Revisión y redefinición de la matriz de accesos para un sistema transaccional de una empresa de envíos de dinero

Nancy Rodriguez Garcia

Asesor

Jhon Fernando Sánchez Alvarez

Universidad Nacional Abierta y a Distancia UNAD

Escuela de Ciencias básicas, tecnología e ingeniería ECBTI

Ingeniería de Sistemas

2025

Tabla de Contenido

Lista de Tablas

Lista de Figuras

Resumen

Una empresa que se encuentra en crecimiento es de vital importancia manejar y controlar la información a la que puede acceder un empleado, desempeñando de forma óptima sus actividades; actualmente la empresa no cuenta con ningún sistema que permita controlar, asignar y eliminar el tipo de permiso asignado.

Desde el área de seguridad se puede observar que no existe un control de creación de permisos que se asignan a los usuarios en la plataforma de la empresa, adicional no cuenta con una debida organización que permita mantener un control de accesos y acumulan permisos que ya no requieren al momento de cambiar de áreas o realizar diferentes roles. La empresa se encuentra en crecimiento por ende debe cumplir con la regulación de la norma 27001 que nos indica crear documentos de seguridad, que nos permita tener un control de acceso al sistema transaccional para así administrar y conocer los permisos que tiene cada uno de los empleados de la empresa. La empresa actualmente no cuenta con ningún manejo de acceso, tampoco con un área que realice dicho proceso, es por ello por lo que la propuesta está basada en crear los permisos de acceso a dependiendo del área a la que corresponden.

En este trabajo de grado se implementará una redefinición de la matriz de accesos que permita mantener un control, eliminar, asignar y crear por departamentos los diferentes permisos necesarios para desempeñar sus funciones, mediante la aplicación de Duo que permitirá manejar el acceso a las aplicaciones de la empresa.

***Palabras Clave*:** Control de acceso, gestión de permisos, seguridad de la información, gestión de roles, cumplimiento normativo, protección de datos, asignación de permisos.

Abstract

A company that is growing is of vital importance to manage and control the information that an employee can access, optimally performing their activities; Currently the company does not have any system that allows controlling, assigning and eliminating the type of assigned permit.

From the security area, it can be seen that there is no control over the creation of permissions that are assigned to users on the company platform; in addition, there is no proper organization that allows maintaining access control and they accumulate permissions that are no longer available. required when changing areas or performing different roles. The company is growing; therefore it must comply with the regulation of standard 27001, which tells us to create security documents, which allows us to have access control to the transactional system in order to manage and know the permissions that each of the employees has. of the company. The company currently does not have any access management, nor does it have an area that carries out said process, which is why the proposal is based on creating access permits depending on the area to which they correspond.

In this degree work, a redefinition of the access matrix will be implemented that allows maintaining control, eliminating, assigning and creating by departments the different permissions necessary to perform their functions, through the Duo application that will allow managing access to applications. the company.

Keywords: Access control, permission management, information security, role management, regulatory compliance, data protection, permission assignment.

Introducción

En el contexto actual de crecimiento de las empresas, la correcta gestión y control de los accesos a la información es un factor clave para garantizar la eficiencia y seguridad en el desarrollo de las actividades diarias de los empleados. Para una empresa en expansión, contar con un sistema adecuado que permita asignar, gestionar y eliminar permisos de acceso a la información es de vital importancia. Sin embargo, la empresa en cuestión actualmente no dispone de ninguna herramienta que facilite este control de accesos, lo que genera posibles riesgos en la seguridad de la información, así como la acumulación de permisos innecesarios cuando los empleados cambian de roles o departamentos.

El problema identificado en el trabajo de grado se refiere a la necesidad de revisar y redefinir la matriz de accesos de un sistema transaccional utilizado por la empresa de envíos de dinero. Actualmente, la estructura de accesos podría no estar alineada con las necesidades actuales de la empresa, lo que podría generar riesgos de seguridad, ineficiencia en la operación y posibles incumplimientos regulatorios.

Desde el área de seguridad, se ha identificado que no existe un control estructurado sobre la creación y asignación de permisos, lo que dificulta mantener un acceso adecuado y organizado a las plataformas corporativas. Esto no solo compromete la seguridad, sino también la eficiencia operativa de los procesos internos. En este sentido, la empresa debe alinearse con las mejores prácticas y estándares internacionales, como la Norma ISO 27001, que establece la necesidad de contar con controles de acceso bien definidos, garantizando la protección de la información sensible y cumpliendo con las regulaciones de seguridad.

La falta de un área específica encargada de gestionar estos accesos y permisos ha hecho que la propuesta de este proyecto sea fundamental. Este trabajo de grado tiene como objetivo la

implementación de un sistema organizado de gestión de permisos de acceso basado en una matriz de accesos que permita la asignación y eliminación de permisos de forma dinámica y por departamentos. Además, se utilizará la herramienta Duo para gestionar de manera más eficiente el acceso a las aplicaciones y sistemas transaccionales de la empresa, garantizando un control adecuado que se ajuste a las necesidades de cada área y rol.

El propósito principal de este trabajo es realizar una revisión exhaustiva y redefinición de la matriz de accesos para un sistema transaccional en una empresa de envíos de dinero. La matriz de accesos es crucial para gestionar la seguridad, la autorización y la asignación de permisos dentro del sistema, lo que asegura que solo los usuarios autorizados tengan acceso a funcionalidades específicas, previniendo fraudes o accesos no autorizados. Este proceso de revisión y redefinición tiene como objetivo optimizar la estructura de accesos, garantizando que se alineen mejor con las necesidades operativas y de seguridad de la empresa.

A través de la redefinición de esta matriz de accesos, se busca optimizar el control de la información y garantizar que solo las personas autorizadas tengan acceso a los recursos necesarios para desempeñar sus funciones, minimizando riesgos y cumpliendo con los estándares de seguridad establecidos.

Justificación

El desarrollo de este trabajo tiene como fin el control de accesos en una empresa que permitirá agilizar el proceso asignación de permisos de acceso, y me permite aplicar los conocimientos técnicos aprendidos con las diferentes materias vistas durante la carrera. El alcance del sistema transaccional de la empresa abarca desde la recepción de solicitudes de envío de dinero, el procesamiento de la transacción, la verificación de la identidad del remitente y del destinatario, hasta la entrega segura de los fondos en el destino final. El impacto en el negocio es significativo, ya que un sistema eficiente garantiza la satisfacción del cliente, promueve la fidelidad hacia la empresa y genera un flujo constante de operaciones. El control de accesos es crucial para una empresa de envíos de dinero por varias razones fundamentales. En primer lugar, el control de accesos garantiza la seguridad y la integridad de las transacciones financieras, protegiendo la información confidencial y evitando posibles fraudes o accesos no autorizados a los sistemas informáticos.

Además, en el contexto de una empresa de envíos de dinero, el control de accesos ayuda a cumplir con las regulaciones y normativas establecidas para prevenir el lavado de dinero y el financiamiento del terrorismo. Al implementar medidas estrictas de control de accesos, la empresa puede demostrar su compromiso con la seguridad y la transparencia en sus operaciones.

Por último, el control de accesos contribuye a mantener la confianza de los clientes, ya que estos se sienten más seguros al saber que sus transacciones están protegidas por sistemas robustos y medidas de seguridad efectivas.

Objetivos

Objetivo General

Revisar y redefinir la matriz de accesos del sistema transaccional de la empresa de envíos de dinero, para mejorar la seguridad, asegurar el cumplimiento de normativas y optimizar la gestión de permisos de acceso a los recursos y funciones del sistema.

Objetivos Específicos

Realizar un diagnóstico exhaustivo del estado actual de la matriz de accesos, identificando debilidades, riesgos y áreas de mejora en términos de seguridad y eficiencia operativa. Se elaborar un informe con un análisis detallado de las vulnerabilidades, áreas de riesgo y oportunidades de mejora, con un puntaje de riesgo asociado a cada área identificado. Este diagnóstico debe realizarse en un plazo de 4 semanas.

Estudiar los diferentes roles y perfiles dentro de la empresa, identificando las necesidades específicas de acceso para cada tipo de usuario y ajustando la asignación de permisos según los requerimientos reales. Completar un mapeo de roles y perfiles de todos los usuarios con acceso al sistema, documentando los permisos asignados y ajustando al menos un 90% de las asignaciones de acceso que no estén alineadas con las funciones reales, en un plazo de 6 semanas.

Validar y ajustar los permisos de acceso a las funcionalidades y datos sensibles del sistema, garantizando que los usuarios solo tengan acceso a lo estrictamente necesario para cumplir con sus tareas. Realizar una revisión de los permisos de acceso de al menos el 100% de los usuarios, garantizando que el 95% de los permisos estén correctamente alineados con la política de "mínimo privilegio", dentro de un periodo de 3 semanas.

Planteamiento del Problema

Viamericas es una empresa que, como muchas otras en el entorno empresarial actual, maneja información sensible y valiosa. La protección de datos privados de usuarios y el control de acceso a recursos de la empresa son cruciales para mantener la seguridad y la integridad de la información. El entorno en el que se encuentra el problema involucra la gestión de accesos y permisos en sistemas transaccionales que pueden ser críticos para las operaciones de la empresa.

Contexto y Antecedentes

Sistema Transaccional Actual

A. Características del Sistema Transaccional

En el contexto de Viamericas, el sistema transaccional que gestiona los accesos a los recursos y aplicaciones de la empresa puede estar experimentando problemas debido a:

Gestión Manual de Accesos: La gestión manual de accesos, utilizando métodos como correos electrónicos o hojas de cálculo, es susceptible a errores humanos y falta de actualización. La falta de automatización crea un riesgo inherente de inconsistencias que pueden comprometer la seguridad del sistema. Según *ISO/IEC 27001* (2013), una de las normas clave en gestión de seguridad de la información, la gestión de accesos debe ser sistemática y documentada para reducir riesgos de accesos no autorizados y violaciones de seguridad.

Falta de Automatización: La ausencia de un sistema automatizado para la gestión de accesos puede resultar en procesos ineficientes y lentos. Los usuarios pueden tener que esperar mucho tiempo para obtener permisos o modificaciones en su acceso, lo que afecta la productividad. La automatización en la gestión de accesos no solo mejora la eficiencia, sino que también reduce el riesgo de errores y asegura la asignación correcta de permisos según roles. Según *NIST Special Publication 800-53* (2020), la automatización de la gestión de identidades y

accesos es una práctica recomendada para mejorar la seguridad y el cumplimiento, especialmente en sistemas que manejan información sensible.

Control Ad-hoc: En algunos casos, los usuarios podrían tener accesos sin una evaluación rigurosa de sus necesidades reales o de sus roles dentro de la empresa. El control de accesos ad-hoc y sin una evaluación rigurosa de las necesidades de los usuarios puede permitir accesos no autorizados. *ISO/IEC 27002* (2013), que establece controles específicos para la gestión de accesos, recomienda que la asignación de permisos sea estrictamente proporcional al rol y las responsabilidades del usuario, para minimizar los riesgos de exposición a datos no autorizados.

Problemas Asociados

Seguridad de los Datos: Sin un control adecuado de accesos, los datos sensibles están expuestos a riesgos. Según *la Ley General de Protección de Datos Personales (GDPR)* de la Unión Europea, el acceso a la información personal debe ser restringido solo a personas autorizadas y basado en una evaluación de riesgos. Las violaciones a estas normativas pueden resultar en sanciones significativas para las empresas.

Inconsistencias en la Gestión de Permisos: La gestión manual puede llevar a errores en la asignación de permisos. Por ejemplo, los usuarios que cambian de rol o dejan la empresa pueden no tener sus accesos actualizados de manera oportuna, creando brechas de seguridad. Los errores en la asignación de permisos pueden tener consecuencias graves, especialmente cuando los usuarios cambian de rol o abandonan la empresa. *ISO/IEC 27001* enfatiza la necesidad de mantener registros precisos y actualizados sobre los accesos para garantizar que los permisos sean apropiados y estén en conformidad con las políticas de seguridad de la empresa.

Falta de Auditoría y Monitoreo: El monitoreo de accesos es vital para detectar accesos no autorizados y asegurar que las políticas de seguridad sean seguidas. La *Ley Sarbanes-Oxley*

(SOX) en EE.UU. establece que las empresas deben implementar controles internos de auditoría para detectar accesos y manipulaciones no autorizadas de datos financieros y otros recursos críticos. Esto dificulta la identificación de accesos inadecuados o no autorizados y la implementación de medidas correctivas.

Cumplimiento Normativo: El incumplimiento de las normativas de protección de datos, como el *GDPR* o la *Ley de Privacidad de Consumo de California (CCPA)*, puede resultar en sanciones severas. Estos marcos legales requieren que las empresas implementen controles adecuados para proteger los datos personales y garantizar que solo los usuarios autorizados tengan acceso a esta información.

Antecedentes Relevantes

Historia del Sistema de Control de Accesos

Históricamente, muchas empresas han comenzado con sistemas manuales o básicos para gestionar accesos. En el caso de Viamericas:

Evolución del Sistema: Es probable que el sistema de gestión de accesos de Viamericas haya evolucionado de procesos manuales a métodos más sistematizados, pero aún podría no estar completamente optimizado o automatizado.

Desafíos del Sistema Actual: Los problemas con el sistema actual pueden incluir la falta de integración con otros sistemas empresariales, lo que dificulta la administración centralizada de permisos y el seguimiento de accesos. La falta de integración entre los sistemas empresariales puede dificultar una administración centralizada de accesos. Según el *ISO/IEC 27001*, la integración de sistemas y procesos relacionados con la seguridad de la información es esencial para una gestión eficaz de los accesos y la protección de datos.

Necesidades y Requerimientos

Para abordar estos problemas, Viamericas necesita implementar un sistema de control de accesos que:

Automatización de la Gestión de Permisos: Utilice tecnología para automatizar la asignación, modificación y revocación de accesos, reduciendo la posibilidad de errores humanos. De acuerdo con el *NIST Special Publication 800-53* (2020), la automatización permite una gestión de accesos más coherente y menos propensa a errores, lo que refuerza la seguridad global del sistema.

Establecimiento de Políticas Claras: Defina y aplique políticas de seguridad detalladas que aseguren que los accesos sean adecuados a los roles y responsabilidades de cada usuario. Según *ISO/IEC 27002* (2013), las políticas de seguridad deben ser específicas y alinearse con los objetivos empresariales, asegurando que los accesos sean gestionados adecuadamente según el principio de “necesidad de saber”.

Funcionalidades de Auditoría: Implemente herramientas de monitoreo y auditoría que permitan revisar y analizar los accesos, identificar posibles brechas de seguridad y tomar medidas correctivas.

Cumplimiento con Normativas: Asegure el cumplimiento con regulaciones de protección de datos y seguridad para evitar sanciones y proteger la información sensible. La *Ley GDPR* y otras regulaciones internacionales exigen que las empresas gestionen los accesos de manera que se minimicen los riesgos de violación de datos y se protejan los derechos de los usuarios.

Impacto de Accesos No Controlados en Empresas Similares

Es fundamental considerar los impactos que los accesos no controlados pueden tener en empresas similares dentro de la industria financiera y de servicios de dinero. En empresas de esta naturaleza, los accesos no controlados pueden resultar en los siguientes impactos:

Riesgo de Fraude: La falta de control sobre quién tiene acceso a los sistemas puede permitir que empleados no autorizados o actores malintencionados realicen transacciones fraudulentas. Esto podría resultar en pérdidas económicas significativas y en la pérdida de confianza de los clientes. Según un informe de PwC, el 49% de las empresas en el sector financiero han experimentado algún tipo de fraude interno, en gran parte relacionado con accesos no controlados.

Violación de Regulaciones de Seguridad: Las empresas de envíos de dinero están sujetas a regulaciones estrictas, como la Ley de Secreto Bancario y las normativas de seguridad de datos. El acceso no controlado puede derivar en violaciones de estas normativas, lo que podría resultar en sanciones o multas severas. Por ejemplo, The Financial Conduct Authority (FCA) reporta que las infracciones relacionadas con el control de accesos en instituciones financieras pueden resultar en multas de hasta 10 millones de libras.

Exposición a Ataques Cibernéticos: Los sistemas sin acceso controlado son más susceptibles a ser hackeados, lo que puede llevar a la exposición de datos sensibles de clientes, como información bancaria y personal. Según IBM's 2020 Cost of a Data Breach Report (IBM, 2020), las violaciones de seguridad causadas por accesos no controlados pueden incrementar significativamente los costos asociados con la gestión de incidentes de seguridad.

Interrupción Operativa: El acceso no autorizado a sistemas clave puede interrumpir la operación diaria de la empresa, causando demoras en las transacciones y afectando la reputación de la empresa ante los clientes. En empresas similares, se ha observado que incluso pequeños incidentes de acceso no controlado pueden generar grandes interrupciones en las operaciones, afectando la eficiencia de los servicios prestados.

Pérdida de Confianza del Cliente: El control deficiente de accesos puede afectar directamente la confianza de los clientes en la seguridad de los servicios de la empresa. Esto se traduce en la disminución de la base de clientes y la lealtad hacia la marca. En el sector de envíos de dinero, donde la confianza es crucial, cualquier brecha de seguridad puede tener efectos devastadores.

Problema Principal: Control de Accesos

El problema principal para resolver abarca varias áreas críticas relacionadas con la gestión de permisos y la seguridad de la información. A continuación, se detallan los problemas específicos que se buscan resolver:

Falta de Control Efectivo en la Asignación y Gestión de Permisos

Inconsistencias en la Asignación de Permisos: La asignación de permisos y accesos puede realizarse de forma manual, lo que lleva a inconsistencias y errores. Los permisos pueden no ser actualizados oportunamente cuando los usuarios cambian de roles o dejan la empresa, resultando en accesos no autorizados o innecesarios.

Gestión Ad-hoc de Permisos: La falta de un sistema centralizado y automatizado para gestionar los permisos puede llevar a una gestión ad-hoc, donde los accesos se asignan sin un control riguroso o documentación adecuada. Esto puede causar desorganización y falta de claridad sobre quién tiene acceso a qué recursos.

Riesgos de Seguridad por Accesos Indebidos

Accesos No Autorizados: Sin un control de accesos robusto, los usuarios pueden obtener accesos a sistemas o datos que no están alineados con sus roles y responsabilidades. Esto aumenta el riesgo de exposición de información sensible y la posibilidad de acciones malintencionadas, ya sea por parte de empleados actuales o antiguos.

Vulnerabilidad a Amenazas Internas: Los accesos indebidos, ya sea intencionales o accidentales, pueden resultar en vulnerabilidades significativas. Los empleados que no deberían tener acceso a ciertos datos podrían manipular o divulgar información confidencial, afectando la integridad y confidencialidad de los datos.

Deficiencias en la Auditoría y Monitoreo

Falta de Registro y Monitoreo de Accesos: Un sistema manual a menudo carece de capacidades efectivas para registrar y monitorear los accesos en tiempo real. Esto dificulta la identificación de actividades sospechosas o inusuales y la capacidad de responder a incidentes de seguridad de manera oportuna.

Dificultades en la Auditoría de Seguridad: La ausencia de un registro detallado y estructurado de accesos hace que sea complicado realizar auditorías y revisar la efectividad de las políticas de seguridad. Esto impide la evaluación precisa de los controles de acceso y la implementación de medidas correctivas.

Cumplimiento Normativo y Legal

Inadecuada Protección de Datos: La falta de un control riguroso sobre los accesos puede llevar a incumplimientos de regulaciones de protección de datos y privacidad, como GDPR o HIPAA. Esto no solo conlleva riesgos legales y financieros, sino que también afecta la reputación de la empresa.

Desafíos en la Implementación de Políticas de Seguridad: Sin un sistema adecuado, puede ser difícil implementar y mantener políticas de seguridad eficaces que cumplan con los estándares regulatorios y las mejores prácticas de la industria.

Importancia del Control de Accesos: Casos Concretos de Incidentes y su Impacto

El control de accesos es un aspecto fundamental para garantizar la seguridad de los sistemas transaccionales, especialmente en empresas como Viamericas, que manejan grandes volúmenes de datos sensibles y transacciones monetarias. Sin embargo, la falta de un adecuado control de accesos puede provocar incidentes graves que afecten tanto la operación interna como la reputación de la empresa. A continuación, se incluyen ejemplos de incidentes documentados y cifras que subrayan el impacto de la mala gestión de accesos.

Ejemplos de Incidentes en la Industria:

Caso de Capital One (2019): En uno de los incidentes de ciberseguridad más conocidos en la industria financiera, un empleado de una empresa de terceros consiguió acceso no autorizado a los servidores de Capital One debido a una configuración incorrecta de los permisos de acceso. Este incidente expuso más de 100 millones de registros de clientes, incluyendo datos sensibles como números de tarjetas de crédito. La causa principal fue la gestión deficiente de los permisos de acceso, lo que resultó en un costo de $80 millones en multas y remedios legales.

Caso de Uber (2016): En 2016, un ataque cibernético a Uber comprometió los datos de más de 57 millones de usuarios. La brecha se debió a la mala gestión de las credenciales de acceso de los ingenieros de Uber, que permitieron a los atacantes obtener acceso a información personal y financiera de los usuarios. Aunque el ataque se descubrió en 2017, Uber no notificó a los afectados hasta mucho después, lo que resultó en la pérdida de confianza y en multas regulatorias por violación de la Ley de Protección de Datos.

Impacto de la Mala Gestión de Accesos:

Pérdidas Financieras: Según el 2020 Cost of a Data Breach Report de IBM, las empresas que enfrentan brechas de seguridad por accesos no controlados experimentan un costo promedio de $3.86 millones debido a la pérdida de datos, la recuperación de incidentes y las multas regulatorias. En el caso de una empresa de envíos de dinero como ViAmericas, este costo podría multiplicarse por la exposición de información financiera y personal sensible.

Impacto en la Confianza del Cliente: Según Forrester (2021), el 65% de los clientes abandonan sus relaciones comerciales con instituciones financieras después de una brecha de datos significativa. En la industria de los envíos de dinero, donde la confianza del cliente es

crucial, la gestión inadecuada de accesos puede generar una pérdida irreversible de clientes y, por ende, de ingresos.

Cifras sobre el Impacto de la Mala Gestión de Accesos:

Fraude Interno: El Informe Global sobre Crimen Económico y Fraude de PwC (2020) muestra que el 49% de las empresas del sector financiero han experimentado incidentes de fraude interno, muchos de los cuales se originaron por fallas en el control de accesos. Este tipo de incidentes puede ser devastador, no solo en términos financieros, sino también en términos de reputación.

Costos Operativos: Según el Ponemon Institute, el costo promedio de una violación de seguridad en una empresa debido a accesos no controlados puede superar los $4 millones. Esto incluye la interrupción de los servicios, la gestión de la crisis, las investigaciones forenses y el costo de la comunicación a los clientes afectados.

Impacto de la Mala Gestión de Accesos: Cifras y Estadísticas Relevantes

El control adecuado de los accesos es esencial para garantizar la seguridad en los sistemas transaccionales de empresas como ViAmericas, que manejan datos sensibles y realizan transacciones financieras. La mala gestión de accesos puede derivar en incidentes graves, como fraudes internos, fugas de datos o ciberataques, los cuales afectan tanto la integridad de las operaciones como la confianza de los clientes. A continuación, se presentan estadísticas claves sobre el impacto de los accesos no controlados:

Ataques Internos por Accesos No Controlados:

Según el Informe Global sobre Crimen Económico y Fraude de PwC (2020), el 49% de las empresas en el sector financiero han sufrido fraudes internos debido a accesos no controlados o mal gestionados. Estos fraudes suelen originarse cuando los permisos de acceso no se

gestionan de manera adecuada, lo que permite a los empleados o contratistas obtener privilegios indebidos para alterar o desviar fondos.

Porcentaje de Fraudes Relacionados con Accesos Indebidos:

El Informe de Forrester (2021) señala que el 34% de los fraudes en las instituciones financieras están relacionados directamente con accesos indebidos. Esto incluye tanto fraudes cometidos por empleados con acceso a sistemas internos, como ataques externos facilitados por credenciales comprometidas debido a malas prácticas de gestión de accesos.

Fugas de Datos y Accesos No Controlados:

Según el 2020 Cost of a Data Breach Report de IBM, el 60% de las brechas de seguridad se deben a accesos no controlados. Estas brechas pueden incluir la exposición de información financiera, datos personales de clientes o registros transaccionales, lo cual no solo afecta la seguridad sino también la reputación de la empresa. La mala gestión de los accesos aumenta la probabilidad de que personas no autorizadas obtengan acceso a estos datos sensibles.

Costos Financieros de la Mala Gestión de Accesos:

El costo promedio de una brecha de seguridad por accesos no controlados es significativo. Según el Informe de IBM (2020), el costo promedio por cada brecha es de $3.86 millones. Este monto incluye tanto las pérdidas económicas derivadas de la violación, como los costos asociados con la recuperación del incidente, las multas regulatorias y las demandas legales de los clientes afectados.

Porcentaje de Empresas Afectadas por Incidentes de Accesos No Controlados:

Un estudio realizado por Vanson Bourne (2020) muestra que el 52% de las empresas globalmente han experimentado incidentes relacionados con accesos no controlados. Esto refleja

la magnitud del problema y la necesidad urgente de establecer políticas de seguridad más estrictas en cuanto al control de accesos.

Impacto en la Confianza del Cliente:

De acuerdo con el Ponemon Institute (2021), el 65% de los clientes abandonan a una empresa después de que sus datos sean comprometidos por una brecha de seguridad significativa. Esto demuestra cómo los incidentes relacionados con accesos mal gestionados no solo afectan las finanzas de la empresa, sino que también tienen un impacto negativo en la relación con los clientes.

Impacto del Problema

Problemas específicos

En Viamericas, la falta de un control de accesos efectivo representa un riesgo significativo para la seguridad de los datos privados de los usuarios y para la protección general de la información de la empresa. El problema principal para resolver abarca varias áreas críticas relacionadas con la gestión de permisos y la seguridad de la información. A continuación, se detallan los problemas específicos que se buscan resolver:

Falta de Control Efectivo en la Asignación y Gestión de Permisos

Inconsistencias en la Asignación de Permisos: La asignación de permisos y accesos puede realizarse de forma manual, lo que lleva a inconsistencias y errores. Los permisos pueden no ser actualizados oportunamente cuando los usuarios cambian de roles o dejan la empresa, resultando en accesos no autorizados o innecesarios. La falta de actualización de los permisos puede generar brechas de seguridad, como se indica en la Guía de Buenas Prácticas de Seguridad de la Información del NIST (2020).

Riesgos de Seguridad por Accesos Indebidos

Accesos No Autorizados: Sin un control de accesos robusto, los usuarios pueden obtener accesos a sistemas o datos que no están alineados con sus roles y responsabilidades. Esto aumenta el riesgo de exposición de información sensible y la posibilidad de acciones malintencionadas, ya sea por parte de empleados actuales o antiguos. Según *ISO/IEC 27002* (2013), un sistema de gestión de accesos debe estar documentado y estandarizado, y debe contar con un enfoque proactivo para asignar, modificar y revocar accesos en función de los roles y las responsabilidades dentro de la organización.

Vulnerabilidad a Amenazas Internas: Las amenazas internas representan un riesgo significativo para la seguridad de la información. *NIST SP 800-53* (2020) reconoce que los empleados pueden representar tanto un riesgo intencional como accidental, lo que destaca la necesidad de un control de accesos sólido para prevenir el acceso indebido a datos sensibles. Los empleados que no deberían tener acceso a ciertos datos podrían manipular o divulgar información confidencial, afectando la integridad y confidencialidad de los datos.

Deficiencias en la Auditoría y Monitoreo

Falta de Registro y Monitoreo de Accesos: Un sistema manual a menudo carece de capacidades efectivas para registrar y monitorear los accesos en tiempo real. Esto dificulta la identificación de actividades sospechosas o inusuales y la capacidad de responder a incidentes de seguridad de manera oportuna. El ISO/IEC 27001 (2013) establece que las organizaciones deben implementar procesos para la auditoría continua de accesos y actividades, lo que permite detectar y abordar problemas de seguridad de manera oportuna.

Dificultades en la Auditoría de Seguridad: La ausencia de un registro detallado y estructurado de accesos hace que sea complicado realizar auditorías y revisar la efectividad de las políticas de seguridad. Esto impide la evaluación precisa de los controles de acceso y la

implementación de medidas correctivas. Según ISO/IEC 27002 (2013), un sistema de gestión de accesos debe incluir registros de auditoría detallados que permitan verificar la efectividad de las políticas de seguridad y realizar ajustes cuando sea necesario.

Problemas Actuales

Los problemas, desafíos o deficiencias en la matriz de accesos del sistema transaccional pueden ser críticos y deben abordarse con prontitud. Algunas de las posibles problemáticas podrían incluir:

Vulnerabilidades de seguridad: Posibles brechas en el sistema que podrían ser explotadas por actores malintencionados para acceder a información confidencial o realizar transacciones no autorizadas.

Acceso no autorizado: Falta de un control estricto sobre quién tiene acceso al sistema, lo que podría exponerlo a riesgos significativos de seguridad.

Inconsistencias en los permisos de acceso: Situaciones en las que los usuarios tienen permisos que no se corresponden con sus roles o responsabilidades, lo que puede llevar a mal uso de la información o a errores operativos. Estos problemas pueden comprometer la integridad y la seguridad del sistema transaccional, así como la confianza de los clientes en la empresa. Es fundamental identificar y abordar estas deficiencias para fortalecer la infraestructura de seguridad y garantizar operaciones confiables y seguras.

Riesgos Asociados

Los riesgos asociados a los problemas identificados en la matriz de accesos del sistema transaccional son significativos y podrían tener consecuencias graves para la empresa de envíos de dinero. Algunos de los riesgos potenciales incluyen:

Posibilidad de fraudes: La existencia de vulnerabilidades o accesos no autorizados aumenta el riesgo de que se perpetren fraudes financieros, comprometiendo la integridad del sistema y generando pérdidas económicas.

Pérdida de datos sensibles: Las deficiencias en la matriz de accesos podrían conducir a la exposición de información confidencial de los clientes, lo que a su vez podría resultar en la pérdida de confianza por parte de estos y dañar la reputación de la empresa.

Sanciones regulatorias: Incumplir con las regulaciones y normativas en materia de seguridad y protección de datos podría acarrear sanciones financieras y legales por parte de las autoridades regulatorias, afectando la viabilidad y reputación de la empresa.

Daño a la reputación de la empresa: Cualquier incidente relacionado con accesos no autorizados, vulnerabilidades o fraudes podría provocar un daño significativo a la reputación de la empresa, afectando su posición en el mercado y la percepción pública. Es crucial abordar estos riesgos mediante la implementación de medidas efectivas para fortalecer el control de accesos y garantizar la seguridad integral del sistema transaccional.

Cumplimiento Normativo

La empresa de envíos de dinero está sujeta a regulaciones específicas, como GDPR (Reglamento General de Protección de Datos) o PCI-DSS (Estándar de Seguridad de Datos para la Industria de Tarjetas de Pago), es fundamental que el proyecto de mejora en el control de accesos contribuya al cumplimiento normativo de manera efectiva.

En el caso del GDPR, el proyecto se enfocaría en garantizar que los accesos a datos personales estén estrictamente controlados y que se cumplan los principios de protección de datos, incluyendo la limitación del acceso a la información personal y la implementación de medidas técnicas y organizativas para garantizar la seguridad de los datos. Por otro lado, en

relación con el PCI-DSS, el proyecto podría orientarse a asegurar que los accesos al entorno de procesamiento de pagos estén adecuadamente restringidos y que se cumplan con los requisitos específicos en cuanto a la protección de la información de tarjetas de pago.

Para abordar el cumplimiento normativo con GDPR y PCI-DSS, es crucial considerar las siguientes estrategias dentro del proyecto de mejora en el control de accesos:

Identificación y clasificación de datos: Es fundamental identificar y clasificar los datos personales y financieros que se manejan en el sistema transaccional. Esta clasificación permitirá aplicar controles de accesos más rigurosos a la información más sensible, en línea con los requisitos de protección de datos del GDPR y PCI-DSS.

Implementación de controles de acceso basados en roles: La adopción de un modelo de control de acceso basado en roles permite asignar permisos específicos a los usuarios según sus funciones y responsabilidades. Esto contribuye a la limitación del acceso a la información personal y financiera, cumpliendo con los principios del GDPR y los requisitos de PCI-DSS.

Registro y monitoreo de accesos: La implementación de mecanismos de registro y monitoreo detallado de los accesos al sistema transaccional permiten demostrar que se están cumpliendo con las directrices de auditorías requeridas por ambas regulaciones. Esto incluye la capacidad de rastrear quién accede a qué datos, cuándo y con qué propósito.

Reforzamiento de medidas de seguridad: El proyecto debe incluir la implementación o mejora de medidas técnicas para proteger la seguridad de los datos, como el cifrado, la autenticación multifactor, el control de sesiones, entre otros, en línea con los requisitos específicos tanto del GDPR como del PCI-DSS.

A continuación, se relaciona cada normativa con la solución propuesta y cómo se cumple:

Tabla 1.

Normativas con la solución propuesta

Normativa	Requisito Específico	Solución Propuesta	Cumplimiento
GDPR (Reglamento General de Protección de Datos)	Artículo 5: Principios de tratamiento de datos personales Integridad, confidencialidad, y disponibilidad. Acceso restringido a datos personales.	Implementación de RBAC (Role-Based Access Control), donde los usuarios solo acceden a datos necesarios para su función. Uso de autenticación multifactor (MFA).	Cumple con la restricción de acceso, garantizando que solo los usuarios autorizados tengan acceso a los datos.
GDPR (Reglamento General de Protección de Datos)	Artículo 32: Seguridad del tratamiento Implementación de medidas de seguridad para proteger datos personales.	Implementación de MFA, autenticación robusta y monitorización de accesos con registros detallados.	Se garantiza la protección de los datos personales mediante la implementación de medidas de seguridad adecuadas.
PCI-DSS	Requisito 7: Restringir acceso a datos de tarjetas Solo personal autorizado puede acceder a datos financieros. - Permisos según el principio de necesidad de saber.	Uso de RBAC para asignar accesos solo a personal autorizado según su rol. Implementación de MFA para acceso a sistemas que contienen datos de pago.	Asegura que solo el personal autorizado puede acceder a datos sensibles según su necesidad de conocimiento.
PCI-DSS	Requisito 10: Seguimiento y monitoreo Registro y auditoría de todos los accesos a sistemas que contienen datos de tarjetas.	Implementación de registro detallado de accesos (logs), incluyendo fecha, hora, usuario, IP y acciones realizadas. Monitoreo continuo para detectar accesos no autorizados.	Cumple con el monitoreo y registro de todos los accesos a datos sensibles, con auditoría periódica.
ISO 27001	Control A.9.2.1: Control de acceso a sistemas y aplicaciones Implementación de controles adecuados para el acceso a sistemas.	Implementación de RBAC, autenticación fuerte, y auditoría continua de accesos para verificar que solo los usuarios con permisos adecuados puedan acceder.	Asegura que el acceso a sistemas de información se gestione según los requisitos de seguridad y se audite regularmente.

ISO 27001	Control A.12.4.1: Registros de acceso Asegurar la integridad y protección de registros de acceso a sistemas.	Implementación de registro inmutable de accesos con logs protegidos de alteraciones y almacenados de manera segura.	Cumple con la integridad de los registros de acceso, asegurando que no se puedan modificar y se almacenan de forma segura.

Nota: Tabla con las normativas y su solución propuesta y su cumplimiento

Impacto en la Seguridad

Una matriz de accesos bien controlada tendrá un impacto significativo en la mejora de la seguridad del sistema transaccional, protegiendo la confidencialidad, integridad y disponibilidad de los datos y transacciones de la siguiente manera:

Confidencialidad de los datos: Al implementar controles de acceso restrictivos basados en roles, se garantiza que solo los usuarios autorizados tengan acceso a la información relevante para sus funciones. Esto evita el riesgo de exposición de datos sensibles a usuarios no autorizados, lo que fortalece la confidencialidad de la información personal y financiera.

Integridad de los datos: Una matriz de accesos bien controlada también contribuye a preservar la integridad de los datos al limitar quién tiene la capacidad de modificar o eliminar información dentro del sistema transaccional. Esto ayuda a prevenir alteraciones no autorizadas en los datos, garantizando su exactitud y fiabilidad.

Disponibilidad del sistema: Al restringir adecuadamente los accesos y asignar permisos según roles específicos, se minimiza el riesgo de interferencias maliciosas o accidentales que puedan afectar la disponibilidad del sistema transaccional. Esto contribuye a mantener la operatividad continua del sistema, asegurando que esté disponible para su uso cuando sea necesario. Además, una matriz de accesos bien diseñada puede ayudar a detectar y prevenir actividades sospechosas o inusuales dentro del sistema, lo que fortalece aún más la seguridad al proporcionar una capa adicional de protección contra posibles amenazas internas o externas.

Mejora de la Eficiencia

La revisión y control de la matriz de accesos puede tener un impacto significativo en la mejora de la eficiencia operativa al reducir el tiempo y los recursos necesarios para gestionar el acceso de los usuarios de manera adecuada de las siguientes maneras:

Simplificación de la gestión de accesos: Al establecer una matriz de accesos clara y bien definida, se simplifica el proceso de asignación y gestión de permisos. Los administradores pueden basarse en roles predefinidos para otorgar rápidamente los accesos necesarios a los usuarios, evitando la necesidad de configuraciones individuales complejas.

Reducción de errores humanos: Al estandarizar la gestión de accesos a través de una matriz controlada, se minimiza el riesgo de errores humanos en la asignación de permisos. Esto contribuye a una mayor precisión y consistencia en la gestión de accesos, reduciendo la posibilidad de otorgar accidentalmente accesos indebidos o excesivos. 3. Agilización del proceso de incorporación y desvinculación: Una matriz de accesos bien estructurada facilita el proceso de incorporación y desvinculación de usuarios. Al contar con roles predefinidos y claras políticas de acceso, se agiliza la asignación inicial de permisos para nuevos empleados y la revocación o ajuste rápido de accesos al producirse cambios en las responsabilidades o salidas del personal.

Cumplimiento normativo simplificado: Una matriz controlada facilita la demostración del cumplimiento normativo en lo que respecta al control de accesos, lo que puede agilizar las auditorías y evaluaciones regulatorias al proporcionar una visión clara y coherente de cómo se gestionan los accesos dentro del sistema transaccional.

En resumen, la revisión y control efectivo de la matriz de accesos no solo contribuye a mejorar la seguridad, sino que también optimiza la eficiencia operativa al simplificar la gestión de accesos, reducir errores, agilizar procesos clave y facilitar el cumplimiento normativo.

Beneficios Tangibles

La implementación exitosa del proyecto de control de acceso no solo puede conducir a una reducción palpable en los incidentes de seguridad, sino también a un aumento en la confianza del cliente, mejoras significativas en la eficiencia operativa y una mayor capacidad para cumplir con las regulaciones establecidas. Los beneficios tangibles que se esperan obtener con la implementación del proyecto de control de acceso incluyen:

Reducción de incidentes de seguridad: Se espera una disminución significativa en los incidentes de seguridad relacionados con accesos no autorizados o inadecuados al sistema transaccional, lo que puede resultar en la protección de datos sensibles y la mitigación de riesgos asociados con posibles brechas de seguridad.

Aumento de la confianza del cliente: Al garantizar la confidencialidad, integridad y disponibilidad de los datos y transacciones a través de un control riguroso de accesos, se espera que la percepción de seguridad por parte de los clientes aumente, generando mayor confianza en la organización y sus servicios.

Mejora de la eficiencia operativa: La implementación efectiva de una matriz controlada de accesos puede conducir a una mayor eficiencia operativa al simplificar procesos relacionados con la gestión de permisos, reducir errores y agilizar tareas asociadas a la incorporación, desvinculación y cambios en los roles de los usuarios.

Cumplimiento normativo mejorado: Se espera que el proyecto contribuya a una mayor facilidad en el cumplimiento normativo en lo que respecta al control de accesos, lo que puede resultar en una reducción del tiempo y esfuerzo dedicado a auditorías y evaluaciones regulatorias.

Costo-Beneficio

El análisis costo-beneficio del proyecto de control de acceso es fundamental para demostrar que los beneficios derivados superarán los costos asociados con su implementación y mantenimiento a lo largo del tiempo. A continuación, se detallan algunos aspectos a considerar:

Costos asociados con la implementación y mantenimiento:

Inversión inicial en tecnología y software de gestión de accesos.

Costos de capacitación para el personal en la utilización del nuevo sistema.

Posibles gastos relacionados con la consultoría externa para la implementación.

Costos continuos de mantenimiento, actualizaciones y soporte técnico.

Beneficios esperados:

Reducción de incidentes de seguridad que podrían resultar en costos significativos por pérdida de datos, interrupciones operativas o daño a la reputación.

Aumento de la confianza del cliente, lo que puede traducirse en retención de clientes existentes y adquisición de nuevos clientes.

Mejora de la eficiencia operativa, lo que podría conducir a ahorros en tiempo y recursos dedicados a la gestión de accesos.

Cumplimiento normativo mejorado, reduciendo posibles multas o sanciones por incumplimiento.

Al realizar un análisis detallado, se espera demostrar que los beneficios derivados del proyecto superarán los costos asociados con su implementación y mantenimiento a lo largo del tiempo. Este análisis proporcionará una visión clara del retorno de la inversión (ROI) esperado, respaldando la viabilidad y el valor del proyecto.

Plan de Implementación

El plan de implementación para llevar a cabo la revisión y control de la matriz de accesos debe abordar varias fases del proyecto, asignar recursos necesarios, establecer un cronograma y definir las responsabilidades del equipo. A continuación, se presenta un esbozo general del plan:

Fase 1: Evaluación inicial

Recursos necesarios: Equipo de auditoría interna, personal de TI, expertos en seguridad.

Responsabilidades del equipo: El equipo de auditoría interna liderará la evaluación inicial, identificando los puntos críticos y áreas de mejora en la matriz de accesos existente.

Cronograma: 2 semanas.

Fase 2: Diseño y planificación

Recursos necesarios: Equipo de TI, expertos en gestión de accesos.

Responsabilidades del equipo: El equipo de TI trabajará en el diseño de la nueva matriz de accesos,

considerando las recomendaciones de la evaluación inicial y las mejores prácticas en seguridad informática.

Cronograma: 3 semanas.

Fase 3: Implementación

Recursos necesarios: Equipo de TI, personal de soporte técnico, usuarios clave para pruebas piloto.

Responsabilidades del equipo: El equipo de TI llevará a cabo la implementación del nuevo sistema, con el

soporte del personal técnico y la participación activa de usuarios clave para pruebas piloto.

Cronograma: 6 semanas.

Fase 4: Capacitación y despliegue completo

Recursos necesarios: Equipo de capacitación, personal de TI.

Responsabilidades del equipo: El equipo de capacitación proporcionará formación adecuada sobre el

nuevo sistema a todo el personal relevante, mientras que el equipo de TI supervisará el despliegue completo

y la transición efectiva al nuevo sistema.

Cronograma: 2 semanas.

Fase 5: Monitoreo y ajustes

Recursos necesarios: Equipo de seguridad informática, personal de TI.

Responsabilidades del equipo: El equipo de seguridad informática supervisará el monitoreo continuo del sistema para identificar posibles mejoras o ajustes necesarios, mientras que el equipo de TI estará disponible para realizar los cambios correspondientes.

Cronograma: Duo

Este plan detallado proporciona una estructura clara para la revisión y control de la matriz de accesos, asegurando que se asignen los recursos adecuados, se establezcan responsabilidades claras y se cumplan los plazos previstos para cada fase del proyecto.

Riesgos y Mitigaciones

Durante la implementación del proyecto de revisión y control de la matriz de accesos, es importante identificar posibles riesgos y proponer estrategias de mitigación para abordarlos de manera efectiva. Algunos riesgos y sus correspondientes mitigaciones podrían ser:

Tabla 2.

Riesgos y mitigaciones

Riesgo	Descripción	Mitigación
Accesos indebidos debido a falta de capacitación	El personal no está completamente capacitado en el manejo de permisos y accesos, lo que puede llevar a errores en la asignación de permisos.	Capacitación continua: Entrenamiento regular sobre políticas de acceso y uso de herramientas de autenticación. Evaluaciones periódicas: Simulaciones y ejercicios para evaluar la comprensión de las políticas.
Accesos no autorizados	Un usuario no autorizado puede acceder a sistemas sensibles debido a brechas en los controles de acceso.	Monitorización proactiva: Implementación de sistemas de monitoreo en tiempo real. Detección de anomalías: Herramientas para identificar comportamientos inusuales. Procedimientos de respuesta a incidentes: Plan de acción rápido para contener y analizar el incidente.
Interrupciones operativas por fallos en la gestión de accesos	Un fallo en el sistema de gestión de accesos podría interrumpir la operación o bloquear el acceso a los usuarios necesarios.	Redundancia en sistemas críticos: Uso de sistemas secundarios para asegurar la disponibilidad de los accesos. Planes de recuperación ante desastres (DRP): Protocolo para restaurar accesos de forma rápida. Accesos temporales: Procedimientos manuales para otorgar accesos mientras se resuelve el problema.
Falta de control sobre accesos privilegiados	La asignación incorrecta de permisos de acceso privilegiado podría comprometer la seguridad de la infraestructura y los datos.	Revisión y ajuste regular de permisos: Evaluaciones periódicas de los accesos otorgados. Principio de menor privilegio (PoLP): Solo otorgar los permisos estrictamente necesarios.
Accesos incorrectos por errores humanos	Los errores humanos en la asignación de accesos pueden dar lugar a permisos incorrectos, poniendo en riesgo la seguridad.	Automatización de procesos de acceso: Uso de herramientas que minimicen los errores manuales. Revisión y validación de permisos: Implementación de un proceso de doble validación para garantizar la precisión.
Acceso no autorizado a datos sensibles o financieros	La falta de controles en el acceso a datos sensibles, como información financiera o personal, podría resultar en fugas o mal uso de la información.	Autenticación multifactor (MFA): Implementación de MFA para usuarios con acceso a datos sensibles. Políticas de acceso estricto: Revisión continua y aprobación de accesos a

		datos sensibles por parte de responsables.
Falta de documentación en la asignación de permisos	La falta de documentación adecuada sobre los accesos asignados dificulta el control y seguimiento de los permisos otorgados.	Registro detallado de accesos: Implementación de un sistema que registre y audite todas las solicitudes y asignaciones de accesos. Auditorías regulares: Revisiones periódicas de los accesos y documentación para garantizar la transparencia.

Nota: Se identifican posibles riesgos y proponer estrategias de mitigación

Al identificar estos riesgos potenciales y proponer estrategias efectivas de mitigación, se podrá abordar los desafíos que puedan surgir durante la implementación del proyecto, asegurando una transición exitosa hacia la nueva matriz de accesos.

Delimitación del proyecto

Se controlará el acceso a la información que ya se encuentra almacenada dentro del sistema de las empresas disponibles.

El escenario en cual se desarrollará el presente trabajo será dentro de la empresa Viamericas S.A

Se pretende manejar una base con los permisos asignados a las aplicaciones de la empresa.

Marco Conceptual y Teórico

Control de Acceso es un mecanismo fundamental en la gestión de la seguridad informática, utilizado para garantizar que solo los usuarios autorizados tengan acceso a los recursos o datos de una organización. Según Villegas (2023), el control de acceso se basa en la identificación y autenticación de los usuarios, seguida de la autorización, que define qué acciones o recursos están permitidos según el perfil o rol del usuario. Este proceso asegura que se protejan los recursos de la organización y se minimicen los riesgos de acceso no autorizado.

Tipos de Control de Acceso

Villegas (2023) clasifica los sistemas de control de acceso en dos tipos principales:

Sistemas de Control de Acceso Autónomos: Son aquellos sistemas independientes que permiten controlar el acceso a recursos, como puertas o zonas específicas, sin depender de una conexión a un sistema centralizado. Estos sistemas no almacenan registros detallados de los eventos ocurridos, lo que limita su capacidad de monitoreo.

Sistemas de Control de Acceso en Red: A diferencia de los sistemas autónomos, estos sistemas están integrados en una red que se conecta a un servidor central o a un software de gestión de acceso. Esto permite la creación de registros detallados de todas las operaciones realizadas, lo que facilita la auditoría y el seguimiento en tiempo real de las acciones de los usuarios. La implementación de este tipo de sistemas aumenta la seguridad y permite un control más eficiente de los accesos.

En el proyecto de revisión y redefinición de la matriz de accesos para una empresa de envíos de dinero, el control de acceso en red sería la opción más adecuada. Este sistema permitiría registrar todas las operaciones realizadas sobre el sistema transaccional, incluyendo la asignación de permisos de acceso a los datos sensibles como los registros de clientes, las

transacciones financieras y los recursos administrativos. Implementar un control de acceso basado en roles (RBAC) permitiría a la empresa otorgar permisos específicos a diferentes empleados según su rol, minimizando riesgos de acceso no autorizado y mejorando la eficiencia operativa.

Seguridad de la información: La seguridad de la información se refiere al conjunto de prácticas, políticas y medidas adoptadas para proteger la confidencialidad, integridad y disponibilidad de los datos dentro de una organización. Toro (2021) explica que la seguridad de la información abarca el uso de diversas técnicas, como la criptografía, la gestión de accesos, las auditorías de seguridad, y la implementación de políticas de protección, para salvaguardar los datos sensibles frente a amenazas internas y externas.

La seguridad de la información es crucial para cualquier organización, ya que los datos manejados no solo son un activo valioso, sino que también están sujetos a normativas regulatorias que exigen su protección. Por ejemplo, el Reglamento General de Protección de Datos (GDPR) en la Unión Europea establece que las organizaciones deben implementar medidas de seguridad adecuadas para proteger los datos personales de los individuos, lo que refuerza la importancia de un control de accesos adecuado y la seguridad de la información en general.

En el contexto del proyecto de redefinición de la matriz de accesos, la seguridad de la información es crítica para proteger los datos sensibles que maneja la empresa de envíos de dinero. Esto incluye información personal de los clientes, registros de transacciones y datos bancarios. A través de un control de acceso adecuado, la empresa puede garantizar que solo las personas con la autorización necesaria puedan acceder a estos datos, cumpliendo con normativas de seguridad como la Ley de Protección de Datos Personales, por ejemplo si un empleado

cambia de puesto dentro de la empresa, es crucial que sus accesos a sistemas sensibles (como datos de clientes o transacciones) sean revisados y ajustados, evitando que continúe teniendo permisos innecesarios para acceder a estos datos. Esto ayuda a prevenir accesos no autorizados y protege la confidencialidad de los datos.

Objetivos de la Seguridad de la Información

Según la *ISO/IEC 27001* (2013), los tres principales objetivos de la seguridad de la información son:

Confidencialidad: Asegurar que la información solo sea accesible para las personas autorizadas.

Integridad: Proteger los datos contra alteraciones no autorizadas.

Disponibilidad: Garantizar que la información esté accesible y usable cuando sea necesario.

Gestión de Roles

La gestión de roles es una práctica dentro del control de acceso que implica asignar permisos de acceso a los usuarios en función de sus roles dentro de la organización. Según Sandhu et al. (1996), en un modelo de control de acceso basado en role, los usuarios se agrupan en roles que reflejan sus funciones dentro de la organización, y a estos roles se les asignan permisos específicos sobre los recursos del sistema. Los usuarios, a su vez, heredan los permisos de los roles que se les asignan, lo que simplifica la gestión y control de accesos.

En el proyecto de redefinición de la matriz de accesos, la gestión de roles es fundamental para asegurar que cada empleado tenga acceso solo a los recursos necesarios para realizar su trabajo. Por ejemplo, los agentes de servicio al cliente podrían tener acceso a los datos básicos de

los clientes, pero no a los registros de transacciones financieras, mientras que el personal administrativo o gerencial podría tener acceso completo a ambos tipos de datos.

Control de Accesos Basado en Roles (RBAC)

El Control de Accesos Basado en Roles (RBAC) es una metodología de control de accesos que asigna permisos a los usuarios según su rol dentro de la organización. En lugar de asignar permisos individualmente a cada usuario, se asignan roles, y cada rol tiene un conjunto predeterminado de permisos asociados. Los usuarios reciben acceso a recursos en función del rol que desempeñan, lo que simplifica la gestión y aumenta la seguridad, ya que los permisos son limitados y controlados según las necesidades de cada puesto.

Características del RBAC:

Asignación de Roles: Los usuarios se agrupan en roles, como Administrador, Empleado, Supervisor, etc. Estos roles tienen permisos predefinidos que corresponden a las responsabilidades laborales de cada uno.

Minimización de Privilegios: La asignación de permisos a través de roles asegura que los usuarios solo tengan acceso a los recursos que necesitan para desempeñar sus funciones, lo que reduce el riesgo de acceso no autorizado o uso indebido de información.

Escalabilidad: RBAC es particularmente eficaz en organizaciones grandes donde los roles son bien definidos y los usuarios tienen necesidades de acceso similares dentro de un grupo o departamento.

Ventajas de RBAC:

Simplicidad: Facilita la administración de permisos, ya que se asignan a los roles y no a cada usuario individualmente.

Mejora en la Seguridad: Al asignar permisos según roles y no de forma individual, se reduce el riesgo de otorgar permisos innecesarios a los usuarios.

Cumplimiento de Normativas: RBAC facilita el cumplimiento de normativas de seguridad de la información, como ISO/IEC 27001 (A.9 - Control de acceso).

Desventajas de RBAC:

Rigidez: RBAC puede ser inflexible en situaciones donde las necesidades de acceso de los usuarios cambian con frecuencia o son muy específicas, ya que los permisos están estrictamente definidos por los roles**.**

Control de Accesos Basado en Atributos (ABAC)

El Control de Accesos Basado en Atributos (ABAC) es un enfoque más flexible y dinámico que asigna permisos a los usuarios basándose en atributos de los usuarios, los recursos y el contexto del acceso. En lugar de usar un conjunto predefinido de roles, ABAC permite especificar reglas detalladas que consideran atributos como la ubicación del usuario, la hora del día, el dispositivo que se está utilizando, el nivel de seguridad de la red, entre otros.

Características del ABAC:

Atributos del Usuario: Los permisos se asignan según atributos específicos del usuario, como su cargo, departamento, grupo, etc.

Atributos del Recurso: Los permisos también pueden depender de atributos de los recursos a los que se intenta acceder, como el tipo de datos, la sensibilidad del recurso, etc.

Atributos del Contexto: ABAC permite la toma de decisiones dinámicas basadas en el contexto del acceso, como la hora del día o la ubicación geográfica del usuario.

Reglas y Políticas: ABAC utiliza políticas basadas en reglas que especifican las condiciones bajo las cuales un usuario puede acceder a un recurso. Esto puede incluir reglas

como "un empleado solo puede acceder a los datos de cliente si está en la oficina y es durante el horario laboral".

Ventajas de ABAC:

Mayor Flexibilidad: ABAC permite personalizar las políticas de acceso de manera detallada, lo que lo hace ideal para organizaciones con necesidades complejas de control de accesos.

Adaptabilidad: Debido a su capacidad para considerar múltiples atributos y condiciones contextuales, ABAC puede adaptarse a escenarios en constante cambio o a entornos dinámicos.

Mejor Gestión de Riesgos: Al permitir el control detallado de los accesos según múltiples atributos, ABAC puede ser más efectivo en la gestión de riesgos.

Desventajas de ABAC:

Complejidad: La implementación de ABAC puede ser más compleja que RBAC, ya que requiere la creación y mantenimiento de políticas detalladas y reglas para evaluar atributos.

Mayor Carga Administrativa: Debido a la cantidad de atributos y reglas a gestionar, ABAC puede generar una carga administrativa mayor, especialmente si los atributos o reglas cambian con frecuencia.

Comparativa entre RBAC y ABAC

Tabla 3.

Comparación RBAC vs ABAC

Característica	RBAC	ABAC
Flexibilidad	Limitada a los roles predefinidos	Alta, ya que permite evaluar múltiples atributos y condiciones contextuales.
Simplicidad de Implementación	Relativamente simple y fácil de implementar	Requiere una planificación y mantenimiento detallados.
Escalabilidad	Muy adecuado para organizaciones con roles bien definidos	Ideal para organizaciones con necesidades complejas o dinámicas.

Seguridad	Buen control, pero puede ser inflexible para escenarios complejos	Mejor para entornos dinámicos y escenarios de alta seguridad.
Cumplimiento Normativo	Facilita el cumplimiento de normas como ISO 27001	Puede adaptarse mejor a regulaciones complejas que exigen un control detallado de accesos.

Nota: Tabla comparativa RBAC vs ABAC, la elección entre RBAC y ABAC dependerá de las necesidades específicas de seguridad de la organización.

Gestión de Identidades y Accesos (IAM)

La gestión de identidades y accesos (IAM) es un enfoque integral que garantiza que las personas, sistemas y dispositivos que interactúan con la infraestructura de TI de una empresa tengan los permisos adecuados para acceder a los recursos necesarios, sin comprometer la seguridad ni violar las políticas internas. La gestión de identidades y accesos abarca varios aspectos, entre ellos, la autenticación (verificación de la identidad del usuario), la autorización (determinación de los recursos a los que un usuario puede acceder) y la auditoría (registro y monitoreo de actividades de acceso).

Definición y Principios de Gestión de Identidades y Accesos (IAM)

IAM se refiere al conjunto de políticas, procesos y tecnologías que una organización utiliza para gestionar y asegurar el acceso a sus sistemas y datos. De acuerdo con la definición de ISO/IEC 27001:2013, el control de acceso es uno de los elementos clave de la seguridad de la información y debe ser gestionado adecuadamente para asegurar la confidencialidad, integridad y disponibilidad de los datos (ISO/IEC 27001:2013, Anexo A, A.9). El objetivo principal de la gestión de accesos es asegurar que los usuarios solo tengan acceso a los recursos necesarios para realizar sus tareas, siguiendo el principio de mínimo privilegio.

Componentes Principales del IAM:

Autenticación: Se refiere al proceso de verificar que un usuario o sistema sea quien dice ser. Esto se logra mediante contraseñas, autenticación multifactor (MFA), biometría y otros métodos.

Autorización: Determina qué recursos pueden ser accedidos por un usuario autenticado. Este proceso se basa en roles y políticas que asignan permisos específicos a diferentes usuarios o grupos de usuarios. Es importante que solo se otorguen los privilegios necesarios para realizar las tareas requeridas.

Auditoría y Supervisión: Implica el seguimiento de todas las actividades de acceso para identificar patrones inusuales o posibles incidentes de seguridad. Los registros de auditoría permiten una revisión post-incidente para evaluar la magnitud de las brechas de seguridad.

Revocación de Accesos: El IAM también incluye procesos de revocación de acceso para cuando un empleado ya no necesita acceder a los recursos (por ejemplo, en caso de cambio de rol o salida de la organización). La falta de este control puede llevar a accesos no autorizados y brechas de seguridad.

Normas y Autores Relevantes en IAM:

La ISO/IEC 27001 establece la necesidad de controles de acceso robustos, detallando en el Anexo A (A.9) cómo los accesos deben ser gestionados y monitoreados para reducir riesgos de seguridad. Además, resalta la importancia de revisar regularmente los accesos para asegurar que los usuarios solo tengan acceso a la información necesaria y pertinente a sus funciones.

SO/IEC 27001:2013, "Information technology Security techniques Information security management systems Requirements", es una norma clave que define las políticas de control de acceso y gestión de identidades en el ámbito de la seguridad de la información.

NIST SP 800-53, una publicación del Instituto Nacional de Estándares y Tecnología (NIST), proporciona directrices para establecer políticas y controles de acceso dentro de un sistema de gestión de la seguridad de la información.

Gartner (2020), en su informe sobre gestión de identidades y accesos, resalta la creciente necesidad de implementar soluciones IAM eficientes debido a los crecientes ataques cibernéticos y la complejidad de gestionar identidades en un entorno híbrido de trabajo.

La Importancia de IAM en la Seguridad de la Información

La gestión de identidades y accesos (IAM) es fundamental para prevenir incidentes de seguridad como el fraude interno y las brechas de datos. Según el informe de Gartner (2020), 35% de las brechas de seguridad son causadas por accesos mal gestionados, ya sea por contraseñas débiles, permisos inapropiados o fallos en la revocación de accesos. Además, los ataques internos son responsables del 60% de las fugas de datos en muchas empresas, lo que subraya la importancia de tener un sistema IAM adecuado para mitigar estos riesgos.

Importancia de MFA en la Seguridad de Accesos

La MFA es clave en la seguridad de accesos porque agrega una capa de defensa extra. Incluso si un atacante consigue obtener una contraseña o PIN, necesitaría también el segundo o tercer factor de autenticación para tener acceso a las cuentas o sistemas. Esto hace que sea mucho más difícil para los atacantes comprometer cuentas, especialmente en un entorno de trabajo donde los accesos a sistemas críticos deben ser estrictamente controlados.

La **ISO/IEC 27001**, norma de referencia en la gestión de la seguridad de la información, establece que la autenticación debe ser adecuada para proteger la confidencialidad, integridad y disponibilidad de los activos de información (ISO/IEC 27001:2013, A.9). En particular, el control de acceso debe basarse en una evaluación de riesgos y establecer medidas adecuadas, lo

que incluye la utilización de MFA en escenarios donde se gestionan datos sensibles o de alto valor.

Beneficios de la Autenticación Multifactor (MFA)

Prevención de accesos no autorizados: MFA reduce significativamente la probabilidad de que un atacante logre acceder a un sistema, incluso si ha obtenido las credenciales de acceso de un usuario.

Cumplimiento de normas de seguridad: Muchas regulaciones de privacidad y seguridad de datos, como el Reglamento General de Protección de Datos (GDPR), ISO 27001 o HIPAA, exigen la implementación de MFA para proteger el acceso a sistemas sensibles.

Protección contra ataques de phishing y robo de contraseñas: MFA dificulta que los atacantes puedan utilizar credenciales comprometidas para obtener acceso a los sistemas, incluso si tienen la contraseña correcta.

Mayor control sobre el acceso: Con MFA, los administradores pueden tener un control más fino sobre los usuarios que tienen acceso a sistemas críticos, asegurando que solo los usuarios que hayan completado correctamente los pasos de autenticación sean autorizados.

Comparación de MFA con Métodos Tradicionales de Autenticación

Tabla 4.

Comparación de MFA

Autenticación	Ventajas	Desventajas	Ejemplo
Contraseña tradicional	Fácil de implementar	Susceptible a ataques de fuerza bruta, phishing y robo de contraseñas	Ingreso de contraseña
MFA (Autenticación multifactor)	Aumenta significativamente la seguridad, reduce el riesgo de accesos no autorizados	Requiere hardware adicional o apps de autenticación	Código OTP a través de un teléfono móvil, huella dactilar

Nota: Tabla de comparación de MFA, la implementación de MFA fortalece significativamente la seguridad de los sistemas al requerir múltiples factores de verificación.

Marco Jurídico

Ley Estatutaria 1581 de 2012, la cual tiene como objeto “desarrollar el derecho constitucional que tienen todas las personas a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bases de datos o archivos, y los demás derechos, libertades y garantías constitucionales a que se refiere el artículo 15 de la Constitución Política; así como el derecho a la información consagrado en el artículo 20 de misma.

Aquí observamos Ley Estatutaria 1581 de 2012 nos muestra los principios que se aplicarían para salvaguardar la confidencialidad, integridad y disponibilidad de la información.

Metodología

Para el proyecto de implementación de un sistema de control de accesos en Viamericas, la elección del modelo de desarrollo es crucial para garantizar que el sistema se desarrolle de manera eficiente y cumpla con los requisitos de seguridad y funcionalidad necesarios. A continuación, se detalla el modelo de desarrollo recomendado y cómo se aplicará al proyecto:

Enfoque metodológico

Descripción del Enfoque: Enfoque Mixto

Un enfoque mixto combina métodos cualitativos y cuantitativos para obtener una comprensión completa y rica del problema. Este enfoque permite analizar tanto la experiencia y percepción subjetiva de los usuarios (cualitativo) como los datos objetivos y medibles sobre el sistema y su funcionamiento (cuantitativo).

Métodos Cualitativos:

Entrevistas y Encuestas Cualitativas: Se realizarán entrevistas en profundidad y encuestas abiertas con los usuarios finales, administradores de sistemas y otros stakeholders para comprender sus experiencias, percepciones y desafíos con el sistema de control de accesos actual.

Observación Directa: Se llevará a cabo la observación de cómo los usuarios interactúan con el sistema de gestión de accesos para identificar problemas prácticos y áreas de mejora desde una perspectiva operativa.

Análisis de Casos de Estudio: Se estudiarán casos específicos de problemas relacionados con el control de accesos que hayan ocurrido en la empresa para entender sus causas y consecuencias.

Métodos Cuantitativos:

Análisis de Datos de Uso: Se recopilarán y analizarán datos sobre el uso del sistema de acceso actual, como los registros de accesos, los tiempos de respuesta para la gestión de permisos, y la frecuencia de incidencias de seguridad.

Encuestas Estructuradas: Se utilizarán encuestas estructuradas para recopilar datos estadísticos sobre la satisfacción de los usuarios, la eficacia percibida del sistema y la frecuencia de problemas relacionados con el acceso.

Evaluación de Rendimiento del Sistema: Se medirán indicadores clave de rendimiento (KPIs) del sistema actual, como la tasa de errores en la asignación de permisos y el tiempo requerido para la administración de accesos.

Justificación de la Elección del Enfoque Mixto

El enfoque mixto es ampliamente reconocido por su capacidad para proporcionar una visión más completa de los problemas al integrar datos cualitativos y cuantitativos. Según Creswell y Plano Clark (2017), un enfoque mixto en proyectos como este permite combinar los beneficios de la comprensión profunda que proporcionan los métodos cualitativos (como las entrevistas y las observaciones) con la objetividad y el análisis riguroso que proporcionan los métodos cuantitativos (como los análisis de registros de acceso y las encuestas).

Este enfoque ha sido utilizado en proyectos similares, como el estudio de McKeen y Guimaraes (2003), donde se utilizó un enfoque mixto para mejorar los sistemas de gestión de accesos en empresas de tecnología. El uso combinado de entrevistas con empleados y análisis de datos de acceso permitió no solo identificar los puntos de dolor desde la perspectiva del usuario, sino también obtener datos claros sobre la eficiencia y las fallas del sistema, lo que llevó a una mejora sustancial en la seguridad y la operatividad.

Complejidad del Problema: El problema de control de accesos en Viamericas es complejo, ya que involucra tanto aspectos técnicos (como la seguridad del sistema y la gestión de permisos) como aspectos humanos (como la experiencia del usuario y las percepciones sobre el sistema). El enfoque mixto permite capturar esta complejidad al integrar tanto datos objetivos como subjetivos.

Comprensión Integral:

Perspectiva Cualitativa: Proporciona una comprensión profunda de las experiencias y percepciones de los usuarios, lo cual es esencial para identificar problemas prácticos y mejorar la usabilidad del sistema. Ayuda a entender cómo los usuarios interactúan con el sistema y cuáles son sus principales preocupaciones y necesidades.

Perspectiva Cuantitativa: Ofrece datos concretos y medibles que permiten evaluar la eficacia del sistema actual y medir el impacto de las soluciones propuestas. Permite identificar patrones y tendencias en el uso del sistema y en las incidencias de seguridad.

Mejora del Proceso de Toma de Decisiones: El enfoque mixto facilita una toma de decisiones más informada y fundamentada al proporcionar una visión completa de los problemas y las posibles soluciones. Los datos cualitativos pueden explicar el "por qué" detrás de los problemas identificados a través de datos cuantitativos, y viceversa.

Validación y Prueba de Soluciones: Utilizando un enfoque mixto, es posible probar las soluciones propuestas desde dos perspectivas. Los datos cuantitativos pueden evaluar la eficacia de las soluciones en términos de métricas objetivas, mientras que los datos cualitativos pueden proporcionar retroalimentación sobre la aceptación y la experiencia del usuario con las soluciones implementadas.

Aplicación del Enfoque Mixto al Proyecto

Fase de Investigación Inicial:

Realizar entrevistas y encuestas cualitativas para comprender los problemas actuales y las necesidades de los usuarios.

Recolectar y analizar datos cuantitativos sobre el uso del sistema actual y las incidencias de seguridad.

Desarrollo y Prueba de Soluciones:

Implementar soluciones basadas en los hallazgos cualitativos y cuantitativos.

Monitorear y evaluar la eficacia de las soluciones a través de métricas cuantitativas y retroalimentación cualitativa.

Revisión Continua:

Continuar recopilando datos cualitativos y cuantitativos para realizar ajustes y mejoras continuas en el sistema de control de accesos.

Modelo de Desarrollo: Ágil (Agile)

El enfoque ágil es altamente beneficioso para el proyecto de "Revisión y Redefinición de la Matriz de Accesos para un Sistema Transaccional de una Empresa de Envíos de Dinero", debido a las características de flexibilidad, adaptabilidad y entrega continua de valor que ofrece este marco. A continuación, se profundiza en cómo el enfoque ágil se adapta a las necesidades específicas de este tipo de proyecto, proporcionando ejemplos concretos:

El enfoque ágil permite trabajar en iteraciones cortas (sprints) de manera incremental, lo cual es especialmente útil para un proyecto como la revisión de la matriz de accesos. A medida que se revisan los accesos y se ajustan los permisos, pueden surgir nuevos requerimientos o ajustes necesarios debido a cambios en la normativa, nuevas vulnerabilidades de seguridad o decisiones organizacionales que afectan la estructura de los roles de usuario.

Ejemplo específico: Durante la fase inicial de la revisión de la matriz de accesos, puede surgir la necesidad de rediseñar el acceso de ciertos roles debido a nuevas políticas de seguridad. Con el enfoque ágil, el equipo puede abordar estos cambios en el siguiente sprint, sin afectar el progreso general del proyecto, garantizando así que se mantenga la flexibilidad para adaptarse a nuevas necesidades. (Beck, K., Beedle, M., van Bennekum, A., Cockburn, A., Cunningham, W., Fowler, M., ... & Thomas, D. 2001).

Colaboración Continua entre Equipos Multidisciplinarios

Un aspecto clave del enfoque ágil es la colaboración constante entre diferentes equipos de trabajo. En proyectos de sistemas transaccionales y seguridad, es fundamental la comunicación entre el equipo de desarrollo de software, los responsables de la seguridad, los administradores del sistema y los usuarios finales. El trabajo conjunto asegura que las modificaciones a la matriz de accesos sean viables tanto desde el punto de vista técnico como operativo, alineándose con los objetivos de negocio.

Ejemplo específico: En este tipo de proyecto, las pruebas de accesos se pueden realizar de manera iterativa, y los cambios se validan con los equipos de seguridad y operaciones después de cada sprint. La retroalimentación constante entre estos equipos puede identificar problemas de accesos erróneos o inconsistentes en tiempo real, permitiendo que se solucionen antes de que se completen las iteraciones finales. (Highsmith, J. ,2002).

Priorización de Tareas y Resolución de Riesgos

La metodología ágil facilita la gestión de riesgos y la priorización de tareas. En un proyecto relacionado con la seguridad de los accesos a un sistema transaccional, los riesgos asociados a accesos incorrectos o mal configurados pueden tener consecuencias graves, como

fraudes o pérdida de datos. El enfoque ágil permite identificar y abordar estos riesgos de manera temprana y constante durante todo el proceso.

Ejemplo específico: Durante los primeros sprints, el equipo puede identificar que un grupo de usuarios tiene acceso a datos más sensibles de lo que se requiere. Este riesgo puede ser priorizado y solucionado rápidamente en el siguiente ciclo de trabajo, sin esperar a la fase final del proyecto. La revisión continua de los accesos y su categorización en cada iteración permite mitigar estos riesgos antes de que se conviertan en problemas mayores. (Schwaber, K., & Sutherland, J. 2017).

Transparencia y Visibilidad

La naturaleza del enfoque ágil permite una mayor transparencia y visibilidad del progreso del proyecto, lo que es clave en proyectos de revisión y redefinición de accesos. Con reuniones diarias (stand-ups), revisiones de sprint y demostraciones de los avances, todas las partes interesadas, incluidos los responsables de seguridad, pueden estar al tanto del progreso en tiempo real y proporcionar feedback inmediato.

Ejemplo específico: Al final de cada sprint, el equipo puede presentar un informe sobre los cambios implementados en la matriz de accesos y su impacto en la seguridad y la funcionalidad del sistema. Esta visibilidad continua permite que los stakeholders ajusten sus expectativas o proporcionen comentarios en tiempo real, lo que aumenta la eficiencia y la alineación entre los objetivos del negocio y los resultados del proyecto. (Highsmith, J. 2002).

Reducción de Riesgos Mediante Entregas Incrementales

El enfoque ágil favorece la entrega continua de valor mediante entregas incrementales. Este aspecto es fundamental en proyectos de seguridad, como la revisión de una matriz de accesos, donde cada entrega parcial puede incluir mejoras en la seguridad o ajustes en la

estructura de accesos. Las entregas incrementales permiten detectar y corregir problemas de manera temprana, antes de que se conviertan en riesgos mayores.

Ejemplo específico: Al final de cada sprint, el equipo podría entregar una actualización de la matriz de accesos revisada con un conjunto específico de permisos ajustados o roles modificados. Estos cambios podrían ser probados en entornos de desarrollo o pruebas, asegurando que el sistema de acceso se alinee con los requerimientos de seguridad en todo momento. (Beck, K., Beedle, M., van Bennekum, A., Cockburn, A., Cunningham, W., Fowler, M., ... & Thomas, D. (2001).

Mejora Continua a Través de la Retroalimentación

En el enfoque ágil, la mejora continua es un principio clave. Cada iteración proporciona la oportunidad de ajustar y optimizar los procesos y resultados. Este aspecto es esencial en un proyecto de redefinición de accesos, donde los cambios pueden generar nuevas necesidades de ajuste conforme se descubren problemas o se identifican oportunidades de mejora.

Ejemplo específico: Después de cada revisión del sprint, el equipo recibe retroalimentación sobre la calidad y seguridad de los cambios realizados en la matriz de accesos. Esto permite que se realicen ajustes constantes en la forma en que se gestionan los permisos, asegurando que el sistema evolucione en función de las necesidades cambiantes del negocio. (Schwaber, K., & Sutherland, J. 2017).

Aplicación del Modelo Ágil al Proyecto

Fase de Planificación Inicial

Definición de Requisitos y Objetivos: Se realizará una reunión inicial con los stakeholders de Viamericas para definir los requisitos básicos del sistema de control de accesos.

Esto incluirá identificar las necesidades de seguridad, los tipos de permisos necesarios y los flujos de trabajo de los usuarios.

Creación de un Product Backlog: Se creará una lista priorizada de funcionalidades y mejoras deseadas, conocida como el Product Backlog. Esto incluirá historias de usuario relacionadas con la gestión de accesos, la seguridad, la auditoría y el cumplimiento normativo.

Desarrollo Iterativo

Sprints que Estiman para completar el proyecto: El proyecto se dividirá en ciclos de desarrollo cortos Para este proyecto específico, se estima que se necesitarán entre 5 y 7 Sprints para completar la redefinición de la matriz de accesos, dependiendo de la complejidad de los requisitos y las pruebas que se necesiten realizar.

Sprint 1-2: Revisión inicial de la matriz de accesos actual, identificación de brechas y requerimientos iniciales. Aquí se definirá la arquitectura de la nueva matriz de accesos.

Sprint 3-4: Implementación de los primeros cambios en la matriz, incluyendo la integración con la herramienta de gestión de accesos seleccionada (como Duo), y configuración inicial.

Sprint 5-6: Pruebas y ajustes de seguridad, además de la implementación de la nueva estructura de permisos.

Sprint 7: Revisión final y puesta en marcha de la nueva matriz de accesos, ajustes de última hora y formación a los usuarios finales.

Medición del Éxito de Cada Sprint: El éxito de cada Sprint se medirá en

Cumplimiento de los Objetivos del Sprint: El equipo de Scrum establecerá objetivos claros al inicio de cada Sprint. Si estos objetivos se completan, el Sprint será considerado

exitoso. Esto incluye la entrega de funcionalidades completas y operativas que son acordadas previamente.

Definición de Hecho (DoD): Según el marco ágil, cada funcionalidad debe cumplir con los criterios de "Definición de Hecho" (DoD) para ser considerada completa. Esto incluye pruebas unitarias, revisión de código, y validación de que la funcionalidad cumple con los requisitos establecidos.

Retroalimentación de los Stakeholders: Durante las reuniones de revisión del Sprint (Sprint Review), los stakeholders clave (tales como los responsables de seguridad y usuarios del sistema) proporcionarán retroalimentación sobre la funcionalidad entregada. La satisfacción de los stakeholders es una métrica crítica de éxito.

Resolución de Problemas: Se evaluará la capacidad del equipo para abordar y resolver cualquier impedimento o problema durante el Sprint, y cuán rápidamente se solucionan las incidencias.

Cumplimiento de Tiempo y Presupuesto: El seguimiento de los plazos de entrega y la gestión eficiente de los recursos son componentes clave para medir el éxito del Sprint.

Testing y Validación Continua

Participación de Usuarios Finales en las Pruebas: Uno de los principios fundamentales del enfoque ágil es la colaboración continua con los usuarios finales para asegurar que las funcionalidades desarrolladas cumplen con sus expectativas y necesidades. En este sentido:

Usuarios Finales Participantes: Durante las fases clave del proyecto, los usuarios finales estarán involucrados en las pruebas de aceptación. Esto incluye, pero no se limita a, miembros del equipo de soporte técnico, operaciones, gestión de accesos y otros roles de seguridad. La

participación de estos usuarios en las pruebas de aceptación de usuario (UAT) garantizará que la nueva matriz de accesos cumpla con los requerimientos operacionales y de seguridad.

Pruebas de Aceptación de Usuario (UAT): Al final de cada Sprint, los usuarios finales podrán interactuar con las funcionalidades entregadas y proporcionar retroalimentación. Las pruebas se realizarán en un ambiente controlado para garantizar que no haya efectos adversos en los sistemas existentes.

Implementación y Despliegue

Despliegue Gradual: El sistema se implementará en fases para minimizar riesgos. Inicialmente, se desplegará una versión piloto en un entorno de prueba o en una parte del sistema. Después de verificar su estabilidad y funcionalidad, se procederá al despliegue completo.

Capacitación y Soporte: Se proporcionará capacitación a los usuarios y al personal de administración del sistema. Se establecerá un soporte técnico para resolver cualquier problema que pueda surgir durante y después del despliegue.

Mantenimiento y Mejora Continua

Actualizaciones y Mejoras: Después del despliegue, el sistema seguirá siendo mejorado con base en la retroalimentación continua de los usuarios y en la evolución de las necesidades de seguridad. Los sprints adicionales se utilizarán para implementar nuevas funcionalidades, ajustes y correcciones.

Monitoreo y Evaluación: Se llevará a cabo un monitoreo continuo del sistema para asegurar su correcto funcionamiento y su capacidad para responder a nuevos desafíos de seguridad.

Criterios de Aceptación para la Funcionalidad

El éxito del proyecto depende en gran medida de la calidad de las funcionalidades entregadas en cada Sprint. Por lo tanto, es crucial establecer criterios de aceptación claros y detallados para cada funcionalidad clave relacionada con la nueva matriz de accesos. Algunos ejemplos de criterios de aceptación para la matriz de accesos podrían incluir:

Tabla 5.

Criterios de aceptación

Criterios	Criterio	Criterio de Aceptación
Gestión de Roles y Permisos	Los roles y permisos deben ser configurables de acuerdo con las políticas de seguridad de la organización.	La herramienta debe permitir la asignación de permisos de manera eficiente según los roles establecidos y debe auditar cualquier cambio realizado.
Autenticación Multifactor (MFA)	Los usuarios deben ser requeridos a autenticarse mediante al menos dos factores de autenticación.	La funcionalidad debe permitir que el proceso de MFA sea aplicable a todos los usuarios que accedan a información sensible, y debe integrarse sin problemas con el sistema de gestión de identidades.
Auditoría y Registro de Accesos	La herramienta debe registrar todos los accesos y cambios de permisos.	El sistema debe generar registros detallados accesibles para su revisión periódica. Los informes deben incluir la identificación del usuario, la fecha y hora de acceso y las acciones realizadas.
Integración con Herramientas Existentes	La nueva matriz de accesos debe integrarse correctamente con las herramientas de seguridad ya existentes, como Duo.	El sistema debe permitir la autenticación y gestión de accesos sin afectar la funcionalidad de los sistemas existentes.

Note: Tabla criterios de aceptación, Los criterios de aceptación definen las condiciones mínimas que debe cumplir una funcionalidad para ser considerada completa

Fases del Proyecto

Análisis de Requisitos

Para desarrollar un sistema de control de accesos efectivo en Viamericas, es fundamental realizar un análisis exhaustivo de los requisitos del sistema. Este análisis debe incluir la recopilación de información de diversas fuentes y el uso de múltiples métodos para garantizar que se aborden todas las necesidades y preocupaciones relacionadas con el control de accesos y la seguridad de los datos. A continuación, se detalla cómo se recopilarán y analizarán los requisitos del sistema:

Tabla 6.

Recopilación de requisitos

RECOPILACIONN DE REQUISITOS			
	Objetivo	Método	Participantes
Entrevistas	Obtener información detallada y específica de los stakeholders clave, incluidos usuarios finales, administradores del sistema y responsables de seguridad de TI.	Realizar entrevistas individuales y grupales. Preparar un conjunto de preguntas abiertas y específicas que exploren: Necesidades y expectativas en cuanto al control de accesos. Problemas y limitaciones del sistema actual. Requisitos específicos de seguridad y cumplimiento. Documentar las respuestas y observar el contexto para identificar temas recurrentes y necesidades no expresadas explícitamente.	Usuarios finales que interactúan regularmente con el sistema. Administradores y personal de TI responsables de la configuración y gestión de accesos. Responsables de cumplimiento y seguridad.
Cuestionarios	Recopilar datos cuantitativos y cualitativos de un grupo más amplio de usuarios para obtener una visión general de las percepciones y necesidades relacionadas con el control de accesos.	Diseñar cuestionarios estructurados con preguntas de opción múltiple, escalas de Likert y preguntas abiertas. Incluir secciones sobre: Usabilidad del sistema actual, nivel de satisfacción con la gestión de accesos, identificación de problemas comunes y necesidades no satisfechas.	Personal que utiliza el sistema de control de accesos en su trabajo diario. Administradores de sistemas y usuarios de diferentes niveles y departamentos.

		Distribuir el cuestionario a una muestra representativa de usuarios y personal involucrado en la gestión de accesos.	

	Objetivo	Metodo	Documentos a Revisar
Revisión de Documentación	Revisar documentos existentes para comprender el contexto actual del sistema de control de accesos y los requisitos de seguridad y cumplimiento.	Examinar documentación técnica y de procesos relacionados con el sistema actual, incluidos manuales de usuario, procedimientos operativos estándar (SOPs) y políticas de seguridad. Revisar informes de auditoría previos, registros de incidentes de seguridad y documentación de cambios en el sistema.	Manuales del sistema de control de accesos actual. Políticas de seguridad y acceso. Registros de incidentes y problemas de seguridad. Documentación de auditorías anteriores.

	Objetivo	Método	Áreas de Observación
Observación Directa	Observar cómo los usuarios interactúan con el sistema de control de accesos para identificar problemas prácticos y áreas de mejora.	Realizar sesiones de observación en el lugar de trabajo donde los usuarios utilizan el sistema. Documentar cómo los usuarios gestionan permisos, acceden a datos y enfrentan problemas. Identificar cuellos de botella, dificultades y flujos de trabajo ineficientes.	Proceso de solicitud y aprobación de permisos. Uso diario del sistema por parte de los usuarios. Gestión de accesos por parte del personal administrativo.

	Objetivo	Metodo	Casos a Estudiar
Análisis de Casos de Estudio	Analizar casos específicos de problemas relacionados con el control de accesos para comprender mejor los desafíos y las implicaciones.	-Recopilar y estudiar casos de incidentes de seguridad, errores de permisos y violaciones de datos. -Realizar entrevistas con personas involucradas en estos casos para obtener detalles adicionales y lecciones aprendidas.	-Incidentes de acceso no autorizado. -Problemas de configuración de permisos que afectaron la operación. -Casos de violaciones de seguridad y sus impactos.

Nota: La recopilación de requisitos es clave para asegurar que el sistema cumpla con las necesidades y expectativas del usuario final.

Tabla 7.

Análisis de Requisitos

Análisis de Requisitos				
	Método	Herramientas	Criterios de Priorización	Participantes
Organización y Consolidación de Datos	Agrupar los datos recopilados de entrevistas, cuestionarios, revisión de documentación y	Utilizar herramientas de análisis cualitativo (como software de análisis de datos cualitativos) para		

	observación en categorías temáticas. -Identificar patrones y temas recurrentes para construir una imagen coherente de los requisitos y problemas.	categorizar y codificar datos cualitativos. -Analizar datos cuantitativos con herramientas estadísticas para identificar tendencias y áreas de preocupación.		
Priorización de Requisitos	-Evaluar los requisitos en función de su impacto en la seguridad, la eficiencia operativa y la satisfacción del usuario. - Utilizar métodos como el análisis de impacto y la matriz de priorización para clasificar los requisitos según su importancia y urgencia.		-Riesgo de seguridad. -Necesidades críticas de los usuarios. -Requisitos regulatorios y de cumplimiento.	
Validación de Requisitos	-Revisar los requisitos recopilados con los stakeholders clave para asegurar que reflejan adecuadamente sus necesidades y expectativas. -Realizar sesiones de validación para confirmar que los requisitos son claros, completos y viables.			-Usuarios finales. -Administradores del sistema. -Personal de seguridad y cumplimiento.

Nota: Análisis y recopilación de requisitos, el análisis de requisitos permite identificar, refinar y validar las necesidades del proyecto para asegurar una solución coherente y viable.

Diseño del Sistema

Tabla 8.

Diseño del Sistema

Diseño de la Matriz de Accesos				
La matriz de accesos es una herramienta que define quién tiene acceso a qué recursos y qué tipo de acceso tienen. Es esencial para asegurar que los permisos sean otorgados correctamente y que el acceso a la información se controle de manera efectiva.				
Recolección de Información para la Matriz de Accesos		Diseño de la Matriz de Accesos		
Identificación de Recursos y Datos:	Definición de Roles y Permisos	Estructura de la Matriz	Definición de Reglas de Acceso	Documentación y Aprobación
Inventario de Recursos: Identificar todos los recursos y datos que	-Roles de Usuario: Definir roles basados en las funciones y responsabilidades dentro de la empresa.	Filas y Columnas: Las filas representarán los roles de usuario, mientras que las	Reglas de Control de Acceso: Establecer reglas claras sobre cómo se asignan y	-Documentación: Documentar la matriz de accesos y las reglas de control de acceso.

necesitan protección. Esto incluye bases de datos, aplicaciones, sistemas de archivos, y otros recursos sensibles. Clasificación de Datos: Clasificar los datos según su sensibilidad y nivel de protección requerido (por ejemplo, datos personales, datos financieros, información confidencial).	Ejemplos de roles incluyen Administrador, Usuario de TI, Usuario Final, Auditor, etc. -Permisos Asociados: Determinar qué permisos están asociados con cada rol. Los permisos pueden incluir lectura, escritura, eliminación, y administración de datos o recursos.	columnas representarán los recursos y datos. Cada celda de la matriz indicará los permisos asignados a cada rol sobre cada recurso. Formato: La matriz se puede diseñar en formato de tabla, utilizando herramientas como hojas de cálculo (Excel, Google Sheets) o software especializado en gestión de accesos.	revocan permisos. Esto incluye políticas de mínimos privilegios (los usuarios tienen solo los permisos necesarios para realizar su trabajo) y separación de funciones (segregar funciones críticas para evitar conflictos de interés).	-Aprobación: Revisar y obtener la aprobación de los stakeholders clave, incluidos los responsables de seguridad y gestión de TI, para asegurar que la matriz de accesos cumpla con los requisitos de seguridad y operativos.

Nota: a tabla de diseño del sistema presenta de forma estructurada los principales componentes del sistema

Tabla 9.

Diseño del Sistema de Monitoreo y Control

Diseño del Sistema de Monitoreo y Control							
El sistema de monitoreo y control es esencial para supervisar el acceso a los recursos y detectar actividades sospechosas. Incluye mecanismos para registrar, auditar y alertar sobre eventos relacionados con el acceso.							
Componentes del Sistema de Monitoreo y Control			Diseño del Sistema de Monitoreo			Capacitación y Procedimientos	
Registro de Actividades (Logging)	Herramientas de Monitoreo	Auditoría de Accesos	Definición de Requisitos	Integración con Sistemas Existentes	Configuración y Personalización	Capacitación del Personal	Procedimientos Operativos
Eventos a Registrar: Definir los tipos de eventos que se deben registrar, como accesos exitosos y fallidos, cambios en permisos, y actividades administrativas.	-Software de Monitoreo: Implementar herramientas de monitoreo y gestión de eventos, como sistemas de gestión de información y eventos de seguridad	Auditorías Programadas: Establecer procedimientos para realizar auditorías periódicas de los registros de acceso para verificar el cumplimiento de las políticas de seguridad y	Requisitos de Monitoreo: Identificar los requisitos específicos de monitoreo basados en los riesgos de seguridad, los requisitos de	Integración de Datos: Asegurar que el sistema de monitoreo se integre con otros sistemas y aplicaciones existentes para centralizar la recopilación y el análisis de datos.	Configuración de Parámetros: Configurar los parámetros del sistema de monitoreo, como las reglas de alerta, los umbrales de eventos y los métodos de reporte.	Entrenamiento: Proporcionar capacitación al personal sobre el uso del sistema de monitoreo y control, incluyendo cómo interpretar los registros y	Procedimientos de Respuesta: Desarrollar y documentar procedimientos operativos para responder a incidentes detectados por el sistema de monitoreo.

Formato de Registros: Establecer el formato y nivel de detalle de los registros para asegurar que proporcione la información necesaria para auditorías y análisis.	(SIEM), para recopilar y analizar registros en tiempo real. -Alertas y Notificaciones: Configurar alertas para notificar a los administradores sobre eventos críticos, como intentos de acceso no autorizado o cambios inesperados en permisos.	detectar posibles problemas. -Informes de Auditoría: Generar informes de auditoría detallados para revisar el acceso a los recursos, identificar tendencias y posibles riesgos de seguridad.	cumplimiento y las necesidades operativas.	Compatibilidad: Verificar que las herramientas de monitoreo sean compatibles con la infraestructura de TI actual y con las tecnologías utilizadas en Viamericas.	Personalización: Personalizar las herramientas de monitoreo para adaptarse a las necesidades específicas de Viamericas y garantizar que se adapten a los flujos de trabajo y políticas de seguridad de la empresa.	responder a alertas.	Mantenimiento: Establecer procedimientos para el mantenimiento y actualización continua del sistema de monitoreo y control.

Nota: Tabla Diseño del Sistema de Monitoreo y Control, resume los componentes esenciales del Sistema de Monitoreo y Control, detallando su función principal y la interacción entre ellos

Esquema para la redefinición de la matriz de accesos

La matriz de accesos es una herramienta esencial para gestionar quién tiene acceso a qué recursos en un sistema, asegurando que los usuarios solo puedan realizar acciones que correspondan a sus roles y responsabilidades. El objetivo principal de esta redefinición es mejorar la seguridad, garantizar el cumplimiento de normativas y optimizar el uso de los recursos del sistema.

Análisis de Roles y Permisos Actuales

Tabla 10.

Análisis de Roles y Permisos

Roles y permisos		
Rol	Acceso a Recursos	Acciones Permitidas

Administrador	Bases de datos, Panel de administración	Crear/Modificar/Eliminar usuarios, gestionar transacciones
Agente de atención	Registro de clientes, Panel de consultas	Consultar transacciones, modificar datos de clientes
Supervisor	Informes de transacciones, Historial de actividades	Ver informes, aprobar transacciones
Usuario regular	Cuenta propia, Información básica de transacciones	Consultar saldo, realizar transacciones

Nota: Tabla de roles y permisos, la tabla define los roles del sistema y los permisos asociados a cada uno, asegurando un control de acceso adecuado

Redefinición de la Matriz de Accesos

Tiempo Actual de Gestión de Permisos y Reducción Esperada

Actualmente, el proceso de gestión de permisos en el sistema transaccional requiere una intervención manual significativa, lo que resulta en tiempos prolongados para asignar y modificar accesos. En promedio, el tiempo actual de gestión de permisos es de 7 a 13 días laborales, dependiendo de la complejidad de los roles y el número de solicitudes. Esta demora puede afectar la eficiencia operativa y retrasar la habilitación de nuevos empleados o cambios necesarios en los permisos de acceso.

Con la redefinición de la matriz de accesos y la implementación de un sistema más automatizado y alineado con los principios de la ISO 27001, se espera reducir este tiempo a menos de 1 día laboral por solicitud. La automatización de la asignación de accesos y la integración de políticas claras permitirán acelerar los procesos y reducir los tiempos de espera, mejorando la eficiencia y la capacidad de respuesta a las necesidades operativas.

Nivel de Error en la Asignación de Accesos y Mejora Esperada

Actualmente, el nivel de error en la asignación de accesos es un desafío significativo. Se estima que alrededor del 15-20% de las solicitudes de acceso contienen errores, ya sea por la asignación incorrecta de roles, permisos insuficientes o acceso indebido a información sensible.

Estos errores no solo generan riesgos de seguridad, sino que también requieren tiempo adicional para ser corregidos, lo que impacta la productividad de los equipos y compromete la seguridad general del sistema.

Con la redefinición de la matriz de accesos y la implementación de un sistema más robusto y automatizado, se espera reducir el nivel de error a menos del 5%, minimizando la posibilidad de asignaciones incorrectas. Esto se logrará mediante la integración de controles automáticos que validen los permisos y roles en tiempo real, así como la actualización constante de las políticas de acceso, lo que permitirá una mayor precisión en la asignación de accesos.

Pasos del Proceso de Redefinición

Evaluación de Roles y Necesidades:

Revisión de las responsabilidades de los usuarios.

Redefinir roles y accesos, eliminando permisos innecesarios.

Asignación de Permisos según el Principio de "Menor Privilegio":

Asegurar que los usuarios solo tengan los permisos estrictamente necesarios para cumplir con su función.

Ajustes de Seguridad:

Implementar acceso basado en tiempo (e.g., permisos solo durante ciertas horas).

Añadir autenticación multi-factor para ciertos roles sensibles.

Revisión y Aprobación:

Validación de la nueva matriz con todas las partes interesadas.

Aprobación por parte del equipo de seguridad. Nueva Matriz de Accesos

Tabla 11.

Matriz de Acceso

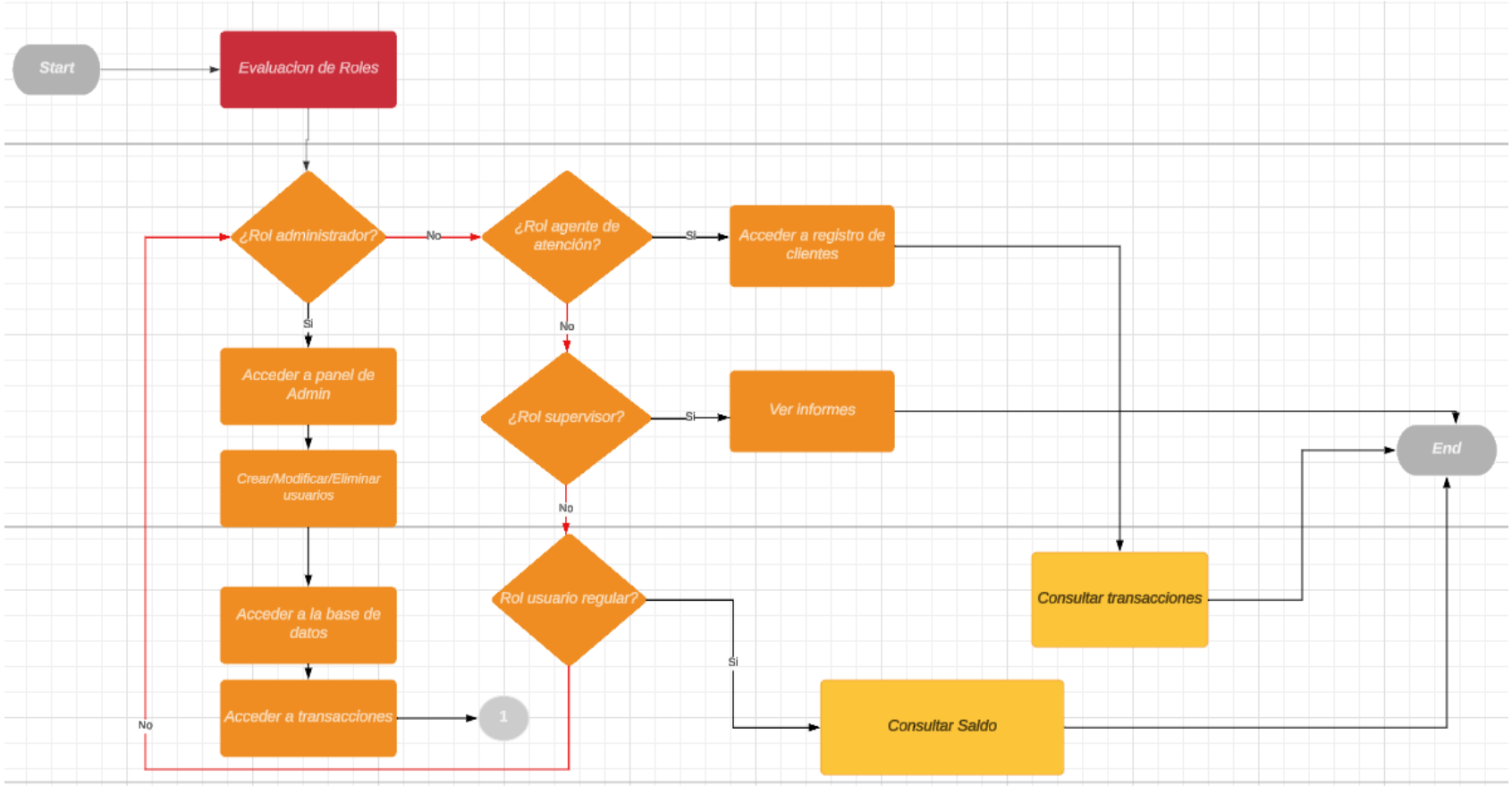
Rol	Acceso a Recursos	Acciones Permitidas
Administrador	Bases de datos, panel de administración, reportes	Crear/Modificar/Eliminar usuarios, gestionar transacciones
Agente de atención	Panel de consultas, registro de clientes	Consultar y modificar datos de clientes, consultar transacciones
Supervisor	Informes de transacciones, historial de actividades	Aprobar transacciones, ver informes
Usuario regular	Cuenta propia, Información básica de transacciones	Consultar saldo, realizar transacciones

Nota: Tabla de matriz de accesos

Figura de Flujo de Acceso y Roles

Figura 1.

Diagrama de Flujo Accesos y Roles



Nota : Diagrama del flujo de accesos y roles, el diagrama de flujo ilustra cómo los usuarios acceden a diferentes partes del sistema según su rol.

Prototipo de Interfaz: Gestión de Roles y Permisos

El prototipo de interfaz de gestión de roles y permisos debe ser intuitivo para los administradores del sistema, permitiéndoles asignar, modificar y visualizar los permisos asociados a cada rol de usuario dentro de un sistema transaccional.

Pantalla Principal de Gestión de Roles:

La pantalla principal permitirá a los administradores ver todos los roles de usuario definidos en el sistema, así como los recursos y permisos asociados a cada rol.

Elementos de la pantalla:

Lista de roles: Muestra todos los roles de usuario disponibles (Administrador, Agente, Supervisor, Usuario Regular).

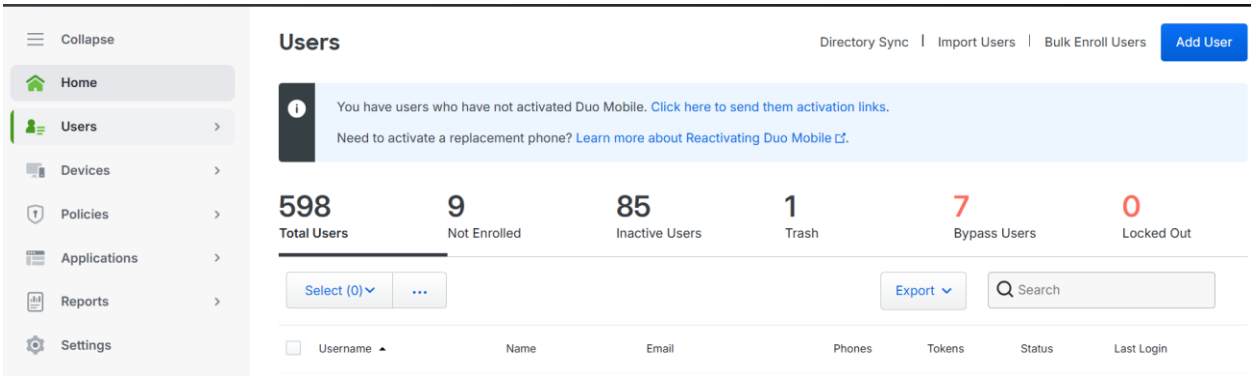
Botones de acción: Para agregar, editar o eliminar roles.

Filtro de búsqueda: Permite buscar roles específicos.

Columnas: Nombre de user, descripción, email, permisos asignados, status

Grafica 1.

Interfaz de Plataforma DUO



Nota: Interfaz gráfica de plataforma Duo, se observa total de usuarios registrados

Estructura de Permisos

La estructura de permisos define qué usuarios pueden acceder a qué recursos dentro del sistema, asegurando que cada rol tenga acceso a solo aquellos recursos que son necesarios para realizar sus funciones. Este enfoque sigue el principio de "menor privilegio", garantizando que cada usuario tenga los permisos más limitados posibles según su rol.

Estructura de Permisos de Acceso por Rol:

Tabla 12.

Estructura de Permisos

Rol	Acceso a Recursos	Permisos Permitidos
Administrador	Base de Datos, Panel de Administración, Transacciones, Reportes	Leer, Escribir, Modificar, Eliminar en todos los recursos
Agente de Atención	Registro de Clientes, Consultas de Transacciones	Leer, Modificar datos de clientes, Consultar transacciones
Supervisor	Reportes, Historial de Actividades	Leer Reportes, Aprobar Transacciones
Usuario Regular	Cuenta Propia, Información Básica de Transacciones	Leer Saldo, Realizar Transacciones

Nota: Estructura de permisos, con rol permisos y recurso, presenta la estructura de permisos asignados a cada rol del sistema, detallando las acciones y niveles de acceso permitidos.

Administrador: Este rol tiene acceso completo a todos los recursos del sistema. Puede leer, escribir, modificar o eliminar información en las bases de datos, el panel de administración, los registros de clientes, etc.

Agente de Atención: Tiene acceso limitado a los registros de clientes y la capacidad de consultar o modificar datos de clientes. No tiene acceso a configuraciones del sistema ni a transacciones de otros usuarios.

Supervisor: Este rol puede revisar los reportes y supervisar las actividades, pero no tiene acceso para modificar las bases de datos o crear usuarios. Puede aprobar transacciones realizadas por otros agentes.

Usuario Regular: Solo tiene acceso a su propia cuenta y puede realizar transacciones básicas como consultar su saldo o hacer transferencias.

Fases del Proyecto

Instrumentos y Técnicas

Para el desarrollo e implementación de un sistema de control de accesos para la empresa Viamericas, utilizando Duo Mobile y otras herramientas de seguridad, es esencial seleccionar las herramientas de software, lenguajes de programación y plataformas adecuadas.

Herramientas de Desarrollo

Duo para la Gestión de Accesos: Justificación de la Herramienta

Se ha mencionado que se utilizará **Duo** como la herramienta principal para la gestión de accesos en el sistema transaccional. A continuación, se detalla por qué esta herramienta ha sido seleccionada frente a otras opciones disponibles en el mercado, como Microsoft Azure AD, Okta o RSA SecurID.

Facilidad de Implementación y Uso:

Una de las principales razones por las que Duo se ha seleccionado es por su simplicidad en la implementación y su experiencia de usuario intuitiva. Según un informe de Gartner (2020), Duo ha sido clasificado como líder en el sector de gestión de accesos debido a su facilidad de integración con sistemas ya existentes y su enfoque en la autenticación multifactor (MFA). Esto reduce la carga operativa y los costos asociados con la configuración y mantenimiento del sistema.

Seguridad Avanzada:

Duo ofrece una capa adicional de seguridad mediante su solución de autenticación multifactor (MFA), lo que aumenta la protección frente a accesos no autorizados. La herramienta es especialmente efectiva para proteger las identidades de los usuarios, que es uno de los puntos más vulnerables en los sistemas de TI. En comparación con RSA SecurID y Microsoft Azure

AD, que también ofrecen soluciones MFA, Duo ha demostrado ser más adaptable a diferentes tipos de dispositivos y entornos, permitiendo una gestión de accesos más dinámica y escalable. Según el Informe de Seguridad de Duo (2021), más del 90% de las empresas que implementan Duo reportan una reducción significativa en los incidentes de acceso no autorizado.

Compatibilidad y Escalabilidad:

Duo se integra fácilmente con una amplia variedad de aplicaciones y sistemas, independientemente de la infraestructura tecnológica existente. Esto la convierte en una opción ideal para empresas que utilizan diferentes plataformas y que necesitan una solución de seguridad unificada. En contraste, herramientas como Microsoft Azure AD y Okta pueden requerir una mayor personalización y esfuerzo de integración, lo que podría aumentar los costos y el tiempo de implementación.

Cumplimiento con Normativas de Seguridad:

Duo también cumple con diversas normativas internacionales de seguridad, como la ISO 27001, GDPR y PCI-DSS, lo que lo convierte en una opción sólida para proteger información sensible en el sector financiero, como es el caso de Viamericas. Esto asegura que, al utilizar Duo, se mantendrán los estándares requeridos para el manejo de datos personales y transacciones financieras (como se muestra en la tabla normativa con la solución propuesta pag.28)

El **GDPR** establece que las empresas deben garantizar que los datos personales sean tratados de manera segura y accesible solo por las personas autorizadas.

La **normativa PCI-DSS** regula el almacenamiento, procesamiento y transmisión de datos de tarjetas de pago (datos financieros).

A continuación, se muestra tabla comparativa con ventajas y desventajas de las soluciones actuales:

Tabla Comparativa: Soluciones de Gestión de Accesos

Tabla 13.

Tabla comparativa

Características	Duo	Microsoft Azure AD	Okta	RSA SecurID
Facilidad de Implementación	Alta: Fácil de integrar y configurar en sistemas existentes.	Moderada: Puede requerir más tiempo de configuración y personalización.	Moderada: Requiere configuración detallada para integraciones.	Baja: Requiere configuraciones complejas y mantenimiento continuo.
Compatibilidad Multiplataforma	Alta: Funciona en diversos dispositivos (móviles, web, sistemas operativos).	Alta: Compatible con plataformas Microsoft y otros servicios en la nube.	Alta: Soporta una amplia gama de aplicaciones y dispositivos.	Moderada: Limitada en algunos dispositivos y plataformas.
Autenticación Multifactor (MFA)	Sí: MFA avanzado y opciones de autenticación biométrica.	Sí: MFA incluido, pero depende de la suscripción y la configuración.	Sí: MFA disponible, pero requiere integraciones adicionales.	Sí: MFA, pero con opciones más limitadas en comparación.
Escalabilidad	Alta: Fácil de escalar sin afectar la operación.	Alta: Ideal para empresas grandes con infraestructura de Microsoft.	Alta: Escalable para grandes organizaciones.	Baja: Requiere ajustes continuos para escalar en grandes empresas.
Seguridad	Alta: Alta protección mediante MFA y políticas adaptables.	Alta: Buena seguridad, pero depende de la configuración y el plan.	Alta: Seguridad robusta, pero más compleja de configurar.	Alta: Fuerte seguridad, pero menos flexible en comparación.
Costos	Moderados: Precios competitivos y flexibles según el tamaño de la empresa.	Alta: Costo elevado, especialmente para empresas que no usan toda la infraestructura de Microsoft.	Alta: Costos variables dependiendo del número de usuarios y configuraciones.	Moderados: Costo por licencia, con mantenimiento adicional.
Cumplimiento Normativo	Cumple con ISO 27001, GDPR, PCI-DSS, entre otros.	Cumple con estándares como ISO 27001, pero requiere	Cumple con normas de seguridad, pero más complejo en su aplicación.	Cumple con normativas, pero su enfoque está más en

		configuraciones específicas.		autenticación tradicional.
Soporte y Actualizaciones	Excelente: Soporte 24/7 y actualizaciones regulares.	Bueno: Soporte amplio, pero dependiente de las suscripciones de Microsoft.	Excelente: Soporte 24/7, actualizaciones frecuentes.	Moderado: Soporte limitado, especialmente en versiones más antiguas.

Nota: Tabla comparativa, soluciones de gestión de accesos, resume las principales características y ventajas de diferentes soluciones de gestión de accesos.

Herramientas de Autenticación y Control de Accesos

Duo Mobile:

Descripción: Aplicación para autenticación multifactor (MFA) que proporciona métodos de verificación adicionales para asegurar la identidad del usuario.

Uso: Autenticación push, códigos de un solo uso (TOTP), y gestión de dispositivos.

Azure Active Directory (AD):

Descripción: Servicios de gestión de identidades y acceso (IAM) para la integración con el sistema de control de accesos.

Uso: Gestión de usuarios, autenticación única (SSO), y sincronización de directorios.

Lenguajes de Programación

Python:

Descripción: Lenguaje de programación versátil usado para scripts de automatización y desarrollo de backend.

Uso: Desarrollo de scripts de backend, automatización de tareas y pruebas.

Plataformas y Entornos

Plataformas en la Nube: AWS / Microsoft Azure / Google Cloud Platform

Descripción: Proveedores de servicios en la nube que ofrecen infraestructura como servicio (IaaS), plataformas como servicio (PaaS) y soluciones de seguridad.

Uso: Hospedaje de servidores, almacenamiento de datos, y servicios de autenticación y autorización.

Sistemas Operativos: Linux (Ubuntu, CentOS):

Descripción: Sistemas operativos utilizados en servidores y entornos de producción.

Uso: Hospedaje de aplicaciones y servicios.

Windows Server:

Descripción: Sistema operativo para servidores que puede ser utilizado en entornos corporativos.

Uso: Hospedaje de aplicaciones empresariales y servicios de autenticación.

Bases de Datos:

Técnicas de Recolección de Datos

Técnicas de Recolección de Datos

Tabla 14.

Técnica de Recolección de Datos

	Encuestas
Encuestas a Usuarios Finales	Objetivo: Obtener información sobre las expectativas y preocupaciones de los usuarios respecto al control de accesos y la autenticación multifactor.
	Contenido: Preguntas sobre la experiencia actual con la autenticación, problemas de seguridad percibidos, y sugerencias para la mejora.
	Método: Encuestas en línea distribuidas a través de plataformas como Google Forms o SurveyMonkey.
	Objetivo: Recopilar información sobre las necesidades técnicas y operativas relacionadas con la gestión del sistema de autenticación.

Encuestas a Administradores de Sistemas	Contenido: Preguntas sobre las características necesarias, integración con sistemas existentes, y políticas de seguridad.
	Método: Encuestas estructuradas enviadas por correo electrónico o completadas en reuniones.
	Entrevistas
Entrevistas con Administradores de TI y Seguridad	Objetivo: Obtener una visión detallada sobre los requisitos técnicos, desafíos y expectativas para la integración de Duo Mobile.
	Contenido: Preguntas sobre la configuración de políticas de seguridad, integración con otras herramientas, y criterios de éxito.
	Método: Entrevistas cara a cara o virtuales utilizando herramientas como Zoom o Microsoft Teams.
Entrevistas con Usuarios Clave	Objetivo: Identificar las necesidades específicas y preocupaciones de un grupo representativo de usuarios que interactuarán con el sistema.
	Contenido: Preguntas sobre el uso actual de autenticación, problemas con el proceso actual, y expectativas sobre la nueva solución. Método: Entrevistas individuales o en grupos pequeños.
	Pruebas de Usabilidad
Pruebas de Usabilidad con Duo Mobile	Objetivo: Evaluar la facilidad de uso y la eficiencia del sistema de autenticación multifactor desde la perspectiva del usuario.
	Contenido: Sesiones donde los usuarios interactúan con Duo Mobile para realizar tareas específicas, como iniciar sesión o configurar la autenticación multifactor.
	Método: Sesiones de prueba en las que se observa y se graba la interacción de los usuarios con la aplicación para identificar problemas y áreas de mejora.
Pruebas de Accesibilidad	Objetivo: Asegurar que el sistema sea accesible para todos los usuarios, incluyendo aquellos con discapacidades.
	Contenido: Evaluaciones para comprobar la compatibilidad con tecnologías de asistencia y el cumplimiento de las directrices de accesibilidad.
	Método: Pruebas realizadas con usuarios que tienen diversas necesidades de accesibilidad y herramientas de evaluación de accesibilidad.
	Análisis de Datos Existentes
Revisión de Registros de Seguridad y Accesos	Objetivo: Analizar los registros actuales de seguridad y acceso para identificar patrones y problemas recurrentes.
	Contenido: Datos sobre intentos de acceso no autorizados, problemas de autenticación y vulnerabilidades.
	Método: Revisión y análisis de informes generados por el sistema de gestión de accesos existente.

Análisis de Políticas y Procedimientos Actuales	Objetivo: Evaluar las políticas de seguridad actuales y su efectividad en la protección de datos.
	Contenido: Documentos y directrices sobre control de accesos y procedimientos de seguridad.
	Método: Revisión de documentación interna y análisis comparativo con mejores prácticas de la industria.

Nota: técnicas de recolección de datos, encuestas, entrevistas, pruebas y análisis, describe las diversas técnicas utilizadas para la recolección de datos, detallando su aplicabilidad, ventajas y limitaciones.

Evaluación con Stakeholders: Planificación y Ejecución de Encuestas y Entrevistas

La Evaluación con Stakeholders es un paso esencial para validar los requisitos, identificar problemas y hacer ajustes necesarios del proyecto, como la revisión y redefinición de la matriz de accesos en un sistema transaccional.

Objetivo de la Evaluación con Stakeholders

El objetivo principal de la evaluación con stakeholders es:

Validar requisitos: Verificar que la matriz de accesos sea adecuada a las necesidades de los usuarios finales, administradores y personal de seguridad.

Ajustar detalles críticos: Ajustar la estructura de accesos y roles según el feedback de los stakeholders para garantizar que se cumplan con las necesidades de acceso y seguridad.

Identificar riesgos de seguridad: Detectar problemas relacionados con la protección de datos y accesos no autorizados.

Identificación de Stakeholders

Usuarios finales: Aquellos que usan el sistema transaccional diariamente (empleados, agentes, clientes).

Administradores de TI: Responsables de configurar y mantener el sistema, gestionar los roles y permisos.

Equipo de seguridad: Encargado de asegurar que la matriz de accesos cumpla con los estándares de seguridad y que no haya brechas en la protección de datos.

Gerentes de negocio: Aquellos que necesitan garantizar que el sistema cumpla con las expectativas operativas.

Herramientas para la Recolección de Datos

Para obtener datos de manera estructurada, se utilizará Microsoft Forms. Estas herramientas permiten crear formularios con preguntas de opción múltiple, de texto libre o escalas de valoración, esta opción está integrada con Microsoft Office, ideal si la organización ya usa el ecosistema de Microsoft.

Diseño de la Encuesta o Entrevista

Sección 1: Accesos y Roles

¿Qué tipo de acceso considera que debería tener en el sistema según su rol?

Solo consulta

Consulta y modificación

Acceso total a configuraciones

¿Existen recursos o áreas del sistema a los que considera que no debería tener acceso su rol actual? ¿Cuáles?

¿Cuál es el nivel de complejidad de gestionar los accesos en el sistema actual? (Escala de 1 a 5, donde 1 es muy difícil y 5 es muy fácil)

Sección 2: Seguridad y Riesgos

¿Qué tan preocupado está por la seguridad de sus datos y accesos dentro del sistema actual? (Escala de 1 a 5)

¿Considera que la política de acceso actual cubre adecuadamente los riesgos de fraude o accesos no autorizados?

Sí

No

No estoy seguro

¿Qué medidas de seguridad adicionales sugeriría para mejorar la protección de datos?

Sección 3: Facilidad de Uso

¿Es fácil para los administradores gestionar y asignar permisos a los roles?

Sí

No

¿Cómo calificaría la interfaz de usuario del sistema para gestionar los accesos? (Escala de 1 a 5)

¿Qué sugerencias tendría para mejorar la gestión de accesos desde la interfaz?

Sección 4: Recomendaciones Generales

¿Hay algún otro aspecto relacionado con los accesos, roles o seguridad que le gustaría sugerir o mejorar en el sistema?

¿Cómo ve la relación entre seguridad y facilidad de uso en la nueva matriz de accesos?

Planificación de Entrevistas

Se planificarán las siguientes preguntas clave:

¿Cuáles son las principales preocupaciones que tiene sobre la seguridad de los accesos en el sistema actual?

¿Qué cambios propondría para mejorar los roles y permisos dentro del sistema?

¿Cómo se sienten con respecto a la implementación de nuevas medidas de seguridad, como autenticación multifactor (MFA)?

Frecuencia de las entrevistas: Una vez al inicio del proyecto y luego programar reuniones periódicas para recibir retroalimentación continua.

Implementación de Encuestas y Entrevistas

Envío de Encuestas: Se enviarán las encuestas a través de Google Forms, respondiendo dentro de un plazo definido.

Realización de Entrevistas: Se programarán entrevistas virtuales o presenciales con los stakeholders clave.

Análisis de Resultados

Después de recolectar los datos, se realizará un análisis profundo de las respuestas. Buscando patrones comunes y temas recurrentes que puedan indicar áreas de mejora o riesgos que deben ser atendidos.

Principales Hallazgos: Identificar las áreas críticas donde los stakeholders han señalado problemas o preocupaciones.

Recomendaciones: Ajustar la matriz de accesos basándote en el feedback recibido. Esto incluira cambios en la asignación de permisos, la introducción de nuevas medidas de seguridad, o mejoras en la facilidad de uso del sistema.

Acciones Posteriores a la Evaluación

Tras recibir la retroalimentación de los stakeholders:

Se ajustará la estructura de accesos: Se modifica los roles y permisos según los hallazgos.

Se Implementará nuevas medidas de seguridad: De ser necesario, se implementara nuevas estrategias de protección de datos y autenticación.

Seguimiento y Retroalimentación Continua

Se realizará un seguimiento continuo con los stakeholders después de implementar los cambios. Esto garantizara que el sistema de accesos siga siendo funcional, seguro y alineado con las necesidades de los usuarios.

Métodos de Control y Seguimiento

Planificación y Gestión del Proyecto

Plan de Proyecto Detallado:

Descripción: Desarrollar un plan de proyecto exhaustivo que defina claramente los objetivos, plazos, hitos, y entregables.

Acciones: Incluye cronogramas detallados, asignación de recursos, y tareas específicas para cada fase del proyecto.

Metodología de Gestión de Proyectos:

Descripción: Aplicar una metodología de gestión de proyectos, como Scrum para desarrollo ágil o Waterfall para un enfoque más lineal, dependiendo de las necesidades del proyecto.

Acciones: Utiliza marcos y prácticas de la metodología elegida para planificar, ejecutar y controlar el proyecto.

Monitoreo de Progreso

Reuniones de Seguimiento:

Descripción: Realizar reuniones periódicas (diarias, semanales o quincenales) con el equipo del proyecto para revisar el progreso, discutir problemas y ajustar el plan según sea necesario.

Acciones: Reuniones de equipo, informes de estado, y discusiones sobre desviaciones y ajustes.

Informes de Progreso:

Descripción: Generar informes de progreso regulares que documenten el estado del proyecto en relación con los plazos y objetivos.

Acciones: Crear y distribuir informes a los interesados clave, incluyendo detalles sobre tareas completadas, problemas encontrados y soluciones implementadas.

Control de Calidad y Evaluación

Revisión de Entregables:

Descripción: Revisar y validar los entregables del proyecto para asegurarse de que cumplan con los requisitos establecidos.

Acciones: Realizar revisiones de código, pruebas de funcionalidad y validación de los componentes implementados.

Pruebas de Aceptación:

Descripción: Realizar pruebas de aceptación para verificar que el sistema cumple con los requisitos y expectativas del cliente

Acciones: Ejecución de pruebas de usabilidad, pruebas de seguridad, y validación de integración.

Gestión de Riesgos

Identificación y Evaluación de Riesgos:

Descripción: Identificar riesgos potenciales para el proyecto y evaluarlos en términos de impacto y probabilidad.

Acciones: Desarrollar una matriz de riesgos y un plan de mitigación para abordar problemas antes de que afecten el proyecto.

Monitoreo de Riesgos:

Descripción: Supervisar de manera continua los riesgos identificados y nuevos riesgos que puedan surgir.

Acciones: Revisar regularmente la lista de riesgos, actualizar el plan de mitigación y ajustar las estrategias según sea necesario.

Control de Cambios

Gestión de Solicitudes de Cambio:

Descripción: Implementar un proceso formal para manejar las solicitudes de cambio en el alcance, requisitos o recursos del proyecto.

Acciones: Evaluar el impacto de los cambios, aprobar o rechazar solicitudes y actualizar el plan del proyecto en consecuencia.

Control de Versiones:

Descripción: Utilizar herramientas de control de versiones para gestionar y rastrear cambios en el código y la configuración del sistema.

Acciones: Implementar prácticas de gestión de versiones utilizando sistemas como Git para mantener un historial claro y organizado de cambios.

Gestión de Recursos y Presupuesto

Seguimiento de Recursos:

Descripción: Controlar el uso de recursos del proyecto, incluyendo personal, tiempo y materiales.

Acciones: Revisar el uso de recursos y ajustar las asignaciones según sea necesario para evitar desviaciones significativas.

Control de Presupuesto:

Descripción: Monitorear los costos del proyecto y asegurarse de que se mantengan dentro del presupuesto asignado.

Acciones: Revisar informes financieros, ajustar el presupuesto si es necesario y reportar cualquier desviación significativa.

Comunicación y Documentación

Plan de Comunicación:

Descripción: Establecer un plan de comunicación claro para mantener a todos los interesados informados sobre el progreso del proyecto.

Acciones: Definir canales de comunicación, frecuencia de actualizaciones y responsables de la comunicación.

Documentación del Proyecto:

Descripción: Mantener una documentación completa y actualizada sobre el proyecto, incluyendo requisitos, decisiones, y cambios.

Acciones: Utilizar herramientas de documentación y gestión de proyectos para almacenar y compartir información relevante.

Cronograma

Tabla 15.

Tabla de Cronograma

CRONOGRAMA						
ACTIVIDAD	MES 1	MES 2	MES 3	MES 4	MES 5	MES 6
Análisis	Revisión de procesos y procedimientos que tiene la empresa					
	Revisión de las funciones de los grupos para verificar su rol					
	Revisión de información					
	Análisis de protocolos de seguridad					
Diseñar propuesta		Diseñar una propuesta de mejora a los procedimientos de control de accesos	Describir los requerimientos de información y funcionalidad de la herramienta tecnológica propuesta.			
		Identificar los puntos críticos del flujo de información	Definir los recursos necesarios para la implementación			
Ejecución				Evaluar las herramientas y software	Implementar configuración de herramienta Duo Mobile	
				Definir la herramienta de control de accesos	Administrar permisos de acuerdo con cada rol	
					Desarrollar un canal de comunicación con el ingreso o cambio de cada miembro el grupo	
					Instalar aplicación Duo	Capacitar en el manejo de la aplicación
Monitorización						Monitorear constantemente el manejo e ingreso y asignación de permisos
					capacitación constante	Documentación de todo el proceso

Nota: Cronograma a 6 meses detalla las principales actividades y plazos establecidos para la implementación del proyecto

Recursos Necesarios

Tabla 16.
Recursos

Recursos necesarios		
Recurso	Descripción	Presupuesto ($)
Equipo Humano	Jefe de Seguridad de la información Analista de Seguridad de la información	$25.000.000
Equipos y Software	Computador portátil, SO Windows 10, acceso a las plataformas de la empresa	$9.000.000
Viajes y Salidas de Campo	Acompañamientos y reuniones en sitio	Propio $200.000
Materiales y suministros		No aplica
Bibliografía		
Total $34.200.000		

Nota: tabla de recursos, detalla los elementos necesarios para el desarrollo y ejecución del proyecto

Impacto Esperado

Métricas Específicas para Medir el Éxito del Proyecto

Tabla 17.

Tiempos y métricas para asignar permisos

Tiempo Promedio para Asignar Permisos Antes y Después	
Indicador	Medir el tiempo promedio requerido para asignar o modificar los permisos de acceso a los usuarios en el sistema, tanto antes como después de la redefinición de la matriz de accesos. Antes: El tiempo promedio actual para asignar permisos a los usuarios es de 15 días. Después: El tiempo esperado después de la implementación de la nueva matriz debe reducirse a 7 días (un objetivo de reducción del 50% en el tiempo).
Resultado Esperado	Una reducción en el tiempo de asignación de permisos a los usuarios, que facilitará una gestión más ágil de los accesos y reducirá los cuellos de botella en el proceso de administración de accesos.
Meta	Reducir el tiempo promedio para asignar permisos en un 30% en los primeros 3 meses después de la implementación.
Porcentaje de Reducción en Accesos No Autorizados	
Indicador	Medir el porcentaje de accesos no autorizados al sistema antes y después de implementar la nueva matriz de accesos. Esto puede incluir accesos a áreas sensibles o a recursos fuera del alcance de ciertos roles. Antes: El porcentaje de accesos no autorizados es de 30%. Después: El objetivo es reducir este porcentaje a 5% después de la implementación de la nueva estructura de permisos.
Resultado Esperado	Una disminución significativa en los accesos no autorizados, lo que resultará en una mayor protección de los datos y recursos del sistema, así como un mejor control de seguridad.
Meta	Reducir los accesos no autorizados en un 50% en los primeros 3 meses posteriores a la redefinición de la matriz de accesos.
Conformidad con Normativas y Auditorías Aprobadas	
Indicador	Evaluar la conformidad del sistema de accesos con las normativas internas y externas de seguridad de datos, como los estándares de la ISO 27001 o normativas locales sobre protección de datos (como la Ley de Protección de Datos Personales). Este indicador se puede medir a través de auditorías internas y externas. Antes: El sistema de accesos cumple con un porcentaje de conformidad de 20% según la última auditoría.

	Después: Se espera lograr un cumplimiento del 5% en las auditorías posteriores a la implementación de la nueva matriz.
Resultado Esperado	Cumplir con los estándares de seguridad y privacidad requeridos, lo que aumentará la confianza de los usuarios y reducirá el riesgo de sanciones legales o de cumplimiento.
Meta	Obtener una calificación de conformidad del 100% en la próxima auditoría interna y externa realizada después de la redefinición de la matriz.
	Satisfacción de los Usuarios con el Sistema de Gestión de Accesos
Indicador	Medir la satisfacción de los usuarios (tanto los administradores de TI como los usuarios finales) con respecto a la facilidad de uso, seguridad y eficiencia del sistema de accesos a través de encuestas o entrevistas. Antes: El puntaje de satisfacción en relación con la gestión de accesos es de 2 (en una escala de 1 a 5). Después: El puntaje esperado es de 4 (en una escala de 1 a 5), reflejando una mejora en la experiencia de usuario.
Resultado Esperado	Una mejora en la satisfacción de los usuarios con la gestión de accesos, lo que indicaría que el nuevo sistema es percibido como más eficiente, seguro y fácil de usar.
Meta	Incrementar el puntaje de satisfacción de los usuarios en un 20% después de la implementación de la nueva matriz de accesos.
	Reducción de Errores Humanos en la Asignación de Permisos
Indicador	Indicador: Medir la frecuencia de errores humanos en la asignación de permisos de acceso, como la asignación incorrecta de permisos a usuarios o la asignación de permisos a roles incorrectos. Antes: Los errores humanos en la asignación de permisos ocurren en un 40% de los casos. Después: La meta es reducir los errores humanos en la asignación de permisos a 1%.
Resultado Esperado	Una menor tasa de errores humanos en la gestión de accesos, lo que garantizará que los permisos sean correctos y que se mantenga la integridad y seguridad del sistema.
Meta	Reducir los errores humanos en un 40% en el primer trimestre después de la implementación de la nueva matriz de accesos.

Nota: Tabla de Indicador, resultado y meta de tiempos, detalla los tiempos estimados y las métricas utilizadas para asignar permisos en el sistema

Piloto Previo al Despliegue Completo

Objetivo del Piloto

El propósito de realizar un piloto antes del despliegue completo del nuevo sistema de gestión de accesos es probar la efectividad de la solución, identificar problemas potenciales y hacer ajustes necesarios para asegurar una transición sin contratiempos a la implementación a gran escala.

Tabla 18.

Fases de Piloto

Fases del piloto	
Selección de Participantes	Usuarios de Prueba: Elegir un grupo representativo de usuarios de diferentes áreas de la empresa que interactúan con el sistema de gestión de accesos. -Rol de los Participantes: Incluir tanto usuarios que gestionan permisos (administradores de accesos, IT) como aquellos que solo utilizan el sistema (empleados de distintos departamentos). -Tamaño del Grupo Piloto: Sera un grupo de 5 a 10 usuarios para asegurar una prueba diversa sin ser demasiado grande, lo que permitiría gestionarlo adecuadamente.
Definición de Alcance del Piloto	El piloto incluirá un conjunto limitado de funciones del nuevo sistema de gestión de accesos, tales como: Asignación de permisos y accesos. Revisión y actualización de accesos. Autenticación multifactor (MFA). El piloto debe realizarse bajo condiciones controladas, asegurando que todos los usuarios involucrados comprendan claramente sus responsabilidades.
Configuración del Entorno Piloto	Entorno de Prueba: Crear un entorno aislado o simulado en donde el sistema de gestión de accesos pueda ser probado sin afectar el sistema en vivo. Simulación de Escenarios Reales: Configurar el sistema de acceso con los permisos que los usuarios finales realmente utilizarán en el entorno de producción.
Monitoreo y Evaluación Durante el Piloto	Recopilación de Datos: Medir el impacto en términos de: Tiempo de Asignación de Permisos: Comparar el tiempo de asignación antes y después de la implementación del nuevo sistema. Accesos Incorrectos o No Autorizados: Monitorear el número de accesos fallidos y errores de asignación de permisos. Satisfacción de los Participantes: Realizar encuestas o entrevistas para evaluar la experiencia de los usuarios. Identificación de Problemas: Monitorear de cerca posibles errores o fallos en el sistema, como problemas de sincronización, errores de

	autenticación o cualquier otro inconveniente que puedan enfrentar los usuarios.
Ajustes Basados en Retroalimentación	Durante la fase de prueba, será esencial contar con un proceso ágil para realizar ajustes rápidos según los problemas identificados. Esto puede incluir: Modificar flujos de trabajo si se encuentran ineficiencias. Ajustar la interfaz de usuario si se identifican problemas de usabilidad. Reforzar las políticas de seguridad si se detectan accesos no autorizados o riesgos de seguridad.
Duración del Piloto	El piloto debe durar entre 1 a 2 semanas, tiempo suficiente para obtener resultados significativos y permitir que los participantes se familiaricen con el sistema. Durante este período, se debe asegurar que los usuarios tengan acceso a soporte técnico para resolver problemas rápidamente.
Evaluación y Decisión Final	Análisis de Resultados: Después del período del piloto, se debe evaluar el desempeño general del sistema. Esto incluirá un análisis de las métricas de desempeño y la retroalimentación de los usuarios finales. -Informe de Evaluación: Preparar un informe con los resultados del piloto, que incluirá: Datos sobre la eficiencia del sistema (tiempo de asignación de permisos, tasa de acceso correcto/incorrecto). Feedback sobre la experiencia de los usuarios (satisfacción y facilidad de uso). Identificación de cualquier riesgo de seguridad o inconveniente operativo. Decisión de Despliegue Completo: A partir de los resultados del piloto, tomar una decisión sobre si proceder con el despliegue completo del sistema o si se deben realizar más ajustes.
Comunicación Post-Piloto	Una vez que el piloto haya sido evaluado y se haya tomado la decisión de avanzar, se debe comunicar a todos los participantes los cambios que se han realizado y los beneficios esperados del sistema completo. -Plan de Despliegue Completo: Establecer un plan detallado para la implementación en toda la organización, incluyendo cronograma, capacitación de empleados y cualquier ajuste necesario.

Nota: Tabla de las fases que tendrá el piloto, describe las diferentes fases del piloto, detallando los objetivos y actividades clave en cada etapa.

El proyecto de Revisión y Redefinición de la Matriz de Accesos para un Sistema Transaccional de una Empresa de Envíos de Dinero tendrá un impacto significativo en el cumplimiento de normativas clave, como la Ley 1581 de 2012 de Protección de Datos Personales en Colombia y la ISO/IEC 27001 sobre gestión de seguridad de la información. A

continuación, se detallan cómo se cumplirá con estas normativas y los beneficios que se obtendrán a partir de su implementación, respaldados con citas y ejemplos específicos.

Cumplimiento de la Ley 1581 de 2012 (Protección de Datos Personales en Colombia)

La Ley 1581 de 2012 establece el marco legal para la protección de datos personales en Colombia, obligando a las organizaciones a implementar medidas de seguridad para garantizar la privacidad y la integridad de los datos personales. El proyecto de revisión de la matriz de accesos contribuirá al cumplimiento de esta ley de varias maneras clave:

Tabla 19.

Cumplimiento de la Ley 1581 de 2012

Aseguramiento de Accesos Restrictivos y Controlados		
Justificación	Ejemplo	Referencia
La ley exige que solo los empleados autorizados puedan acceder a datos personales, y los accesos deben estar alineados con los principios de "limitación de la finalidad" y "mínima necesidad". Esto implica que los usuarios deben tener acceso únicamente a los datos que sean estrictamente necesarios para el cumplimiento de sus tareas laborales.	Durante la revisión de la matriz de accesos, se garantizará que los roles de usuario estén definidos de manera que cada uno solo tenga acceso a la información pertinente a su función. Así, se evitará que los empleados accedan a datos sensibles o personales de clientes sin justificación. Esto será validado y documentado en el proceso de redefinición.	La Ley 1581 de 2012, Artículo 8 (Principios para el tratamiento de datos personales) establece que los datos deben ser "tratados con confidencialidad" y "restringidos al acceso autorizado" (Ley 1581 de 2012, 2012).
Implementación de Medidas Técnicas de Seguridad		
Justificación	Ejemplo	Referencia
La ley requiere que las organizaciones implementen medidas de seguridad "razonables" para evitar el acceso no autorizado, la alteración o la pérdida de datos personales.	El proyecto incluirá la implementación de registros detallados de auditoría de accesos (logs), que permitan monitorizar en tiempo real los accesos a los datos personales y asegurarse de que cualquier acceso no autorizado sea identificado rápidamente.	Ley 1581 de 2012, Artículo 17: "El responsable del tratamiento debe adoptar las medidas necesarias para garantizar la seguridad de los datos personales y evitar su alteración, pérdida, consulta, uso o acceso no autorizado."

Nota: Cumplimiento de la Ley 1581 de 2012 (Protección de Datos Personales en Colombia), resume las acciones y medidas adoptadas para garantizar el cumplimiento de la Ley 1581 de 2012

Cumplimiento de la ISO/IEC 27001 (Sistema de Gestión de Seguridad de la Información)

La ISO/IEC 27001 es un estándar internacional que establece los requisitos para un sistema de gestión de seguridad de la información (SGSI). Su implementación en el proyecto garantizará que se sigan las mejores prácticas de seguridad para proteger tanto los datos como los accesos dentro del sistema transaccional. El proyecto contribuirá a cumplir con este estándar de la siguiente manera:

Tabla 20.

Cumplimiento de la ISO/IEC 27001

Gestión de Riesgos Relacionados con los Accesos		
Justificación	Ejemplo	Referencia
ISO/IEC 27001 pone énfasis en la gestión de riesgos como un componente central de la seguridad de la información. El control de accesos es uno de los aspectos clave en la gestión de riesgos, ya que los accesos no autorizados pueden generar vulnerabilidades graves.	Durante el proyecto, se realizará una evaluación de riesgos sobre los accesos actuales, identificando vulnerabilidades potenciales, como usuarios con accesos excesivos. Posteriormente, se implementarán controles y políticas de acceso más estrictas para mitigar estos riesgos, alineándose con los requisitos de la ISO.	ISO/IEC 27001, Control A.9.1: "La gestión de accesos debe implementarse para garantizar que solo se otorgue acceso a la información y recursos basados en las necesidades de trabajo."
Implementación de Auditorías y Registros de Accesos		
Justificación	Ejemplo	Referencia
ISO/IEC 27001 exige la implementación de medidas de monitoreo y auditoría para asegurar que el acceso a la información sea adecuado y seguro.	Como parte de la mejora continua, se establecerán procedimientos de auditoría que registren todos los accesos a los sistemas sensibles. Estos registros permitirán revisar y auditar los accesos para verificar que estén alineados con las políticas y normativas internas de seguridad, garantizando la transparencia y trazabilidad de todas las acciones.	ISO/IEC 27001, Control A.12.4.1: "Los registros de eventos de seguridad deben estar habilitados, almacenados y protegidos para facilitar la auditoría de los accesos y las acciones en el sistema."
Control de Accesos Basado en Roles (RBAC)		
Justificación	Ejemplo	Referencia
La implementación de RBAC (Role-Based Access Control) es una práctica recomendada en ISO/IEC 27001 para asegurar que los usuarios tengan acceso solo a los	El proyecto implementará un modelo de control de accesos basado en roles (RBAC) para asegurar que cada usuario acceda solo a los recursos necesarios según sus responsabilidades laborales. Este	ISO/IEC 27001, Control A.9.2.1: "El acceso a la información y los recursos debe ser restringido y gestionado mediante la asignación de roles y

recursos necesarios para sus roles.	enfoque reducirá el riesgo de accesos no autorizados y garantizará que los permisos se gestionen de manera eficiente.	responsabilidades, basados en el principio de mínimos privilegios."

Nota: Sistema de Gestión de Seguridad de la Información, describe las acciones y medidas implementadas para asegurar el cumplimiento de la norma ISO/IEC 27001.

Relación de Problemas con Requisitos de la Norma ISO 27001

Tabla 21.

Relación de Problemas con Requisitos de la Norma ISO 27001

Problema Actual	Requisito de la Norma ISO 27001	Descripción del Requisito
Accesos no controlados por empleados internos	Cláusula 9.1.2: Control de accesos	Establecer controles para garantizar que solo las personas autorizadas tengan acceso a los sistemas e información.
Gestión insuficiente de permisos y roles	Cláusula 9.2.3: Revisión de permisos de acceso	Revisión periódica de los permisos de acceso de los usuarios para asegurar que sean apropiados y actualizados.
Fugas de datos debido a accesos no autorizados	Cláusula 10.1: Mejora continua del SGSI	Implementar medidas para prevenir y corregir las brechas de seguridad relacionadas con los accesos no autorizados.
Falta de trazabilidad en los accesos al sistema	Cláusula 12.4.1: Registro de actividades	Asegurar que se registre y audite todo acceso y actividad en los sistemas críticos, con un enfoque en la trazabilidad.
Riesgos asociados con empleados y contratistas con acceso no controlado	Cláusula 7.2: Competencia y capacitación	Asegurar que los empleados y contratistas reciban formación en gestión de accesos y seguridad de la información.
Inadecuada gestión de roles y responsabilidades	Cláusula 6.1.1: Análisis y evaluación de riesgos	Identificar, evaluar y gestionar los riesgos relacionados con la gestión de accesos y la protección de la información.

Nota: tabla presenta la relación entre los problemas identificados y los requisitos específicos de la norma ISO 27001

Mejoras en la Seguridad Operativa y Reducción de Riesgos Legales

Tabla 22.

Mejoras en la seguridad Operativa

Prevención de Accesos No Autorizados y Fraudes		
Justificación	Ejemplo	Referencia
Tanto la Ley 1581 como la ISO 27001 destacan la importancia de controlar el acceso a datos personales y recursos sensibles para prevenir fraudes y violaciones de seguridad.	A través de la redefinición de la matriz de accesos, el proyecto contribuirá a evitar accesos erróneos a datos confidenciales y sistemas transaccionales, reduciendo el riesgo de fraudes internos o filtración de datos.	ISO/IEC 27001, Control A.9.2.2: "Los sistemas deben contar con controles para prevenir el acceso no autorizado a información crítica y confidencial."
Satisfacción de las Audiencias Regulatorias		
Justificación	Ejemplo	Referencia
El cumplimiento de la Ley 1581 y de la ISO 27001 proporcionará confianza a las audiencias regulatorias y a los clientes de la empresa, al garantizar que se adoptan prácticas seguras y transparentes para proteger los datos.	El sistema de gestión de accesos mejorado se alinea con las normativas internacionales y locales, permitiendo a la empresa demostrar que cumple con las leyes de protección de datos y que toma medidas activas para proteger la información personal de sus clientes.	ISO/IEC 27001, Control A.18.1.3: "Se debe garantizar el cumplimiento de las obligaciones legales y regulatorias relacionadas con la seguridad de la información."

Nota: Mejoras en la Seguridad Operativa y Reducción de Riesgos Legales, La tabla expone las mejoras propuestas en la seguridad operativa, orientadas a fortalecer los procesos

Este proyecto no solo optimiza la gestión de accesos y mejora la seguridad operativa, sino que también garantiza el cumplimiento de las normativas legales y regulatorias aplicables, como la Ley 1581 de 2012 y la ISO/IEC 27001. A través de la implementación de controles estrictos, auditorías continuas y la adopción de las mejores prácticas internacionales, la empresa no solo protegerá la integridad de sus sistemas, sino que también evitará sanciones legales, mitigando los riesgos operativos y fortaleciendo la confianza de los clientes y las partes interesadas.

Referencias Bibliográficas

Camuña Rodríguez, J. F. (2015). Lenguajes de definición y modificación de datos SQL (UF1472). IC Editorial, p. 59–61. https://elibro-net.bibliotecavirtual.unad.edu.co/es/ereader/unad/44141?page=65

Chavez, J. J. S. (2024, February 13). Controles de acceso: ¿qué son y por qué son importantes para proteger tu empresa? https://www.deltaprotect.com/blog/controles-de-acceso-que-son-y-por-que-son-importantespara-proteger-tu-empresa

De La Caridad Delgado Olivera, L., & Alonso, L. M. D. (2021, March Modelos de Desarrollo de Software. https://www.redalyc.org/journal/3783/378366538003/html/

Hernández, K. (n.d.). En qué consiste un control de ciberseguridad. https://www.servnet.mx/blog/en-que-consiste-un-control-de-ciberseguridad

Insitech. (2023b, October 25). Principales metodologías para el desarrollo de aplicaciones. BLOG - Insitech - BMC Partner - Servicios De Consultoría En TI. https://go.insitech.com.mx/principales-metodologias-para-eldesarrollo-de-aplicaciones/

ISO/IEC 27001:2013. (2013). Tecnología de la información - Técnicas de seguridad - Sistemas de gestión de seguridad de la información. Organización Internacional de Normalización.

¿Qué es la seguridad de AWS? (n.d.-a). [Video]. Amazon Web Services, Inc. https://aws.amazon.com/es/security/

Proware. (2023, September 1). ¿Qué es el control de acceso en seguridad privada? - ProWare HS S.A.S. Proware HS S.A.S. https://www.proware.com.co/blog/control-de-acceso-en-seguridad-privada/

Sandhu, R., Coyne, E. J., Feinstein, H. L., & Youman, C. E. (1996). Role-based access control models. IEEE Computer, 29(2), 38–47.

Sotirios Zygiaris. (2018). Database Management Systems: A Business-Oriented Approach Using ORACLE, MySQL and MS Access (Vol. First edition). Emerald Publishing Limited, p. 171–188.

Talently, Talently, & Talently. (2023, May 23). Power up your workflow: 8 metodologías de desarrollo de software para ser más eficiente. Talently Blog. https://talently.tech/blog/metodologias-desarrollo-softwareworkflow-eficiente/

Toro, R. (2021). Seguridad de la información: Estrategias y medidas de protección. Editorial Infosec.

Valtx. (2022, July 19). Metodologías para el desarrollo de software: ¿Qué son y para qué sirven? Valtx. https://www.valtx.pe/blog/metodologias-para-el-desarrollo-de-software-que-son-y-para-quesirven.

Villegas, J. (2023). Control de acceso y seguridad en sistemas transaccionales. Editorial Tecnológica.