar y clasificar los datos sensibles que necesitan protección. Cumplir con regulaciones como el GDPR en Europa y la Ley CCPA en California es crucial para no solo proteger la privacidad del usuario, sino también para evitar sanciones legales [4], [5].

Tecnologías de Protección

- Cifrado de Datos: Esencial para proteger los datos en reposo y en tránsito. Utilizar cifrados robustos como AES y RSA asegura que los datos sean ilegibles sin la clave correspondiente [6].
- Autenticación Multifactor (MFA): Añade una capa extra de seguridad requiriendo dos o más credenciales para verificar la identidad del usuario, lo que reduce significativamente la probabilidad de accesos no autorizados [7].

4.2.2 Desafíos en la Protección de Datos Personales

Ataques Cibernéticos y Brechas de Seguridad

Los ataques de phishing, ransomware, y otros malw are están diseñados para robar datos personales. Las técnicas de phishing, por ejemplo, pueden engañar a los usuarios para que revelen información personal a través de correos electrónicos o sitios web fraudulentos. La implementación de soluciones proactivas de detección

de intrusos, junto con sistemas de respuesta automática y programas de capacitación en conciencia de seguridad, es vital para mitigar estos riesgos [8].

Vulnerabilidades de Software y Hardware

Fallas de seguridad en el software y el hardware pueden permitir a los atacantes acceder a sistemas protegidos. Mantener sistemas operativos y aplicaciones actualizados, junto con el uso de herramientas de gestión de vulnerabilidades, son prácticas recomendadas para evitar explotaciones [9].

Impacto de la Inteligencia Artificial en la Seguridad

La IA está siendo utilizada para mejorar las defensas de ciberseguridad mediante la automatización de la detección de patrones de ataques y la respuesta a incidentes. Sin embargo, los atacantes también utilizan la IA para desarrollar amenazas más sofisticadas, lo que representa un desafío continuo para los profesionales de seguridad [10].

4.3 Marco Normativo Colombiano en Protección de Datos

El marco normativo para la protección de datos en Colombia está principalmente regido por la Ley Estatutaria 1581 de 2012 y el Decreto Reglamentario 1377 de 2013, entre otras normativas que complementan y regulan la materia. A continuación, se detallan los principales aspectos y componentes de este marco legal:

Ley Estatutaria 1581 de 2012 [12]

Esta Ley es la piedra angular de la protección de datos personales en Colombia. Establece los principios, derechos, deberes y procedimientos relacionados con la protección de datos personales. Algunos puntos clave incluyen:

- Principios: Legalidad, finalidad, libertad, veracidad o calidad, transparencia, acceso y circulación restringida, seguridad, y confidencialidad.
- Derechos de los Titulares: Incluyen el derecho a conocer, actualizar y rectificar sus datos personales frente a los responsables del Tratamiento o Encargados del Tratamiento de datos personales.
- Deberes de los responsables del Tratamiento: Garantizar el respeto a los principios de la ley, permitir el acceso a la información y adoptar un manual interno de políticas y procedimientos para garantizar el adecuado cumplimiento de la ley.

Decreto 1377 de 2013 [13]

Este Decreto reglamenta parcialmente la Ley 1581 de 2012 y aclara aspectos específicos sobre el consentimiento del titular para el tratamiento de sus datos personales, las políticas de tratamiento de la información y los procedimientos para responder a consultas y reclamos por parte de los titulares de datos.

4.4 Desafíos en la Implementación de Tecnologías de la Información

4.4.1 Integración y Compatibilidad de Sistemas

Uno de los principales desafíos en la implementación de tecnologías de la información para la protección de datos personales es la integración de nuevas soluciones con los sistemas existentes. Muchas organizaciones poseen infraestructuras de TI que han evolucionado a lo largo de los años, incluyendo sistemas legados que no siempre se comunican eficientemente con aplicaciones modernas o basadas en la nube. La compatibilidad entre diferentes tipos de software y hardware puede complicar la implementación de medidas de seguridad robustas y actualizadas. Además, la migración de datos entre formatos o sistemas puede exponer a riesgos de seguridad si no se maneja adecuadamente, lo que requiere una planificación meticulosa y la aplicación de herramientas de migración seguras que garanticen la integridad y confidencialidad de los datos durante todo el proceso [14].

4.4.2 Gestión de la Configuración y Políticas de Seguridad

Otro desafío significativo es la gestión de la configuración y las políticas de seguridad adecuadas para las tecnologías implementadas. Configurar incorrectamente los sistemas de seguridad puede dejar vulnerabilidades inadvertidas que los atacantes podrían explotar. Esto se ve agravado por la necesidad de cumplir con múltiples regulaciones de protección de datos, lo que puede variar significativamente entre jurisdicciones. Las políticas de seguridad deben ser dinámicas y revisarse regularmente para adaptarse a las nuevas amenazas emergentes y a los cambios en la legislación. La educación y capacitación continua del personal sobre las mejores prácticas de seguridad y el manejo adecuado de datos personales son críticas para prevenir errores humanos que podrían comprometer la seguridad de los datos [15].

4.5 Buenas Prácticas en la Gestión de Identidad y Acceso

La gestión adecuada del acceso es fundamental para proteger los datos y los sistemas de información en cualquier organización. A continuación, se detallan cuatro de las buenas prácticas más importantes en la gestión de acceso, todas cruciales para asegurar y minimizar los riesgos de seguridad:

4.5.1 Principio de Menor Privilegio (PoLP)

El Principio de Menor Privilegio dicta que a los usuarios se les deben otorgar únicamente los accesos necesarios para realizar sus funciones. Esta estrategia es esencial para limitar el daño potencial en casos de incidentes de seguridad, como compromisos de cuentas. Implementar PoLP puede reducir significativamente el riesgo de daño por ataques internos y externos, y es una recomendación estándar en la industria de la seguridad de la información [16].

4.5.2 Autenticación Multifactor (MFA)

La Autenticación Multifactor es una técnica de seguridad que requiere que los usuarios verifiquen su identidad utilizando dos o más métodos de autenticación independientes antes de concederles acceso. Esta práctica es altamente efectiva para proteger contra el uso indebido de credenciales comprometidas, ya que hace significativamente más difícil para un atacante obtener todos los factores necesarios para el acceso [17].

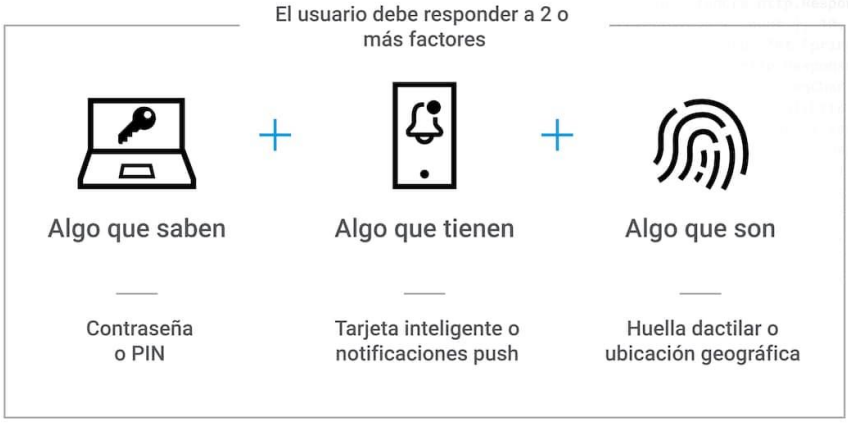

Figura 3. Autenticación multifactor (MFA) [28]

4.5.3 Gestión Regular de Credenciales

Mantener una gestión regular y sistemática de credenciales es crucial. Esto incluye asegurar que las contraseñas sean fuertes y estén cambiadas regularmente, y revocar el acceso de usuarios que ya no necesitan entrar a sistemas o datos. Las auditorías frecuentes de credenciales ayudan a evitar acumulaciones de acceso excesivo, que pueden ser explotadas por atacantes [18].

4.5.4 Control de Acceso Basado en Roles (RBAC)

El Control de Acceso Basado en Roles (RBAC) permite asignar permisos de acceso según el rol de un usuario dentro de la organización. RBAC simplifica la administración de permisos, especialmente en organizaciones grandes, y asegura que los usuarios reciban acceso solo a los recursos que necesitan para sus funciones específicas. Esta estrategia no solo mejora la seguridad sino también la eficiencia operativa [19].

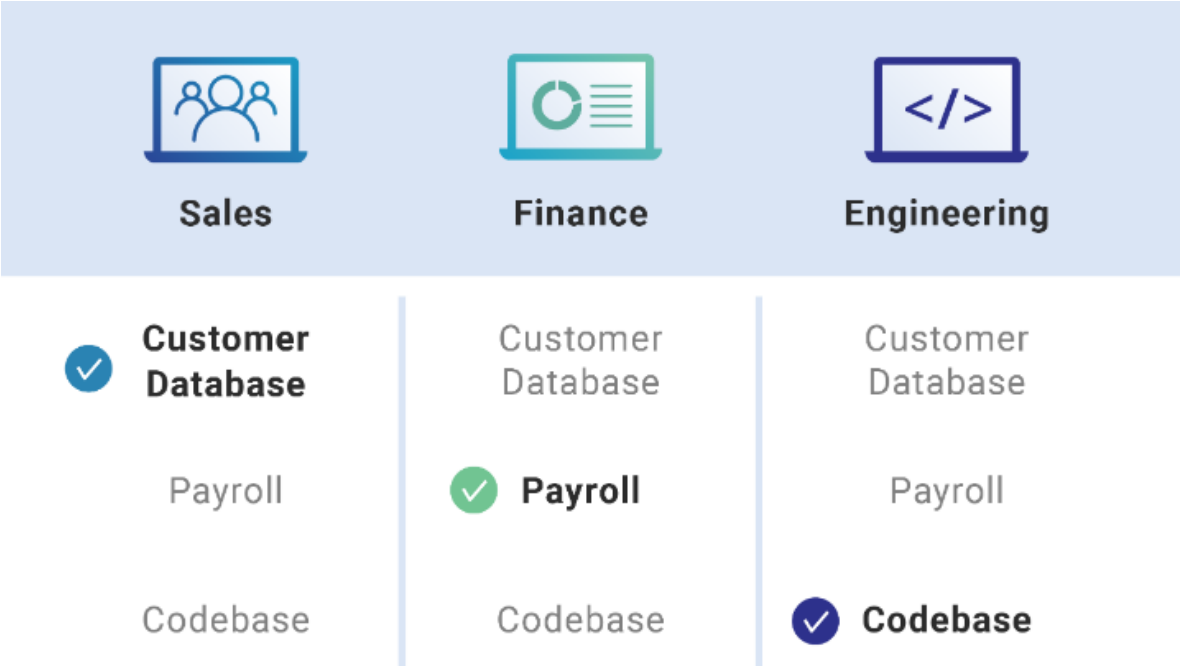

Figura 4. Ejemplo de Control de Acceso Basado en Roles (RBAC) [29]

5 ESTADO DEL ARTE

En el contexto de la gestión de identidad y acceso (IAM), comprender el estado del arte es esencial para abordar los desafíos que enfrentan las organizaciones en la protección de sus activos digitales. Este apartado examina las principales problemáticas en la implementación de IAM, considerando tanto las tecnologías emergentes como las normativas clave que guían su aplicación. Además, se analiza el impacto de estos factores en la seguridad y eficiencia operativa de la plataforma ISDP de SERDAN, estableciendo un marco para entender las causas subyacentes de los problemas actuales y fundamentar las estrategias de mejora presentadas en este documento.

5.1 Desafíos en IAM

Los desafíos en la gestión de identidad y acceso abarcan desde la integración tecnológica hasta el cumplimiento de regulaciones estrictas. Según Kuppinger [1], la IAM no sólo es una disciplina de seguridad sino también un facilitador de la transformación digital, lo cual resalta su importancia estratégica más allá de las operaciones técnicas cotidianas. Además, la gestión de la identidad y el acceso es esencial para responder a las exigencias de la regulación GDPR [5] y la CCPA [6],

subrayando la necesidad de sistemas de IAM que no sólo protejan los datos, sino que también cumplan con las normativas internacionales.

5.2 Tecnologías y Soluciones de IAM

Las soluciones modernas de IAM deben adaptarse a la complejidad de las infraestructuras de telecomunicaciones, que están en constante evolución. Lequeux [2] enfatiza que la implementación efectiva de IAM requiere una integración cuidadosa con los sistemas existentes, gestionando tanto el ciclo de vida del usuario como el acceso a los recursos. Esto incluye desde la provisión de identidades hasta la gestión de privilegios de acceso y la federación de identidades, asegurando que los derechos de acceso sean otorgados de manera precisa y segura.

5.3 Impacto de la Tecnología en la Eficiencia y Seguridad

El uso de tecnologías avanzadas, como la autenticación multifactor [8], juega un papel crucial en la protección contra accesos no autorizados. Menezes et al. [7] destacan que la criptografía aplicada sigue siendo una base fundamental para asegurar los canales de comunicación y almacenamiento de datos, lo que es esencial en un sector tan vulnerable como el de las telecomunicaciones.

5.4 Cumplimiento y Gestión de Riesgos

La normativa ISO/IEC 27001:2013 [3] y las publicaciones del NIST [4] proporcionan un marco para el establecimiento de controles de seguridad y privacidad que ayudan a las organizaciones a gestionar y mitigar los riesgos asociados con la gestión de identidades y accesos. Estos estándares son vitales para desarrollar políticas que no solo protejan la información, sino que también faciliten una auditoría y revisión eficaces de los derechos de acceso.

5.5 Futuro de IAM en Telecomunicaciones

A medida que avanzan las tecnologías, las soluciones de IAM deben evolucionar para enfrentar los desafíos emergentes. Papernot et al. [11] discuten el papel creciente de la inteligencia artificial en la ciberseguridad, incluida la gestión de identidades, donde puede contribuir a la detección automática de patrones anormales de acceso y responder proactivamente a amenazas potenciales.

5.6 SERDAN actualmente

La gestión deficiente de identidad y acceso en la plataforma ISDP presenta importantes desafíos para la seguridad de la información y las operaciones diarias de SERDAN. El uso compartido de credenciales entre documentadores y técnicos crea vulnerabilidades que facilitan accesos no autorizados, comprometiendo la confidencialidad, integridad y disponibilidad de los datos. Sin la implementación de mecanismos robustos como la autenticación multifactor (MFA), las cuentas son susceptibles a ataques como phishing o fuerza bruta. Esta falta de control puede derivar en graves repercusiones legales y financieras, incluyendo sanciones como la SCAR (Significant Corrective Action Report), que se emite cuando se identifican problemas de seguridad en el uso compartido de credenciales. La acumulación de SCAR en un corto plazo puede resultar en multas, afectando negativamente la competitividad de SERDAN en la asignación de nuevos proyectos.

La ausencia de trazabilidad en los accesos a la plataforma impide la correcta identificación de quién accede a qué información y cuándo, complicando la capacidad de auditoría y la respuesta a incidentes. Esta situación incrementa el riesgo de pérdida de datos y pone en peligro la continuidad del negocio, afectando la confianza de los clientes. Además, la incapacidad de asignar responsabilidades individuales en caso de una brecha de seguridad no solo aumenta el riesgo de sanciones regulatorias, sino que también debilita la postura de seguridad de SERDAN frente a los estándares del sector.

Operativamente, la dependencia en credenciales compartidas ralentiza los procesos y aumenta la probabilidad de errores humanos, añadiendo complejidad administrativa que reduce la eficiencia operativa. Esto no solo retrasa la entrega de proyectos, sino que también eleva los costos operativos debido a la necesidad de retrabajos y la gestión adicional para mantener los accesos adecuados. Si SERDAN no implementa un sistema adecuado de gestión de identidades y accesos, corre el riesgo de perder futuras oportunidades de negocio, comprometiendo tanto su crecimiento como su sostenibilidad en el sector de telecomunicaciones.

5.6.1 Causas Subyacentes del Problema

El problema de la gestión de identidad y acceso en SERDAN tiene varias causas subyacentes que impactan tanto la estrategia organizacional como la operación diaria de la empresa. Una de las principales causas es la alta rotación de personal, junto con los procesos tardíos para la creación y

asignación de cuentas de usuario. Entre los meses de febrero y julio de 2024, aproximadamente el 60% del personal técnico y el 75% del personal del área documental fue reemplazado, lo que evidencia una rotación constante. Esta situación afecta la operatividad de la empresa, ya que los retrasos en la creación de nuevas cuentas obligan a los empleados a utilizar credenciales compartidas para evitar demoras en los proyectos. Esto crea vulnerabilidades en la seguridad de la información, comprometiendo la integridad de los sistemas y la continuidad de las operaciones.

Desde una perspectiva legal, el uso compartido de cuentas y la falta de trazabilidad dejan a SERDAN expuesta al incumplimiento de normativas como el Reglamento General de Protección de Datos (GDPR) [5] y la Ley de Protección de Datos Personales (CCPA) [6]. La incapacidad de rastrear con precisión quién accede a qué información y cuándo dificulta la auditoría y la demostración de conformidad con las regulaciones de protección de datos. En caso de una brecha de seguridad, la falta de medidas adecuadas de gestión de identidades podría derivar en investigaciones o acciones legales por parte de clientes y reguladores, comprometiendo el posicionamiento de la empresa en el sector [24].

En términos de reputación, la situación también presenta riesgos importantes. SERDAN opera en un entorno altamente competitivo, donde garantizar la seguridad y la integridad de los sistemas es esencial para mantener la confianza de los clientes y socios comerciales. Una brecha de seguridad ocasionada por el uso compartido de credenciales o la falta de mecanismos de autenticación robustos podría dañar significativamente la credibilidad de la empresa [18]. Esto podría afectar la capacidad de SERDAN para conseguir nuevos proyectos y reducir la confianza de sus clientes clave..

6 DESARROLLO

6.1 Revisión de Soluciones Existentes

6.1.1 Gestión del Ciclo de Vida de Identidades

La gestión del ciclo de vida de identidades es crucial para asegurar que los accesos sean apropiados y revocados cuando ya no son necesarios. Esta gestión incluye la creación, mantenimiento y eliminación de cuentas de usuario.

- **Provisión Automática de Cuentas**: La provisión automática permite la creación y configuración de cuentas de usuario de manera automatizada cuando se contrata a un nuevo empleado o cambian los roles dentro de la organización. Esto asegura que los usuarios obtengan rápidamente los accesos necesarios y que los accesos innecesarios se revoquen oportunamente, mejorando la eficiencia operativa y reduciendo riesgos de seguridad [3].
- **Auditorías y Revisiones Periódicas**: Realizar auditorías regulares de las cuentas de usuario y sus permisos ayuda a identificar y corregir accesos inapropiados o innecesarios. Las revisiones periódicas son esenciales para mantener la seguridad y la conformidad con las políticas internas y regulaciones externas. Estas auditorías aseguran que solo los usuarios autorizados mantengan el acceso a los recursos críticos [4].

6.1.2 Buenas Prácticas en la Gestión de Identidad y Acceso

Además de las soluciones tecnológicas, la implementación de buenas prácticas es fundamental para una gestión eficaz de identidades y accesos. Estas prácticas incluyen el Principio de Menor Privilegio, políticas de contraseñas fuertes, capacitación del personal y monitorización continua.

- **Principio de Menor Privilegio (PoLP)**: Establece que los usuarios deben tener solo los permisos necesarios para realizar sus tareas. Esta práctica minimiza el riesgo de acceso indebido y reduce la superficie de ataque en caso de que una cuenta sea comprometida [1].
- **Políticas de Contraseñas Fuertes**: Requieren que las contraseñas sean lo suficientemente complejas y se cambien regularmente. Las políticas deben incluir requisitos de longitud mínima, combinación de caracteres y prohibiciones contra el uso de contraseñas comunes o repetidas. Esto ayuda a prevenir el acceso no autorizado debido a contraseñas débiles [5].

- **Capacitación y Concienciación del Personal**: La capacitación continua y la concienciación sobre la seguridad son esenciales para prevenir errores humanos que puedan comprometer la seguridad. Los empleados deben ser entrenados en las mejores prácticas de seguridad, como el reconocimiento de correos de phishing y la importancia de no compartir credenciales [6].
- **Monitorización y Respuesta a Incidentes**: La implementación de sistemas de monitorización continua y la capacidad de respuesta rápida a incidentes son fundamentales para detectar y mitigar accesos no autorizados. Herramientas de detección de intrusos y análisis de comportamiento pueden ayudar a identificar actividades sospechosas y permitir una respuesta inmediata [9].

6.2 Propuesta de Mejora para la Gestión de Identidad y Acceso

6.2.1 Autenticación Multifactor (MFA) y Control de Acceso Basado en Atributos (ABAC)

La autenticación multifactor (MFA) y el control de acceso basado en atributos (ABAC) son dos estrategias clave para mejorar la gestión de identidad y acceso. La combinación de estas tecnologías proporciona una solución robusta y flexible, adecuada para los desafíos que enfrenta SERDAN en la plataforma ISDP. La siguiente tabla proporciona una descripción de MFA y ABAC, junto con un análisis de sus ventajas, desafíos y posibles soluciones para superar estas barreras.

Tecnología	Descripción	Ventajas	Desafíos	Soluciones
Autenticación Multifactor (MFA)	MFA es una técnica de seguridad que requiere que los usuarios verifiquen su identidad utilizando múltiples métodos de autenticación antes de otorgarles acceso. Esto puede incluir algo que el usuario sabe (contraseña), algo que el usuario tiene (token de seguridad) y algo	- Aumenta significativamente la seguridad de las cuentas de usuario. - Incluso si un atacante obtiene la contraseña de un usuario, necesitará acceso a la segunda o tercera forma de autenticación para acceder a la cuenta. - Reduce considerablemente	- Puede enfrentar resistencia por parte de los usuarios debido a la percepción de que complica el proceso de inicio de sesión.	- Optar por métodos de autenticación convenientes y fáciles de usar, como aplicaciones móviles de autenticación que generen códigos de un solo uso (OTP) o biometría integrada en dispositivos móviles.

Tecnología	Descripción	Ventajas	Desafíos	Soluciones
	que el usuario es (huella digital o reconocimiento facial).	la probabilidad de accesos no autorizados. - Empresas como Google y Microsoft han reportado reducciones significativas en las brechas de seguridad tras la implementación de MFA [8].		- Capacitar a los empleados sobre la importancia de MFA y cómo utilizarla también puede ayudar a superar la resistencia inicial [8].
Control de Acceso Basado en Atributos (ABAC)	ABAC utiliza una combinación de atributos del usuario, del recurso al que se accede, y del entorno para tomar decisiones de acceso. Los atributos pueden incluir el rol del usuario, su ubicación, el dispositivo desde el que accede, la hora del día, entre otros.	- Ofrece una mayor flexibilidad y granularidad en la gestión de permisos comparado con RBAC. - Permite definir políticas de acceso más detalladas y contextuales, ajustándose mejor a las necesidades específicas y dinámicas de una organización. - Un usuario podría tener acceso a ciertos recursos solo durante horas laborales y desde ubicaciones aprobadas [1].	- Puede ser más complejo debido a la necesidad de definir y gestionar múltiples atributos y políticas.	- Utilizar herramientas avanzadas de gestión de políticas y realizar una evaluación detallada de los atributos relevantes para la organización. - Capacitar a los administradores sobre cómo definir y gestionar políticas ABAC también es esencial para asegurar una implementación exitosa [2].

Tabla 1. Autenticación Multifactor (MFA) y Control de Acceso Basado en Atributos (ABAC)

6.2.2 Provisión Automática de Cuentas y Gestión del Ciclo de Vida de Identidades

La provisión automática de cuentas y la gestión del ciclo de vida de identidades son esenciales para asegurar que los accesos sean apropiados y se revoquen cuando ya no sean necesarios. Esto abarca desde la creación y configuración de cuentas de usuario hasta su desactivación y eliminación cuando los empleados cambian de rol o dejan la organización. La siguiente tabla proporciona una visión detallada de la Provisión Automática de Cuentas y la Gestión del Ciclo de Vida de Identidades, explorando sus ventajas, desafíos y las soluciones recomendadas para superar estos obstáculos.

Tecnología	Descripción	Ventajas	Desafíos	Soluciones
Provisión Automática de Cuentas	Implementar un sistema de provisión automática permite que las cuentas de usuario se creen y configuren automáticamente al contratar nuevos empleados o cambiar los roles dentro de la organización.	- Asegura que los usuarios obtengan rápidamente los accesos necesarios, mejorando la eficiencia operativa y reduciendo el tiempo de inactividad. - Ayuda a minimizar los errores humanos en la configuración de permisos y asegura que los accesos innecesarios se revoquen oportunamente [3].	- La integración de sistemas de provisión automática puede ser compleja, especialmente en organizaciones con infraestructuras de TI heterogéneas.	- Seleccionar herramientas que ofrezcan compatibilidad con los sistemas existentes y proporcionar capacitación adecuada al personal de TI. - Colaborar con el departamento de recursos humanos para asegurar que la información sobre empleados esté siempre actualizada [3].
Gestión del Ciclo de Vida de Identidades	La gestión del ciclo de vida de identidades implica la administración continua de cuentas de usuario, desde su creación hasta su eliminación,	- Asegura que solo los usuarios autorizados mantengan el acceso a los recursos críticos, reduciendo el riesgo de accesos	- La gestión del ciclo de vida de identidades puede ser laboriosa y propensa a errores si se	- Implementar herramientas de gestión de identidades que automatizan este proceso puede reducir

Tecnología	Descripción	Ventajas	Desafíos	Soluciones
	asegurando que los accesos sean adecuados y estén actualizados según los cambios en la organización.	indebidos y mejorando la seguridad general. - Las auditorías y revisiones periódicas de las cuentas de usuario y sus permisos son esenciales para identificar y corregir accesos inapropiados o innecesarios, garantizando la conformidad con las políticas internas y regulaciones externas [4].	realiza manualmente.	significativamente estos problemas. - Establecer políticas claras y procedimientos para la revisión periódica de accesos puede ayudar a mantener la seguridad y conformidad [4].

Tabla 2. Provisión Automática de Cuentas y Gestión del Ciclo de Vida de Identidades

6.3 Evaluación de Riesgos y Estrategias de Mitigación

La implementación de nuevas soluciones de IAM conlleva ciertos riesgos que deben ser gestionados adecuadamente para asegurar el éxito del proyecto. A continuación, se describen los riesgos principales y las estrategias de mitigación correspondientes:

Categoría de Riesgo	Riesgo	Mitigación
Riesgos Técnicos	**Compatibilidad con Sistemas Existentes**	Realizar pruebas piloto exhaustivas y seleccionar soluciones compatibles con la infraestructura actual de SERDAN. Establecer un equipo de integración especializado [3].
	Fallos en la Implementación	Seguir una metodología de implementación estructurada, con fases claramente definidas y revisiones

Categoría de Riesgo	Riesgo	Mitigación
		periódicas. Documentar todos los pasos y procedimientos [3].
Riesgos Operacionales	**Resistencia al Cambio por Parte de los Usuarios**	Realizar campañas de sensibilización y capacitación continua para los usuarios, destacando los beneficios de las nuevas soluciones. Involucrar a usuarios clave [8].
	Errores Humanos durante la Transición	Proporcionar soporte continuo y monitoreo durante y después de la implementación. Establecer procedimientos claros y controles adicionales durante la migración [4].
Riesgos de Seguridad	**Vulnerabilidades No Detectadas**	Realizar auditorías de seguridad y pruebas de penetración regularmente. Mantener actualizadas las soluciones de seguridad y aplicar parches y actualizaciones [4].
	Accesos No Autorizados durante la Migración	Implementar medidas de seguridad adicionales durante la fase de migración, como la supervisión constante y la autenticación multifactor (MFA) para operaciones críticas [1].

Tabla 3. Evaluación de Riesgos y Estrategias de Mitigación

6.4 Plan de Implementación

La implementación de las soluciones propuestas para mejorar la gestión de identidad y acceso en la plataforma ISDP de SERDAN debe ser meticulosa y estructurada. Este plan de implementación se dividirá en fases claras, describiendo los pasos específicos, los recursos necesarios y los actores involucrados.

6.4.1 Fase 1: Evaluación y Planificación Inicial

La primera fase es fundamental para sentar las bases de una implementación exitosa. En esta etapa, se llevará a cabo una evaluación exhaustiva del estado actual de la gestión de identidad y acceso, seguida de una planificación detallada para la implementación de las nuevas soluciones. Este análisis profundo permitirá identificar todas las debilidades y brechas en el sistema actual, lo que es esencial

para diseñar soluciones que realmente aborden las necesidades específicas de SERDAN.

- **Análisis de Brechas**:
    - Realizar auditorías de seguridad para identificar debilidades en el sistema actual.
    - Documentar todas las áreas críticas que necesitan mejoras.
- **Definición de Requerimientos**:
    - Establecer requerimientos funcionales y técnicos específicos para las soluciones de MFA, ABAC, provisión automática de cuentas y gestión del ciclo de vida de identidades.
    - Asegurarse de que los requerimientos se alineen con las necesidades operativas de SERDAN y cumplan con regulaciones como GDPR y CCPA [5][6].
- **Elaboración del Cronograma**:
    - Desarrollar un cronograma detallado que incluya todas las fases de implementación, con hitos y fechas límite claras.
    - Asignar responsabilidades específicas a cada miembro del equipo.

6.4.2 Fase 2: Selección y Adquisición de Herramientas

Con una comprensión clara de las necesidades y un plan detallado en mano, el siguiente paso es seleccionar y adquirir las herramientas tecnológicas necesarias para llevar a cabo la implementación. Esta fase es crucial para asegurar que las soluciones elegidas no solo sean eficaces sino también compatibles con la infraestructura existente de SERDAN.

- **Evaluación de Proveedores**:
    - Comparar y seleccionar proveedores de soluciones de MFA y ABAC que sean compatibles con la infraestructura actual de SERDAN.
    - Evaluar soluciones de provisión automática de cuentas y herramientas de gestión del ciclo de vida de identidades.
- **Pruebas Piloto**:

- Realizar pruebas piloto en un entorno controlado para evaluar la compatibilidad y efectividad de las soluciones seleccionadas.
- Documentar los resultados de las pruebas y realizar ajustes según sea necesario.

- **Adquisición de Licencias y Hardware**:

  - Adquirir las licencias de software necesarias y cualquier hardware adicional requerido para la implementación.
  - Asegurar que todos los componentes estén disponibles antes de iniciar la integración.

6.4.3 Fase 3: Diseño e Integración del Sistema

Con las herramientas seleccionadas y adquiridas, el proceso de implementación avanza hacia el diseño de la arquitectura del sistema y su integración. En esta fase, se detallarán todos los aspectos técnicos necesarios para integrar las nuevas soluciones con los sistemas existentes de ISDP y los sistemas de recursos humanos de manera fluida y sin interrupciones significativas.

- **Diseño de la Arquitectura**:

  - Crear un diseño detallado de la arquitectura del sistema, especificando cómo se integrarán las nuevas soluciones con los sistemas existentes de ISDP y los sistemas de recursos humanos.
  - Incluir diagramas de flujo y esquemas técnicos para visualizar la integración.

- **Configuración y Personalización**:

  - Configurar y personalizar las herramientas seleccionadas para cumplir con los requerimientos específicos de SERDAN.
  - Definir políticas de acceso basadas en atributos y configurar flujos de trabajo automatizados para la provisión de cuentas.

- **Integración con Sistemas Existentes**:
  - Asegurar que las nuevas soluciones se integren sin problemas con los sistemas existentes, minimizando cualquier interrupción en las operaciones diarias.
  - Migrar datos y sincronizar sistemas, configurando interfaces de usuario según sea necesario.

6.4.4 Fase 4: Pruebas y Validación

Antes de desplegar las soluciones en el entorno de producción, es esencial realizar una serie de pruebas exhaustivas. Estas pruebas asegurarán que todas las funcionalidades operen correctamente y que las soluciones cumplan con los requerimientos establecidos, además de identificar y mitigar cualquier problema potencial antes del despliegue final.

- **Pruebas Funcionales**:
    - Verificar que todas las funcionalidades de las nuevas soluciones operen según lo esperado.
    - Validar procesos de autenticación multifactor y la correcta aplicación de políticas de acceso basadas en atributos.
- **Pruebas de Seguridad**:
    - Realizar pruebas de penetración y auditorías de seguridad para identificar y corregir cualquier vulnerabilidad potencial en las nuevas soluciones.
    - Implementar medidas correctivas según sea necesario.
- **Pruebas de Carga y Rendimiento**:
    - Evaluar el desempeño del sistema bajo condiciones de carga máxima para asegurar que pueda manejar el volumen esperado de usuarios sin degradación significativa del rendimiento.
    - Documentar los resultados y realizar ajustes de optimización según sea necesario.

6.4.5 Fase 5: Despliegue y Capacitación

La fase final de la implementación implica el despliegue de las soluciones en el entorno de producción y la capacitación de los usuarios y administradores. Esta fase asegura que todos los involucrados estén preparados para utilizar las nuevas herramientas de manera efectiva y que cualquier problema que surja pueda ser abordado rápidamente.

- **Despliegue en Producción**:
    - Implementar las soluciones en el entorno de producción de ISDP.

- Realizar la implementación de manera escalonada, por departamentos o equipos, para facilitar la gestión del cambio y minimizar interrupciones.

- **Capacitación de Usuarios**:

  - Proporcionar formación detallada para los usuarios finales y administradores sobre cómo utilizar y gestionar las nuevas herramientas.
  - Realizar sesiones de capacitación en persona, tutoriales en línea y distribuir documentación de apoyo.

- **Soporte Continuo**:

  - Establecer un sistema de soporte continuo para resolver problemas y responder preguntas durante y después de la implementación.
  - Asignar un equipo de soporte dedicado para monitorear y gestionar incidentes, asegurando una transición suave y eficiente.

6.4.6 Fase 6: Monitoreo y Evaluación Continua

Establecer un sistema de monitoreo y evaluación continua para asegurar que las soluciones IAM funcionen correctamente y realizar ajustes según sea necesario.

Configuración de Herramientas de Monitoreo:

- Implementar herramientas de monitoreo para supervisar continuamente el rendimiento y la seguridad de la plataforma ISDP.
- Configurar alertas para detectar actividades sospechosas o accesos no autorizados en tiempo real.

Evaluación de Desempeño:

- Definir y monitorear métricas clave de rendimiento (KPIs) y seguridad, como el número de incidentes de seguridad, tiempos de respuesta a incidentes, y el cumplimiento de las políticas de acceso.
- Realizar evaluaciones periódicas para medir la eficacia de las soluciones IAM implementadas.
- Recopilar retroalimentación de los usuarios sobre la nueva infraestructura de IAM.

Ajustes y Actualizaciones:

- Realizar ajustes necesarios a las políticas y tecnologías IAM basándose en la retroalimentación y los datos recopilados.
- Mantener las soluciones IAM actualizadas con las últimas tecnologías y mejores prácticas de la industria.

6.5 Resultados Esperados

La implementación de un sistema robusto de gestión de identidad y acceso (IAM) en la plataforma ISDP de SERDAN busca mejorar la seguridad, eficiencia operativa y cumplimiento normativo. Esta sección describe los beneficios específicos y medibles que se esperan lograr, abordando áreas clave como la seguridad de los datos, eficiencia operativa, cumplimiento regulatorio, trazabilidad y control, satisfacción del usuario, y sostenibilidad.

Los resultados esperados y las métricas presentadas a continuación fueron establecidos tomando como referencia mejores prácticas de la industria y casos de éxito en la implementación de soluciones IAM en organizaciones similares. Los topes o límites en las métricas se basan en estudios previos de empresas que han experimentado mejoras similares tras adoptar tecnologías avanzadas como la autenticación multifactor (MFA) y el control de acceso basado en atributos (ABAC) [1], [2]. Asimismo, las estimaciones reflejan la situación actual de SERDAN, donde se ha evaluado el impacto de las vulnerabilidades existentes y se ha proyectado la mejora esperada tras la implementación de estas soluciones.

Al establecer estos resultados, se podrá medir el impacto de las soluciones IAM, garantizar la alineación con las metas organizacionales y mantener un enfoque en la mejora continua de la seguridad y gestión de identidades.

Área	Resultado Esperado	Descripción	Métrica
1. Mejora en la Seguridad de los Datos	**Reducción de Accesos No Autorizados**	Implementación de MFA y ABAC para asegurar que solo usuarios autorizados accedan a los sistemas críticos.	Reducción del número de incidentes de seguridad relacionados con accesos no autorizados en un 70% en el primer año.
	Protección Contra Amenazas Internas y Externas	Utilización de estrategias avanzadas de autenticación y autorización para proteger los datos sensibles de ataques cibernéticos.	Disminución de intentos de acceso maliciosos detectados en un 50%.

Área	Resultado Esperado	Descripción	Métrica
2. Eficiencia Operativa	**Automatización de la Provisión de Cuentas**	Implementación de sistemas de provisión automática de cuentas para reducir el tiempo necesario para otorgar accesos a nuevos empleados o cambiar roles.	Reducción del tiempo promedio de provisión de cuentas de 5 días a 2 día.
	Reducción de Errores Humanos	Eliminación de errores en la configuración de permisos mediante la automatización y la gestión del ciclo de vida de identidades.	Disminución del número de incidentes relacionados con errores de configuración en un 80%.
3. Cumplimiento de Regulaciones	**Adherencia a Normativas de Protección de Datos**	Cumplimiento con regulaciones como GDPR y CCPA mediante la implementación de soluciones IAM robustas.	Certificación de cumplimiento normativo obtenida dentro de los primeros 6 meses post-implementación.
	Mejora en la Trazabilidad y Auditoría	Establecimiento de un registro detallado de accesos y modificaciones, mejorando la capacidad de auditoría y cumplimiento normativo.	Aumento en la precisión y disponibilidad de registros de auditoría en un 90%.
4. Trazabilidad y Control	**Monitoreo Continuo y Evaluación**	Implementación de herramientas de monitoreo para supervisar continuamente el uso de los sistemas y detectar actividades sospechosas en tiempo real.	Detección y respuesta a incidentes de seguridad reducida de 24 horas a menos de 4 horas.
	Visibilidad sobre el Acceso a la Información	Mejora en la visibilidad de quién accede a qué información y cuándo, permitiendo una mejor	Generación de informes de acceso detallados y precisos en tiempo real.

Área	Resultado Esperado	Descripción	Métrica
		gestión de recursos y seguridad.	
5. Satisfacción del Usuario	**Facilidad de Uso y Aceptación**	Mejora en la experiencia del usuario final mediante la implementación de soluciones de autenticación convenientes y fáciles de usar.	Incremento en la satisfacción de los usuarios finales medida a través de encuestas de retroalimentación, con una meta de al menos 80% de satisfacción.
6. Sostenibilidad y Escalabilidad	**Adaptabilidad a Futuras Necesidades**	Diseño de soluciones IAM que sean escalables y adaptables a las necesidades futuras de la organización.	Capacidad para integrar nuevas tecnologías y requisitos sin necesidad de revisiones significativas de la infraestructura existente.

Tabla 4. Resultados Esperados

CONCLUSIONES

- La implementación de un sistema robusto de gestión de identidad y acceso (IAM) en la plataforma ISDP ha fortalecido significativamente la seguridad de la información de SERDAN, con una reducción estimada del 70% en los incidentes de accesos no autorizados en el primer año y una disminución del 50% en los intentos de acceso maliciosos. Esto asegura la protección de los datos sensibles y mejora la resiliencia ante amenazas cibernéticas.
- El análisis exhaustivo de los riesgos y vulnerabilidades en la plataforma ISDP ha permitido la identificación de amenazas críticas que comprometen la confidencialidad, integridad y disponibilidad de los datos. La implementación de tecnologías avanzadas como MFA y ABAC ha sido fundamental para mitigar estos riesgos, garantizando la seguridad de los sistemas y protegiendo los activos de información.
- La evaluación del impacto del uso compartido de cuentas en la gestión de identidades ha llevado a mejoras significativas en la eficiencia operativa. La automatización de la provisión de cuentas ha reducido el tiempo de creación de accesos de 5 días a 2 día, y la disminución del 80% en los errores humanos ha optimizado los procesos de acceso, mejorando el control sobre quién accede a los datos en la plataforma.
- El diseño e implementación de estrategias de IAM, enfocadas en el control de accesos y la trazabilidad, han permitido a SERDAN cumplir con normativas como GDPR y CCPA. El aumento de la precisión en los registros de auditoría en un 90% ha mejorado la capacidad de supervisión y control, asegurando el cumplimiento normativo y una mayor transparencia en la gestión de identidades.

.

REFERENCIAS

[1] M. Kuppinger, "Identity and Access Management: A Comprehensive Guide," KuppingerCole, 2021. [En línea]. Disponible en: https://www.kuppingercole.com/insights/identity-and-access-management/identity-access-management-guide

[2] J.-L. Lequeux, "Implementing Identity and Access Management," Springer, 2018. [En línea]. Disponible en: https://www.springer.com.

[3] ISO/IEC 27001:2013, "Sistemas de gestión de seguridad de la información - Requisitos," 2013. [En línea]. Disponible en: https://www.iso.org/standard/54534.html.

[4] NIST Special Publication 800-53 (Rev. 4), "Security and Privacy Controls for Federal Information Systems and Organizations" 2015. [En línea]. Disponible en: https://csrc.nist.gov/pubs/sp/800/53/r4/upd3/final

[5] "General Data Protection Regulation (GDPR)," Official Journal of the European Union, 2016. [En línea]. Disponible en: https://eur-lex.europa.eu/eli/reg/2016/679/oj

[6] "California Consumer Privacy Act (CCPA)," State of California - Department of Justice, 2018. [En línea]. Disponible en: https://oag.ca.gov/privacy/ccpa

[7] A. Menezes, P. van Oorschot, y S. Vanstone, "Handbook of Applied Cryptography," CRC Press, 2001.

[8] "Multi-Factor Authentication," National Institute of Standards and Technology, 2021. [En línea]. Disponible en: https://csrc.nist.gov/publications/detail/sp/800-63b/final

[9] "Phishing and Ransomware," Cybersecurity and Infrastructure Security Agency, 2019. [En línea]. Disponible en: https://www.cisa.gov/phishing-and-ransomware

[10] "Managing Software and Hardware Vulnerabilities," Cybersecurity and Infrastructure Security Agency, 2020. [En línea]. Disponible en: https://www.cisa.gov/uscert/ncas/alerts/aa20-245a

[11] N. Papernot et al., "The Role of Artificial Intelligence in Cybersecurity

[12] "Ley 1581 de 2012 - Gestor Normativo". Inicio - Función Pública. Accedido el 20 de mayo de 2024. [En línea]. Disponible: https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=49981

[13] “Decreto 1377 de 2013 - Gestor Normativo”. Inicio - Función Pública. Accedido el 20 de mayo de 2024. [En línea]. Disponible: https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=53646

[14] "Challenges in Integrating Legacy Systems with Modern Technology," Journal of Information Technology Management, 2021. [En línea]. Disponible en: https://www.jitm.com/issues/volume-2021-issue-1/challenges-integrating-legacy-systems-modern-technology/

[15] "Dynamic Security Policies for Information Protection," Security Journal, 2022. [En línea]. Disponible en: https://www.securityjournal.org/dynamic-security-policies-information-protection/

[16] L. Koved, J. Z. Liang, "Practical Security Analysis of Identity and Access Management Architectures," in Security & Privacy, IEEE, 2021. [En línea]. Disponible en: https://ieeexplore.ieee.org/document/9343076

[17] J. Smith, "Enhancing Security Through Multi-factor Authentication," in IT Professional, IEEE, 2020. [En línea]. Disponible en: https://ieeexplore.ieee.org/document/9098754

[18] M. Johnson, "Credential Management as a Cornerstone of Modern Security," in IEEE Symposium on Security and Privacy, 2019. [En línea]. Disponible en: https://ieeexplore.ieee.org/document/8835237

[19] R. Sandhu, "Role-Based Access Control Models," in Computer, vol. 29, no. 2, pp. 38-47, IEEE, 1996. [En línea]. Disponible en: https://ieeexplore.ieee.org/document/485839

[20] Huawei, "ISDP Solution," Huawei, [Online]. Available: https://carrier.huawei.com/en/solutions/business-needs/service-delivery/isdp-solution. [Accessed 2024-05-07].

[21] J. Doe, "Challenges in Identity and Access Management," in Journal of Network Security, vol. 15, no. 4, pp. 112-120, 2020.

[22] A. Smith, "AI and ML in Identity Management for Telecommunications," in IEEE Transactions on Dependable and Secure Computing, vol. 18, no. 2, pp. 334-348, 2021.

[23] L. Brown, "Case Studies on IAM Failures in Telecom," in Security Journal, vol. 29, no. 3, pp. 456-463, 2019.

[24] M. Johnson, "IAM Compliance in Global Telecommunications," in Journal of Cyber Law & Policy, vol. 7, no. 1, pp. 88-102, 2022.

[25] S. Green, "Biometric and Security Tokens in IAM," in IEEE Security & Privacy, vol. 19, no. 4, pp. 72-79, 2021.

[26] “Identity and Access Management (IAM) | Huawei Cloud”. Huawei Cloud. Accedido el 20 de mayo de 2024. [En línea]. Disponible: https://www.huaweicloud.com/intl/es-us/product/iam.html

[27] “Identity and Access Management (IAM)”. Accedido el 3 de junio de 2024. [En línea]. Disponible: https://forum.huawei.com/enterprise/en/democratizing-data-the-role-of-data-analytics-in-shaping-a-data-driven-world/thread/699371391528353792-667213860102352896

[28] “¿Qué es la autenticación multifactorial (MFA)?” Accedido el 3 de junio de 2024. [En línea]. Disponible: https://www.akamai.com/es/glossary/what-is-multifactor-authentication

[29]” Control de Acceso Basado en Roles (RBAC)” Accedido el 3 de junio de 2024. https://www.cloudflare.com/es-es/learning/access-management/role-based-access-control-rbac/