



Universidad Nacional Mayor de San Marcos

Universidad del Perú. Decana de América

Facultad de Ingeniería de Sistemas e Informática

Escuela Profesional de Ingeniería de Sistemas

**Segregación de funciones con control híbrido de
accesos para mejorar la gestión de la información
sensible en una empresa comercializadora de bienes de
capital y servicios**

TESIS

Para optar el Título Profesional de Ingeniero de Sistemas

AUTOR

Christian Manuel MORAN TOLEDO

ASESOR

Félix Armando FERMÍN PÉREZ

Lima, Perú

2025



Reconocimiento - No Comercial - Compartir Igual - Sin restricciones adicionales

<https://creativecommons.org/licenses/by-nc-sa/4.0/>

Usted puede distribuir, remezclar, retocar, y crear a partir del documento original de modo no comercial, siempre y cuando se dé crédito al autor del documento y se licencien las nuevas creaciones bajo las mismas condiciones. No se permite aplicar términos legales o medidas tecnológicas que restrinjan legalmente a otros a hacer cualquier cosa que permita esta licencia.

Referencia bibliográfica

Moran, C. (2025). *Segregación de funciones con control híbrido de accesos para mejorar la gestión de la información sensible en una empresa comercializadora de bienes de capital y servicios*. [Tesis de pregrado, Universidad Nacional Mayor de San Marcos, Facultad de Ingeniería de Sistemas e Informática, Escuela Profesional de Ingeniería de Sistemas]. Repositorio institucional Cybertesis UNMSM.

Metadatos complementarios autor/ asesor

Datos de autor	
Nombres y apellidos	Christian Manuel Moran Toledo
Tipo de documento de identidad	DNI
Número de documento de identidad	15862577
URL de ORCID	-----
Datos de asesor	
Nombres y apellidos	Félix Armando Fermín Pérez
Tipo de documento de identidad	DNI
Número de documento de identidad	08736347
URL de ORCID	https://orcid.org/0000-0001-5606-7309
Datos del jurado	
Presidente del jurado	
Nombres y apellidos	Jorge Luis Chávez Soto
Tipo de documento	DNI
Número de documento de identidad	08675814
Miembro del jurado 1	
Nombres y apellidos	César Augusto Angulo Calderón
Tipo de documento	DNI
Número de documento de identidad	32907109
Datos de investigación	
Línea de investigación	Gobierno y Gestión de TIC

Grupo de investigación	Ninguno
Agencia de financiamiento	Ninguna
Ubicación geográfica de la investigación	Lima
Año o rango de años en que se realizó la investigación	202x - 2025
URL de disciplinas OCDE	https://purl.org/pe-repo/ocde/ford#2.02.04



UNIVERSIDAD NACIONAL MAYOR DE SAN MARCOS
FACULTAD DE INGENIERIA DE SISTEMAS E INFORMATICA
Escuela Profesional de Ingeniería de Sistemas

Acta Virtual de Sustentación de Tesis

Siendo las 15:03 horas del día 27 de noviembre del año 2025, se reunieron virtualmente los docentes designados como miembros de Jurado de Tesis, presidido por el Mg. Jorge Luis Chávez Soto, Mg. Cesar Angulo Calderón (Miembro) y el Ing. Félix Armando Fermín Pérez (Miembro Asesor), usando la plataforma Meet (<https://meet.google.com/otz-uduj-ssp>) para la sustentación Virtual de la tesis Intitulada: “ **SEGREGACIÓN DE FUNCIONES CON CONTROL HÍBRIDO DE ACCESOS PARA MEJORAR LA GESTIÓN DE LA INFORMACIÓN SENSIBLE EN UNA EMPRESA COMERCIALIZADORA DE BIENES DE CAPITAL Y SERVICIOS.**”, del Bachiller: **MORAN TOLEDO, Christian Manuel**; para obtener el Título Profesional de Ingeniero de Sistemas.

Acto seguido de la exposición de la Tesis, el Presidente invitó al Bachiller a responder las preguntas formuladas por los Miembros del Jurado.

El Bachiller, en el curso de sus intervenciones demostró pleno dominio del tema, al responder con acierto y fluidez las preguntas formuladas por los señores miembros del Jurado.

Finalmente habiéndose efectuado la calificación correspondiente por los miembros del Jurado, el bachiller obtuvo la nota de 18 (dieciocho)

A continuación, el Presidente del Jurado Mg. Jorge Chávez Soto, declara al bachiller **Ingeniero de Sistemas.**

Siendo 16:08: horas, se levantó la sesión.

Mg. Jorge Chávez Soto
Presidente

Mg. Cesar Angulo Calderón
Miembro

Félix Armando Fermín Pérez
Miembro Asesor

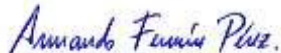
Anexo 1

CERTIFICADO DE SIMILITUD

Yo, **FELIX ARMANDO FERMÍN PEREZ** en mi condición de asesor acreditado con el Dictamen de la UPG o de la **EP N° 000001-2025-EPISI-FISI/UNMSM** de la **tesis/ monografía/ informe de investigación/trabajo académico**, cuyo título es **SEGREGACIÓN DE FUNCIONES CON CONTROL HÍBRIDO DE ACCESOS PARA MEJORAR LA GESTIÓN DE LA INFORMACIÓN SENSIBLE EN UNA EMPRESA COMERCIALIZADORA DE BIENES DE CAPITAL Y SERVICIOS**, presentado por el **bachiller/ magíster/ egresado/ licenciado/ estudiante MORAN TOLEDO CHRISTIAN MANUEL** para optar el grado* el TITULO PROFESIONAL DE **INGENIERO DE SISTEMAS**, CERTIFICO que se ha cumplido con lo establecido en la Directiva de Originalidad y de Similitud de Trabajos Académicos, de Investigación y Producción Intelectual. Según la revisión, análisis y evaluación mediante la plataforma PIDS, el documento evaluado cuenta con el **18.%** de similitud, nivel PERMITIDO para continuar con los trámites correspondientes y para su **publicación en el repositorio institucional**.

Se emite el presente certificado en cumplimiento de lo establecido en las normas vigentes, como uno de los requisitos para la obtención del grado*/ **título***/ especialidad* de Ingeniero de Sistemas.

Lima, 09 de Febrero de 2026

Firma del asesor: 

Nombres y Apellidos del asesor: Félix Armando Fermín Pérez

DNI: 08736347

* Según corresponda: bachiller, magíster, doctor; título profesional o título de segunda especialidad

La vigencia del presente certificado corresponde a un período de noventa (90) días desde la fecha de su emisión; siempre que no haya observaciones en el texto durante el proceso de revisión por el jurado informante o surja alguna contingencia.

DEDICATORIA:

Dedico este trabajo a mis hijos, quienes son mi mayor motivo y fuente de inspiración. Su amor, alegría y fortaleza me impulsaron a seguir adelante en los momentos más exigentes de este proceso.

Todo esfuerzo y sacrificio está reflejado en estas páginas, como un ejemplo de que con amor y dedicación los sueños pueden hacerse realidad

AGRADECIMIENTOS

A mis padres, por ser mi guía constante, por su amor incondicional, su esfuerzo y los valores que me han inculcado desde siempre. Gracias por creer en mí y por enseñarme que la perseverancia y la humildad son las bases del verdadero éxito.

A mis hermanos, por su apoyo, su comprensión y por estar siempre presentes. Cada uno de ustedes ha sido una inspiración y un pilar fundamental en mi camino.

A mi compañera de vida gracias por tu apoyo y paciencia.

A todas las personas que de una u otra forma contribuyeron con su tiempo, conocimiento o compañía durante el desarrollo de esta tesis, mi más sincero agradecimiento.

UNIVERSIDAD NACIONAL MAYOR DE SAN MARCOS
FACULTAD DE INGENIERÍA DE SISTEMAS E INFORMÁTICA
ESCUELA PROFESIONAL DE INGENIERIA DE SISTEMAS

**SEGREGACIÓN DE FUNCIONES CON CONTROL HÍBRIDO DE
ACCESOS PARA MEJORAR LA GESTIÓN DE LA INFORMACIÓN
SENSIBLE EN UNA EMPRESA COMERCIALIZADORA DE BIENES
DE CAPITAL Y SERVICIOS**

Autor : MORAN TOLEDO, Christian Manuel
Asesor : FERMIN PEREZ, Félix Armando
Título : Tesis, para optar el Título Profesional de Ingeniero de Sistemas
Fechas : Octubre de 2025

RESUMEN

La presente investigación propone e implementa un modelo híbrido de control de accesos que combina RBAC (Role-Based Access Control), ABAC (Attribute-Based Access Control) y Autorización por Roles y Procesos, con el fin de fortalecer la Segregación de Funciones (SoD) en la gestión de información sensible de una empresa del sector industrial. A partir del diagnóstico organizacional se identificaron brechas en la asignación de privilegios, controles manuales ineficaces y una baja madurez en la gestión de roles. Ante esta problemática, el modelo desarrollado integra la simplicidad estructural del RBAC, la flexibilidad contextual del ABAC y la alineación operativa de Roles y Procesos, garantizando seguridad, escalabilidad y trazabilidad. Luego de la implementación, se permitió reducir el 26 % de los conflictos de riesgo alto y del 16 % de los de riesgo medio, mientras que el 37 % y 21 % respectivamente se mantuvieron por necesidades operativas justificadas. Asimismo, los indicadores de desempeño (KPI) confirmaron una resolución superior al 90 % de los conflictos SoD y un nivel de privilegios excesivos inferior al 5 %, evidenciando la eficiencia del modelo propuesto y su alineamiento con los controles A.5.15, A.5.18 y A.5.19 de la norma ISO/IEC 27001:2022. Por ende, se concluye que el enfoque híbrido constituye una solución costo-efectiva y adaptable a organizaciones medianas que buscan optimizar su control interno y proteger la información crítica sin incrementar la complejidad tecnológica.

Palabras clave: Control de accesos, Segregación de funciones, RBAC, ABAC, Roles y procesos, Seguridad de la información, ISO/IEC 27001.

MAYOR NATIONAL UNIVERSITY OF SAN MARCOS
FACULTY OF SYSTEMS ENGINEERING
PROFESSIONAL SCHOOL OF SYSTEMS ENGINEERING

SEGREGATION OF DUTIES WITH HYBRID ACCESS CONTROL
TO IMPROVE MANAGEMENT OF SENSITIVE INFORMATION IN
A CAPITAL GOODS AND SERVICES COMPANY

Author : MORAN TOLEDO, Christian Manuel
Adviser : FERMIN PEREZ, Félix Armando
Title : Thesis, to choose the Professional Title System
Date : October 2025

ABSTRACT

This research proposes and implements a hybrid access control model that combines RBAC (Role-Based Access Control), ABAC (Attribute-Based Access Control), and Role-and-Process Authorization, aiming to strengthen Segregation of Duties (SoD) in the management of sensitive information within an industrial company. Based on the organizational assessment, gaps were identified in privilege assignment, ineffective manual controls, and low maturity in role management. To address these issues, the developed model integrates the structural simplicity of RBAC, the contextual flexibility of ABAC, and the operational alignment of Role-and-Process Authorization, ensuring security, scalability, and traceability. After implementation, the system reduced 26% of high-risk and 16% of medium-risk conflicts, while 37% and 21%, respectively, were maintained due to justified operational needs. Furthermore, performance indicators (KPIs) confirmed a resolution rate above 90% of SoD conflicts and less than 5% of excessive privileges, demonstrating the efficiency of the proposed model and its alignment with ISO/IEC 27001:2022 controls A.5.15, A.5.18, and A.5.19. Therefore, it is concluded that the hybrid approach constitutes a cost-effective and adaptable solution for medium-sized organizations seeking to optimize internal control and protect critical information without increasing technological complexity.

Keywords: Access control, Segregation of duties, RBAC, ABAC, Roles and processes, Information security, ISO/IEC 27001.

ÍNDICE

CAPÍTULO I - PLANTEAMIENTO METODOLÓGICO.....	13
1.1. Antecedentes de la problemática.....	13
1.2. Definición del problema	15
1.1.1. Problema principal	15
1.1.2. Problemas específicos	15
1.2. Objetivos	15
1.2.1. Objetivo General.....	15
1.3. Justificación	16
1.4. Tipo de investigación	17
1.5. Población	17
1.6. Técnicas de recolección de datos.....	18
CAPÍTULO II- MARCO TEÓRICO	19
2.1. Seguridad de la Información.....	19
2.1.1. Sistema de Gestión de Seguridad de la Información	19
2.1.2. Gestión de Información Sensible	20
2.2. Segregación de Funciones (SoD).....	21
2.3. Control de Accesos	23
2.3.1. Control de acceso lógico.....	23
2.3.2. Control de acceso físico.....	26
2.3.3. Control híbrido de accesos RBAC-ABAC	27
2.3.4. Autorización por roles y procesos	29
2.4. Normas y Estándares Aplicables.....	30
2.5. Análisis comparativo de modelos de control de accesos y alineación con ISO/IEC 27001:2022	31
CAPÍTULO III- ESTADO DEL ARTE.....	34

CAPÍTULO IV IMPLEMENTACIÓN	39
4.1. Introducción breve	39
4.2. Diseño y desarrollo del modelo propuesto.....	40
4.3. Validación del diseño.....	46
Capítulo V DISCUSIÓN, CONCLUSIONES Y RECOMENDACIONES	51
5.1. Discusión	51
5.2. Conclusiones	53
5.3. Recomendaciones.....	53
REFERENCIAS.....	55
ANEXOS	59
Anexo A. Análisis de conflictos de acceso por empresa y departamento	60
Anexo B Análisis de conflictos por holding según cada empresa	60
Anexo C Análisis de conflictos por holding según los usuarios	61
Anexo D. Gráfico resumen del análisis de conflictos de riesgo alto por holding	62
Anexo E. Gráfico resumen del análisis de conflictos de riesgo medio por holding....	63
Anexo F. Gráfico resumen del análisis de conflictos por holding	63

ÍNDICE DE TABLAS

Tabla 1. Análisis comparativo de modelos de control de accesos y alineación con ISO/IEC 27001:2022	33
Tabla 2. Comparación de las características de los estudios incluidos en el estado de arte	37
Tabla 3. Comparación entre SAP Access Control (Compliance) y el sistema desarrollado	40
Tabla 4. Correspondencia entre controles ISO/IEC 27001 y funcionalidades del sistema de análisis SoD.....	42

ÍNDICE DE FIGURAS

Figura 1. Diagrama de flujo de la gestión de información sensible.....	21
Figura 2. Diagrama de flujo de Segregación de Funciones	22
Figura 3. Esquema del modelo RBAC adaptado de Indenhaus (2017).....	24
Figura 4. Esquema del modelo ABAC adaptado de Axiomatics (2018).....	25
Figura 5. Esquema de los componentes de control de acceso físico (Sánchez, 2022)	27
Figura 6. Matriz de segregación de funciones validada con criterios F1-F2.....	43
Figura 7. Interfaz de la matriz generadora de funciones antes y después de la ejecución.....	44
Figura 8. Reporte de combinaciones de funciones con conflictos detectados.....	45
Figura 9. Informe de SoD con identificación de riesgos y frecuencia de uso.	45
Figura 10. Registro final de validación y justificación del negocio.....	46
Figura 11. Comparación de resultados entre la ejecución inicial y la segunda ejecución.....	47
Figura 12. Estado de los conflictos tras la respuesta de las áreas responsables.	48
Figura 13. KPI 1: % de cuentas con privilegios excesivos	48
Figura 14. KPI 2: % de conflictos de SoD resueltos.....	49

CAPÍTULO I - PLANTEAMIENTO METODOLÓGICO

1.1. Antecedentes de la problemática

En el contexto actual, las organizaciones que operan en sectores altamente regulados y con plataformas críticas como los sistemas ERP enfrentan crecientes desafíos para garantizar la integridad, confidencialidad y disponibilidad de su información sensible. Al respecto, el *IBM Cost of a Data Breach Report (2023)* indica que el costo promedio global de una brecha alcanzó 4,45 millones de USD, con un incremento del 15% en los últimos tres años, lo que subraya el impacto operativo, financiero y reputacional de una gestión deficiente de privilegios de acceso. Esta problemática se vincula directamente con el ODS 9, ya que resalta la necesidad de contar con infraestructuras digitales resilientes e innovadoras, capaces de sostener operaciones seguras en entornos industriales cada vez más interconectados (Organización de las Naciones Unidas, 2023).

En América Latina, y específicamente en el Perú, esta situación es igualmente crítica, para evidenciar ello, el *Índice Nacional de Ciberseguridad (NCSI, 2023)* señala avances en políticas regulatorias, pero también brechas significativas en la gestión de accesos y en la adopción de estándares internacionales, lo que mantiene elevada la vulnerabilidad frente a ciberataques e incidentes internos. En este marco, la Ley N.º 29733 – *Ley de Protección de Datos Personales* establece obligaciones estrictas para la custodia de información, cuya transgresión implica sanciones severas y riesgo reputacional (Congreso de la República del Perú, 2011). Estos vacíos no solo afectan la continuidad operativa, sino también la confianza institucional, aspecto clave del ODS 16, que busca promover instituciones eficaces, responsables y transparentes (Organización de las Naciones Unidas, 2023).

Bajo este panorama, las organizaciones con operaciones de gran escala enfrentan un doble reto: cumplir con estándares como la ISO/IEC 27001:2022 —referente internacional en seguridad de la información— y, al mismo tiempo, implementar modelos técnicos eficaces, tales como la segregación de funciones (SoD) y controles híbridos de acceso, que integren mecanismos físicos y lógicos de protección.

En el caso de estudio, en una empresa peruana del sector de comercialización de bienes de capital y servicios, con aproximadamente 6 000 colaboradores entre personal

directo y tercerizado, las auditorías de seguridad y TI evidenciaron deficiencias estructurales en la gestión de accesos a su ERP. Entre ellas destacan: ausencia de un procedimiento formal para la gestión del ciclo de vida de privilegios (alta, revisión y baja), existencia de cuentas genéricas o inactivas sin responsable asignado, controles débiles sobre datos sensibles y carencia de un esquema efectivo de SoD. Estas brechas incrementan la superficie de ataque, reducen la trazabilidad de acciones de usuario y comprometen el cumplimiento normativo. A nivel de referencia, en 2024 el costo promedio global de una brecha ascendió a 4,88 millones de USD, con un impacto 13 % mayor en sectores industriales, mientras que se estima que el 68 % de los incidentes involucran el factor humano y que el tiempo promedio para detectar y contener un ataque es de 241 días (Kessem, 2025). Estos indicadores ilustran la magnitud del riesgo operativo y la necesidad de controles preventivos más sólidos.

En síntesis, tanto la evidencia de auditoría como los indicadores globales confirman la urgencia de diseñar e implementar un modelo estructurado de control de accesos basado en roles y SoD, que garantice trazabilidad exhaustiva y procedimientos de ciclo de vida de privilegios, en conformidad con la ISO/IEC 27001:202

A partir de este diagnóstico, la alta dirección determinó la pertinencia de un proyecto orientado al diseño e implementación de una solución integral de SoD y control de accesos, con el objetivo de corregir las deficiencias identificadas y fortalecer la gestión de la información sensible en el ERP. En este marco, la presente investigación propone el desarrollo de un prototipo que demuestre la viabilidad de un modelo híbrido de control de accesos, aplicable a los procesos críticos de la organización. El alcance funcional del proyecto comprende alrededor del 80 % de los procesos operativos de la empresa, con participación de *Key Users* en cada área funcional y un esquema de gobernanza articulado entre Seguridad de la Información y las áreas de negocio.

Finalmente, la presente tesis se organiza de la siguiente manera: en el Capítulo I: Planteamiento Metodológico, se expone el problema de investigación, los antecedentes, los objetivos, la justificación y el alcance del estudio; en el Capítulo II: Marco Teórico, se presentan los conceptos fundamentales vinculados con la seguridad de la información, la segregación de funciones y los modelos de control de accesos, así como los estándares internacionales aplicables; el Capítulo III: Estado del Arte revisa investigaciones y enfoques previos, comparando los modelos existentes y destacando sus ventajas y limitaciones; en el

Capítulo IV: Implementación, se describe el diseño, desarrollo y validación del sistema propuesto, incluyendo su alineación con la norma ISO/IEC 27001:2022; posteriormente, en el Capítulo V: Discusión, Conclusiones y Recomendaciones, se interpretan los resultados obtenidos, se contrastan con la literatura y se plantean propuestas de mejora para la organización; finalmente, el Capítulo VI: Referencias recopila las fuentes utilizadas a lo largo de la investigación.

1.2. Definición del problema

1.1.1. Problema principal

La problemática central se enfoca en la necesidad de fortalecer la gestión de la información sensible en una empresa comercializadora de bienes de capital y servicios, debido a que el modelo actual de control de accesos tiene una deficiente segregación de funciones, lo que compromete la trazabilidad, la confidencialidad de los datos y el cumplimiento de normativas internacionales de seguridad. Esta situación expone a la organización a riesgos operativos, legales y de ciberseguridad que afectan la integridad de sus procesos críticos y la confiabilidad de su sistema informático.

1.1.2. Problemas específicos

- La segregación de funciones (SoD) es un proceso manual que se realiza bajo el criterio de los trabajadores, lo que genera ambigüedades en la asignación de accesos, incrementa la exposición a accesos indebidos o excesivos por parte de los colaboradores.
- El modelo actual de control de accesos cumple de manera deficiente los tiempos de atención planteados ante las necesidades solicitadas, lo cual repercute negativamente en la operatividad y en la experiencia de los usuarios internos.
- Las auditorías externas e internas han evidenciado brechas en la gestión de accesos y custodia de información sensible, indicando el 75% del cumplimiento de buenas prácticas y estándares internacionales como la ISO/IEC 27001:2022.

1.2. Objetivos

1.2.1. Objetivo General

Diseñar e implementar un modelo de segregación de funciones con control híbrido de accesos mejora la gestión de la información sensible en una empresa comercializadora de bienes de capital y servicios.

1.2.2. Objetivos Específicos

- OE1: Identificar las deficiencias en el modelo actual de gestión de accesos y su impacto en la protección de la información sensible de la organización.
- OE2: Diseñar un modelo de control de accesos basado en roles de negocio y segregación de funciones, alineado a los procesos clave de la empresa.
- OE3: Implementar el modelo propuesto de segregación de funciones con control híbrido de accesos en un entorno de prueba, alineado a los procesos críticos de la organización.
- OE4: Validar la eficacia del modelo implementado mediante pruebas de concepto, evaluando indicadores de reducción de brechas de seguridad, cumplimiento normativo y mejora de la trazabilidad de accesos.

1.3. Justificación

La creciente digitalización de procesos empresariales ha incrementado significativamente la exposición de las organizaciones a riesgos relacionados con la seguridad de la información. En el caso particular de las empresas comercializadoras de bienes de capital y servicios, que operan con grandes volúmenes de datos sensibles —como información financiera, estratégica y de clientes—, una gestión deficiente de accesos puede comprometer no solo la confidencialidad de los datos, sino también la continuidad operativa, el cumplimiento normativo y la reputación institucional.

En este contexto, se identificaron deficiencias estructurales en el modelo de control de accesos de la empresa objeto de estudio, particularmente la ausencia de una matriz formal de roles y funciones, la falta de criterios claros para la asignación de privilegios, y una débil trazabilidad en la gestión de accesos. Estos hallazgos, señalados en informes de auditoría externa, motivaron la necesidad de implementar un modelo de control de accesos más robusto y alineado con las mejores prácticas internacionales.

La propuesta de implementar un modelo basado en la segregación de funciones (SoD) con un enfoque de control híbrido de accesos, que combine mecanismos físicos y

lógicos, busca mitigar estos riesgos mediante una administración precisa de los privilegios de acceso, alineada a los procesos de negocio. Esta aproximación permitirá fortalecer la seguridad de la información, mejorar la trazabilidad de acciones críticas en los sistemas y facilitar el cumplimiento de estándares como la ISO/IEC 27001:2022 y la Ley N° 29733 sobre protección de datos personales.

Asimismo, este trabajo contribuirá al desarrollo de soluciones replicables para otras organizaciones con necesidades similares, aportando valor tanto a nivel académico como empresarial, al integrar principios de ingeniería de sistemas, gestión de riesgos y gobierno de TI en una propuesta concreta, validada y alineada a las exigencias actuales en ciberseguridad corporativa.

De este modo, la investigación no solo responde a una problemática organizacional concreta, sino que aporta un modelo replicable y de bajo costo, contrastado experimentalmente, que fortalece la gestión de accesos en entornos ERP de gran escala.

1.4. Tipo de investigación

Según Hernández-Sampieri y Mendoza (2018), el estudio se enmarca en un diseño de investigación aplicada, dado que busca responder a una problemática práctica de la *Empresa* mediante la implementación de un modelo híbrido de control de accesos. Asimismo, se adopta un enfoque descriptivo y correlacional, puesto que no solo se caracterizan las brechas existentes en la gestión de accesos, sino que también se analiza la relación entre los diferentes modelos de control (RBAC, ABAC y Roles por Procesos) y su pertinencia para fortalecer la segregación de funciones. Además, la investigación asume un diseño no experimental y transversal, ya que los datos fueron recolectados en un único momento, sin manipular las variables de estudio.

1.5. Población

La población estuvo constituida por todos los colaboradores de la *Empresa* que tienen relación directa o indirecta con los procesos críticos gestionados en el sistema SAP. Cabe mencionar que este universo incluye al personal del área de Tecnologías de la Información, auditores internos y externos, así como usuarios de negocio con acceso a información

sensible en áreas funcionales clave como compras, finanzas, logística y contabilidad. Además, al tratarse de un grupo con responsabilidades diferenciadas sobre el uso, administración o supervisión de accesos, se garantizó que la muestra seleccionada representara de manera proporcional los roles y riesgos vinculados a la seguridad de la información.

1.6. Técnicas de recolección de datos

Para la recolección de datos se empleó la información generada directamente desde el sistema SAP, a través de la ejecución de reportes internos. En particular, se consideraron dos fuentes principales: el reporte de usuarios, que permitió identificar la totalidad de colaboradores con acceso al sistema, y el reporte de accesos y transacciones, que proporcionó el detalle de privilegios asignados y operaciones ejecutadas por cada usuario. Estos reportes constituyeron la base objetiva para el análisis, al ofrecer evidencia verificable de la asignación de roles, el uso de transacciones críticas y los posibles conflictos de segregación de funciones.

CAPÍTULO II- MARCO TEÓRICO

Se definen los siguientes conceptos claves que involucran el estudio referente al marco teórico.

2.1. Seguridad de la Información

La seguridad de la información comprende el conjunto de principios, políticas, prácticas y mecanismos técnicos orientados a proteger los activos informáticos frente a accesos no autorizados, modificaciones indebidas, pérdidas accidentales o destrucción deliberada (Zapata et al., 2015). Por tanto, su objetivo no es solo resguardar datos, sino también garantizar la continuidad del negocio y la confianza organizacional frente a riesgos internos o amenazas externas. Según la ISO/IEC 27001:2022, este enfoque se rige por tres principios fundamentales, conocidos como la tríada CIA: Confidencialidad, Integridad y Disponibilidad.

- Confidencialidad: busca asegurar que la información solo pueda ser accedida por personas, sistemas o entidades debidamente autorizadas, evitando filtraciones o exposiciones indebidas.
- Integridad: garantiza que los datos se mantengan completos, precisos y sin alteraciones no autorizadas, tanto en tránsito como en almacenamiento.
- Disponibilidad: implica que los sistemas y la información crítica estén accesibles en el momento en que se requieren, permitiendo operaciones ininterrumpidas y oportunas.

2.1.1. Sistema de Gestión de Seguridad de la Información

Bajo lo establecido en la ISO/IEC 27001:2022, un SGSI fortalece la gobernanza, reduce riesgos tecnológicos y optimiza la inversión en seguridad, aplicando controles organizacionales, físicos y tecnológicos. En ese sentido, un sistema de gestión de seguridad de la información (SGSI) no puede ser entendida únicamente como la aplicación de herramientas tecnológicas, sino como un sistema integral de control y gobierno que articula

procesos, roles, políticas de acceso, monitoreo constante y una cultura organizacional alineada con la protección de la información (Santos-Olmo et al., 2016).

En el contexto empresarial, especialmente en compañías que comercializan bienes de capital y servicios, la seguridad de la información es crucial debido al manejo de datos técnicos, financieros y estratégicos. Asimismo, organismos como ISACA (2021) destacan la importancia de alinear la gestión de información sensible con marcos de cumplimiento como la Ley de Protección de Datos Personales (LPDP) en el caso peruano, o el Reglamento General de Protección de Datos (GDPR) en contextos internacionales, ya que las brechas en la custodia de información crítica pueden traducirse en sanciones regulatorias severas o pérdida de confianza por parte de los stakeholders.

2.1.2. Gestión de Información Sensible

La gestión de la información sensible comprende el conjunto de acciones estratégicas y operativas orientadas a identificar, clasificar, proteger, almacenar, transferir y eliminar datos que, por su naturaleza, requieren un tratamiento especial. Esta categoría incluye información personal identificable (PII), datos financieros, registros contractuales, estrategias comerciales, archivos técnicos o cualquier otro activo informacional cuyo acceso indebido, modificación o pérdida pueda generar consecuencias legales, económicas o reputacionales para la organización (ISO/IEC 27701, 2020; NIST SP 800-122, 2021).

Según el NIST (2020) su adecuada administración requiere controles claros sobre el acceso, sustentados en principios como el menor privilegio, es decir, otorgar únicamente el acceso mínimo necesario a cada colaborador para el cumplimiento de sus funciones. Este principio, en conjunto con respaldados por políticas internas, tecnologías de protección y capacitación del personal, permite mantener un entorno informático resiliente y conforme a normativas de privacidad y ciberseguridad (ENISA, 2022).

En resumen, la gestión de información sensible no puede entenderse como un procedimiento aislado, sino como una dimensión estratégica del sistema de seguridad de la información de la organización, donde el equilibrio entre accesibilidad y control resulta clave para la continuidad operativa y la protección del valor informacional.



Figura 1. Diagrama de flujo de la gestión de información sensible

Nota. Elaboración propia a partir de ISO/IEC 27701 (2020), NIST SP 800-122 (2021) y ENISA (2022).

2.2. Segregación de Funciones (SoD)

La segregación de funciones (SoD, por sus siglas en inglés: *Segregation of Duties*) es un principio esencial de control interno que consiste en distribuir tareas y responsabilidades críticas entre diferentes personas o unidades, con el objetivo de reducir riesgos operacionales, prevenir fraudes y limitar la posibilidad de errores no detectados. Esta práctica, ampliamente reconocida en disciplinas como auditoría, ciberseguridad y cumplimiento normativo, se considera un pilar en la gestión de riesgos organizacionales (ISACA, 2020).

En el contexto de Tecnologías de la Información, la SoD adquiere una dimensión operativa clave. Por ejemplo, permitir que una sola persona diseñe, pruebe y despliegue una funcionalidad crítica incrementa considerablemente el riesgo de vulnerabilidades no

controladas. Del mismo modo, en plataformas ERP como SAP, separar funciones como crear proveedores, aprobar pagos y ejecutar transacciones resulta esencial para evitar conflictos de interés o accesos indebidos (NIST, 2020).

Al respecto, la norma internacional ISO/IEC 27001:2022, en su control 5.2, destaca explícitamente la importancia de distribuir roles y responsabilidades dentro del sistema de gestión de seguridad de la información, de manera que se reduzcan los riesgos relacionados con privilegios mal asignados y se facilite la trazabilidad de las acciones realizadas (ISO, 2022).

En suma, en la figura 2 se detalla un diagrama con procesos clave para la implementación efectiva de la SoD también requiere herramientas que automaticen la gestión de accesos, generen alertas ante violaciones de políticas, y permitan auditar configuraciones, perfiles y roles en tiempo real. De este modo, se fortalece la postura de seguridad y se facilita la adaptación a entornos regulados.



Figura 2. Diagrama de flujo de Segregación de Funciones

Nota. Elaboración propia a partir de ISACA (2020), ISO (2022) y NIST (2020).

2.3. Control de Accesos

Kayes et al. (2019) menciona que el control de accesos es una de las funciones más críticas dentro de la gestión de la seguridad de la información cuya finalidad es regular quién puede ingresar e interactuar con los activos físicos o digitales dentro de una organización. Por tanto, su correcta implementación permite minimizar el riesgo de accesos no autorizados y proteger la confidencialidad, integridad y disponibilidad de la información sensible. Además, a nivel técnico, los controles de acceso se dividen en lógicos, físicos e híbridos, cada uno con modelos específicos que varían en su complejidad, nivel de detalle y adecuación a distintos entornos de riesgo.

2.3.1. Control de acceso lógico

Este tipo de control se aplica sobre sistemas informáticos, redes, aplicaciones y bases de datos, permitiendo o denegando operaciones como la lectura, escritura, modificación o eliminación de información. Para ello, se utilizan modelos de control de acceso estructurados, entre los cuales destacan:

a) RBAC – Control de Acceso Basado en Roles

El Role-Based Access Control (RBAC) es un modelo de control de accesos que asigna permisos a roles predefinidos en lugar de hacerlo directamente a los usuarios; de esta manera, cada rol agrupa un conjunto de privilegios que los usuarios heredan al ser vinculados a él. Este enfoque, especialmente útil en organizaciones grandes y jerárquicas, facilita la administración al garantizar consistencia entre quienes comparten un rol, permite escalar el control en estructuras con miles de empleados y múltiples procesos críticos, y reduce costos de gestión; sin embargo, exige un diseño inicial riguroso, ya que una definición deficiente de roles puede derivar en vulnerabilidades de seguridad y dificultades administrativas (Fischer-Hellmann, 2012; Indenhaus, 2017).

Características

- El acceso se otorga en función de roles predefinidos.
- Cada rol agrupa un conjunto de permisos.
- Los usuarios se asignan a roles, no directamente a permisos.
- Facilita la administración en organizaciones grandes y jerárquicas.

Ventajas

- Es fácil de entender y administrar.
- Resulta eficiente para gestionar miles de usuarios.
- Garantiza que usuarios con el mismo rol tengan los mismos permisos.
- Al cambiar permisos, basta con modificar el rol en lugar de cada usuario.
- Permite implementar de manera práctica el principio de mínimo privilegio.

Desventajas

- Presenta poca flexibilidad para casos específicos o contextuales.
- Puede generar una proliferación de roles que dificultan la gestión.
- No considera atributos dinámicos como hora, ubicación o dispositivo.
- Depende de un diseño inicial cuidadoso para no comprometer la seguridad.

En suma, RBAC asigna permisos a roles definidos por la función organizacional; los usuarios heredan dichos permisos al ser adscritos a uno o varios roles. En esta línea, como se detalla en la Figura 3, su operación se sustenta en tres relaciones básicas (usuarios–roles–permisos) y en prácticas de role engineering para el alta, revisión y baja de privilegios. Es especialmente eficaz en entornos estables y jerarquizados (p. ej., ERP financieros), donde la estructura de procesos se traduce con facilidad en catálogos de roles mantenibles y auditables (Fischer-Hellmann, 2012).

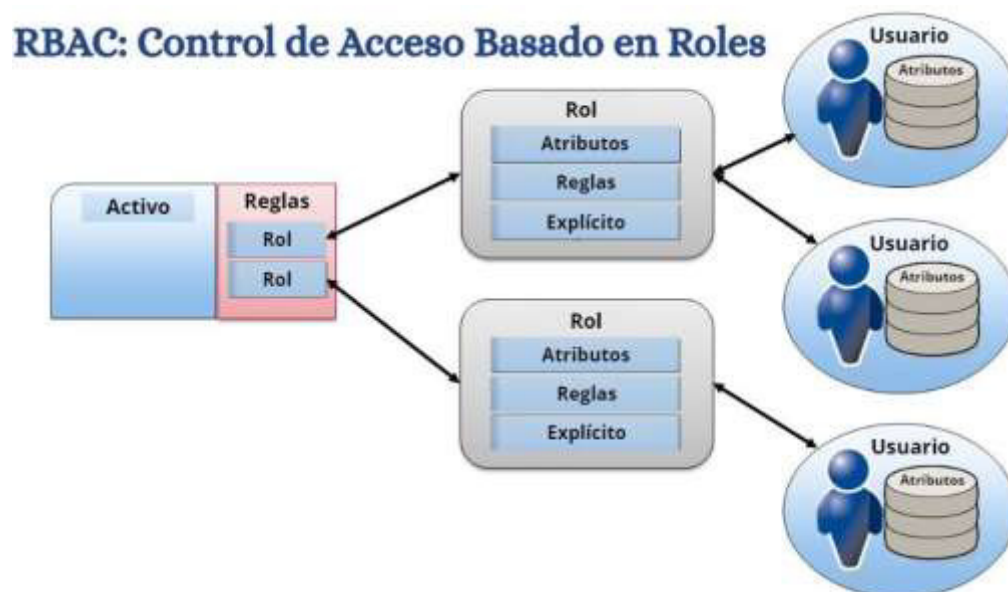


Figura 3. Esquema del modelo RBAC adaptado de Indenhaus (2017).

b) ABAC – Control de Acceso Basado en Atributos

Según Hu et al. (2020) y Huang et al. (2020) el modelo Attribute-Based Access Control (ABAC) decide autorizaciones a partir de atributos del sujeto, del recurso, de la acción y del entorno (ej.: unidad organizativa, criticidad del documento, operación solicitada, ubicación u horario), tal como se muestra en la figura 4. Las políticas se expresan de forma declarativa y se evalúan en un motor de decisión (PDP) que considera contexto y condiciones dinámicas, lo que habilita controles de acceso granulares y adaptativos en escenarios *cloud* o Zero Trust. Además, su adopción exige un gobierno de atributos (calidad, procedencia, ciclo de vida) y un diseño sólido de políticas para evitar ambigüedades.

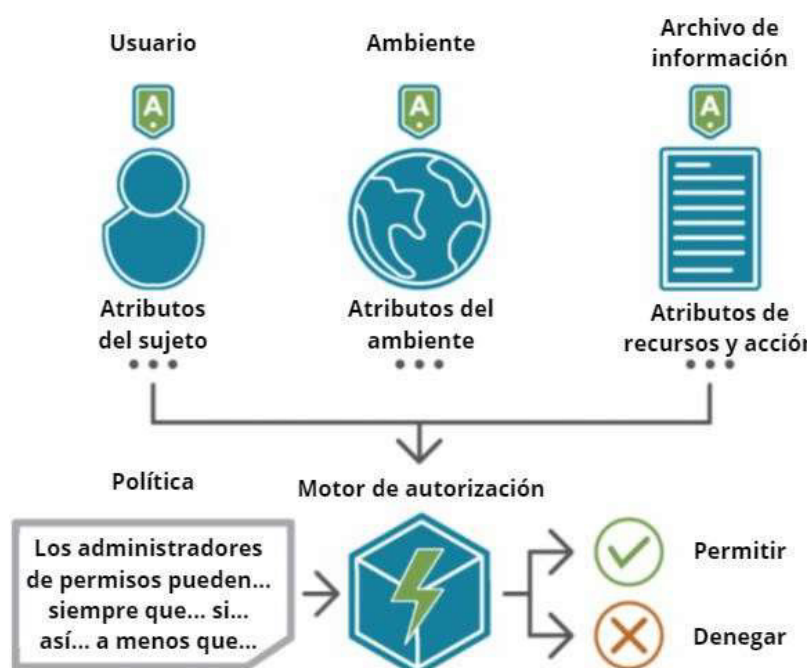


Figura 4. Esquema del modelo ABAC adaptado de Axiomatics (2018).

c) DAC y MAC – Modelos Discrecionales y Mandatorios

El Discretionary Access Control (DAC) otorga a los propietarios de los recursos la capacidad de definir quién puede acceder a ellos. Este modelo es más permisivo y adecuado para entornos de baja criticidad o uso personal. Por el contrario, el Mandatory Access Control (MAC) establece permisos a partir de políticas centralizadas y etiquetas de seguridad. En este caso, el sistema decide quién accede a qué recursos, sin intervención del usuario. Por ello, es común en entornos militares o clasificados, donde la confidencialidad es prioritaria (Hu et al., 2020).

d) Modelos emergentes y alternativos

Entre los enfoques emergentes destacan el Policy-Based Access Control (PBAC) y el Relationship-Based Access Control (ReBAC), que amplían las capacidades de los modelos tradicionales como RBAC y ABAC. Por su parte, el PBAC sobresale por su flexibilidad declarativa, al permitir definir y actualizar políticas independientes de la aplicación, lo que lo hace idóneo en entornos distribuidos y con microservicios; sin embargo, exige un diseño formal y auditorías continuas para evitar conflictos de reglas (Hu et al., 2020; Pal y Jadidi, 2021). Por otro lado, ReBAC introduce un criterio relacional, donde las decisiones de autorización dependen de vínculos explícitos entre entidades, lo que resulta útil en contextos colaborativos y redes sociales, aunque plantea retos de escalabilidad y gestión operativa (Fong, 2011; Rizvi et al., 2015). En comparación con RBAC y ABAC, que priorizan roles y atributos, estos modelos emergentes ofrecen mayor expresividad y adaptabilidad a entornos dinámicos, a costa de una mayor complejidad administrativa.

2.3.2. Control de acceso físico

El control de acceso físico acorde con lo mencionado por ENISA (2022), se refiere a la protección de espacios e infraestructuras sensibles, como centros de datos, salas de servidores o zonas restringidas. Así como se muestra en la figura 5, este tipo de control utiliza dispositivos y controles mecanismos que pueden incluir:

- Tarjetas RFID o magnéticas.
- Cerraduras electrónicas con autenticación por PIN o huella.
- Cámaras de videovigilancia integradas a sistemas de monitoreo.
- Control biométrico (huella, iris, rostro) para niveles altos de autenticación.

Según los enfoques actuales en seguridad física, no basta con controlar la entrada a un edificio; es necesario controlar los niveles internos de acceso según funciones, turnos o perfiles. Esto se alinea con la tendencia a integrar seguridad física y lógica.

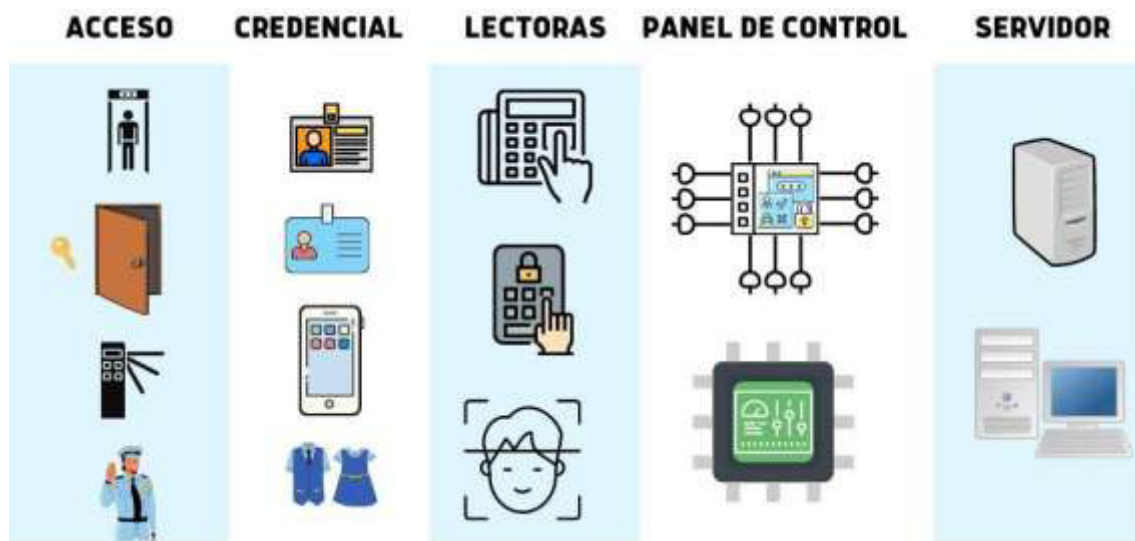


Figura 5. Esquema de los componentes de control de acceso físico (Sánchez, 2022).

2.3.3. Control híbrido de accesos RBAC-ABAC

El control híbrido según NIST (2020) integra las dimensiones física y lógica del acceso, reforzando así la seguridad integral del entorno organizacional. Este enfoque combina múltiples factores, como:

- Ingreso físico autorizado mediante control biométrico o tarjeta,
- Acceso lógico condicionado a variables contextuales (atributos, ubicación, MFA),
- Restricciones de horario, rol y recurso específico.

Por ejemplo, un analista financiero puede acceder al sistema SAP solo si:

1. Ha ingresado físicamente al edificio autorizado,
2. Ha autenticado su identidad con credenciales válidas,
3. Y está en horario laboral permitido.

Este tipo de control fortalece la trazabilidad de los accesos, reduce el riesgo de suplantación y permite una respuesta más rápida ante incidentes. Su adopción ha sido recomendada como parte del enfoque Zero Trust Architecture, donde apelan a siempre verificar los accesos otorgados.

Por otra parte, entre los modelos híbridos de acceso, el Graph-RBAC amplía el RBAC tradicional mediante grafos para consultas relacionales más expresivas. Los modelos temporales y contextuales (TBAC, CBAC, HBAC) incorporan restricciones dinámicas basadas en tiempo, ubicación, dispositivo o comportamiento, útiles en entornos móviles o remotos. Asimismo, los modelos híbridos (RBAC+ABAC o PRBAC) buscan combinar simplicidad y flexibilidad, aunque requieren una mayor coordinación entre capas y se recomiendan como complemento a un modelo base (Aftab et al., 2022; Mohamed et al., 2024).

En el caso del modelo híbrido RBAC–ABAC combina la estructura organizada del control de acceso basado en roles (RBAC) con la flexibilidad del control basado en atributos (ABAC). Este enfoque integra la asignación de permisos a roles predefinidos y, a la vez, introduce atributos dinámicos de usuarios, recursos, acciones y contexto, lo que permite decisiones de autorización más finas y adaptables a entornos cambiantes sin perder simplicidad administrativa (Fischer-Hellmann, 2012; Hu et al., 2020; Huang et al., 2020).

Características

- Combina roles (RBAC) con atributos de usuarios, recursos, acciones y contexto (ABAC).
- Los roles definen el marco general de permisos.
- Los atributos añaden granularidad y flexibilidad (ej. Hora, ubicación, clasificación de datos).
- Permite reglas de acceso más dinámicas sin perder la simplicidad de los roles.

Ventajas

- Escala de manera eficiente en organizaciones con grandes volúmenes de usuarios gracias a la organización de roles.
- Permite condiciones contextuales más precisas al incorporar atributos dinámicos.
- Refuerza la seguridad al reducir accesos innecesarios mediante filtros adicionales.
- Facilita el cumplimiento de regulaciones complejas al soportar políticas avanzadas de control.
- Optimiza la gestión al reutilizar roles y complementar con atributos que afinan el control.

Desventajas

- La administración resulta más compleja al requerir la definición y gestión conjunta de roles y atributos.
- La evaluación de atributos dinámicos puede generar sobrecarga en el desempeño de los sistemas.
- El diseño demanda una arquitectura clara para evitar conflictos o redundancias en permisos.
- La curva de aprendizaje es mayor y requiere capacitación especializada para los administradores.

2.3.4. Autorización por roles y procesos

La Autorización por Roles y Procesos representa una evolución del RBAC clásico, ya que no solo considera los roles de usuario, sino también las etapas o pasos específicos de un flujo de trabajo. Este modelo busca una alineación más estrecha entre la seguridad y los procesos de negocio, reforzando la segregación de funciones al restringir permisos en función de la fase del proceso en la que participa cada usuario (Hu et al., 2020; Huang et al., 2020).

Características

- El acceso se define en función de los roles organizacionales y las etapas de los procesos en los que interviene cada usuario.
- Un mismo rol puede asumir distintos permisos dependiendo del estado o fase del flujo de trabajo.
- Se alinea directamente la seguridad con la operación de los procesos de negocio.
- Refuerza la separación de funciones al evitar que un mismo usuario ejecute actividades incompatibles, como iniciar y aprobar un trámite.

Ventajas

- Asegura una mejor alineación con la operación real al vincular los permisos con la lógica de los procesos.
- Refuerza la seguridad al mitigar riesgos de fraude o conflictos de interés mediante la segregación de funciones.

- Facilita la trazabilidad al permitir auditar con precisión quién ejecutó cada acción y en qué fase del proceso.
- Implementa un control dinámico donde los permisos se ajustan automáticamente conforme avanza el flujo de trabajo.

Desventajas

- Su diseño es complejo, ya que requiere mapear en detalle los procesos y los roles asociados a cada etapa.
- El mantenimiento resulta costoso, ya que cualquier cambio en los procesos obliga a rediseñar las autorizaciones.
- Presenta menor flexibilidad ante accesos excepcionales o ad-hoc.
- Genera sobrecarga administrativa al demandar coordinación constante entre los equipos de seguridad y los responsables de negocio.

2.4. Normas y Estándares Aplicables

La gestión eficaz de la seguridad de la información requiere el alineamiento con marcos normativos y estándares internacionales reconocidos, que ofrecen lineamientos técnicos, organizacionales y legales para proteger los activos de información a lo largo de su ciclo de vida. Entre los más relevantes destacan:

- ISO/IEC 27001:2022: norma internacional que establece los requisitos para implementar y mantener un Sistema de Gestión de Seguridad de la Información (SGSI). Este estándar promueve un enfoque basado en riesgos, incluyendo controles técnicos y organizativos orientados a garantizar la confidencialidad, integridad y disponibilidad de la información (ISO, 2022).
- ISO/IEC 27002: actúa como complemento técnico a la norma anterior, proporcionando una guía detallada para la implementación de controles de seguridad, entre ellos la gestión de accesos, la segregación de funciones, el control de usuarios y la protección de entornos críticos (ISO, 2022).

- NIST SP 800-53 Rev. 5 y NIST SP 800-171: emitidos por el National Institute of Standards and Technology (NIST) de EE.UU., definen un conjunto estructurado de controles de seguridad divididos en categorías como acceso lógico, auditoría, respuesta a incidentes y protección de datos en sistemas federales y contratistas (NIST, 2020).
- Ley N.º 29733 — Ley de Protección de Datos Personales (Perú): norma que regula el tratamiento de los datos personales, obligando a las organizaciones a aplicar medidas de seguridad adecuadas para evitar su uso indebido, pérdida, acceso no autorizado o alteración indebida (Congreso de la República del Perú, 2011).

En síntesis, la presente investigación se fundamenta en principios internacionalmente aceptados para el diseño de soluciones seguras y confiables. Por ende, la segregación de funciones y el control de accesos, integrados bajo un enfoque normativo sólido, permiten reducir vulnerabilidades operativas, mitigar riesgos de incumplimiento y fortalecer la gestión de información sensible en entornos tecnológicos críticos.

2.5. Análisis comparativo de modelos de control de accesos y alineación con ISO/IEC 27001:2022

A continuación, en la tabla 1 se detalla el análisis comparativo de los principales modelos de control de accesos evidencia que su idoneidad depende del contexto organizacional, el nivel de granularidad requerido y la complejidad de administración que la entidad esté dispuesta a asumir. El modelo RBAC destaca por su simplicidad y su alineación natural con la segregación de funciones, lo que lo hace particularmente adecuado para estructuras corporativas jerarquizadas. En contraste, el modelo ABAC ofrece una mayor granularidad y flexibilidad contextual, aunque exige un esfuerzo adicional en la definición y mantenimiento de reglas. Asimismo, los modelos MAC y DAC representan enfoques opuestos: el primero privilegia la seguridad estricta a costa de una menor flexibilidad operativa, mientras que el segundo facilita la administración, pero incrementa el riesgo de errores humanos. Por su parte, PBAC y ReBAC resultan más apropiados en entornos con alta variabilidad, políticas dinámicas y estructuras relacionales complejas. Finalmente, la norma ISO/IEC 27001:2022 no prescribe un modelo específico, pero establece requisitos mínimos obligatorios y fomenta un enfoque basado en riesgos, lo que permite combinar

fortalezas de distintos modelos en soluciones híbridas adaptadas a las necesidades de cada organización.

Modelo	Base	Granularidad	Flexibilidad /Escalabilidad	Administración	Alineación con ISO 27001	Ventajas	Desventajas
RBAC	Roles	Media/Alta	Buena en jerarquías	Sencilla	Buena	Fácil de comprender, refuerza SoD	Baja personalización
ABAC	Atributos	Alta	Muy alta	Compleja	Muy buena	Gran granularidad y contexto	Difícil de gestionar a gran escala
DAC	Discrecional	Media	Alta poco controlada	Descentralizada	Limitada	Flexible, control por usuario	Riesgo de errores humanos
MAC	Etiquetas de seguridad	Alta	Muy baja	Centralizada estricta	Alta en entornos seguros	Muy seguro, mínimo privilegio	Rigidez extrema
PBAC	Políticas formales	Alta	Muy alta	Compleja pero formalizable	Excelente	Políticas auditables y escalables	Complejidad en la política
ReBAC	Relaciones	Alta	Alta	Compleja (grafos)	Emergente	Modelo social natural	Soporte limitado
ISO/IE C 27001 – A.9	No prescribe modelo específico	Según necesidad	Escalabilidad segura	Estructurado y auditable	Establece mínimos obligatorios	Establece controles mínimos obligatorios, fomenta enfoque de riesgos	Requiere diseño organizacional y análisis de riesgos

Tabla 1. Análisis comparativo de modelos de control de accesos y alineación con ISO/IEC 27001:2022

Elaboración propia a partir de Hathaliya & Tanwar (2024), Bian et al. (2024), Vu et al. (2018), Mohanprasath et al. (2023), Cao (2022) y Vogel (2016).

CAPÍTULO III- ESTADO DEL ARTE

El presente capítulo tiene como finalidad examinar los principales estudios relacionados con la segregación de funciones (SoD), el control de accesos y la gestión de información sensible mediante una revisión de la bibliografía. A diferencia de un listado descriptivo, esta revisión bibliográfica integra un análisis crítico que contrasta los enfoques, métricas e indicadores utilizados, así como los resultados obtenidos. Por ende, este procedimiento permite no solo identificar ventajas y limitaciones de los modelos revisados, sino también fundamentar la selección metodológica más apropiada para la organización en estudio.

Así, en el ámbito financiero, Cao (2022) aplicó un modelo RBAC tradicional en sistemas de gestión de información (MIS), evaluando indicadores como la eficiencia en la autenticación y la reducción de inconsistencias. Los resultados evidenciaron mejoras en control interno y trazabilidad de accesos, confirmando que la simplicidad del modelo favorece entornos donde las reglas son estables y el cumplimiento normativo es prioritario. Sin embargo, frente a modelos híbridos y adaptativos, el RBAC clásico mostró limitaciones en flexibilidad para responder a cambios contextuales o dinámicos, lo que restringe su aplicabilidad en organizaciones con alta variabilidad en procesos.

Por otro lado, Vogel (2016) analizó los desafíos de implementación del RBAC en grandes organizaciones multisistema, proponiendo una metodología progresiva de ingeniería de roles. Sus métricas incluyeron la reducción de sobreasignaciones y el alineamiento entre roles y permisos, demostrando que una gestión de roles bien diseñada mejora la auditabilidad y minimiza inconsistencias. En contraste con los hallazgos de Cao (2022), que destacan la utilidad del RBAC en escenarios normativamente estrictos, pero relativamente estáticos, Vogel subrayó que el éxito del modelo depende de una estrategia sólida de diseño de roles, lo que refuerza su vigencia como alternativa sostenible frente a la mayor complejidad de los modelos híbridos y basados en atributos.

En el sector farmacéutico, Hathaliya y Tanwar (2024) analizaron una cadena de suministro descentralizada, implementando un modelo híbrido RBAC–ABAC sobre blockchain. Se evaluaron métricas como latencia, trazabilidad e integridad, concluyendo que

la granularidad de los accesos se incrementaba y mejoraba la seguridad frente a adulteración de medicamentos. Sin embargo, la dependencia de blockchain elevó la complejidad tecnológica, lo que limita su adopción en organizaciones con recursos más reducidos.

Por su parte, Bian et al. (2024) aplicaron este mismo modelo híbrido al sector salud, donde la protección de registros médicos requiere altos niveles de confidencialidad y disponibilidad. Se midieron indicadores como accesos autorizados, disponibilidad del sistema y tiempos de consulta, obteniendo mejoras en seguridad y administración dinámica de datos sensibles. A diferencia del caso farmacéutico, esta investigación mostró que la implementación podía hacerse sin infraestructura blockchain, lo que la vuelve más escalable en entornos hospitalarios. En comparación con Hathaliya y Tanwar (2024), ambos estudios confirman la capacidad de granularidad y adaptabilidad del modelo híbrido, aunque difieren en su costo tecnológico y nivel de complejidad.

En un escenario distinto, Mohanprasath et al. (2023) propusieron un modelo adaptativo para entornos abiertos como redes Wi-Fi públicas y campus educativos, combinando RBAC y ABAC con detección de anomalías y análisis de comportamiento. Se evaluaron indicadores como tasa de detección, falsos positivos y tiempo de reacción, evidenciando que la respuesta en tiempo real fortalece la protección frente a accesos no autorizados. No obstante, en contraste con los entornos empresariales más cerrados, el modelo mostró un mayor costo operativo, ya que la supervisión de falsos positivos incrementa la complejidad de gestión.

Vu et al. (2018) aplicaron el enfoque por roles y procesos en sistemas ERP basados en microservicios, donde la asignación granular de permisos es crítica para evitar conflictos de roles y violaciones de seguridad. Su modelo integró autorizaciones dinámicas ligadas a procesos y roles, evaluando métricas como la cantidad de conflictos detectados y el tiempo de provisión de accesos. Los resultados evidenciaron resiliencia y capacidad de adaptación frente a cambios organizacionales, sin necesidad de rediseñar la estructura del sistema. A diferencia de los modelos híbridos aplicados en salud y farmacéutica, que priorizaron la seguridad de la información sensible, este antecedente pone énfasis en la eficiencia operativa, la reducción de conflictos internos y la provisión ágil de accesos en entornos empresariales complejos.

En todos los casos revisados se observa que la segregación de funciones, junto con distintos modelos de control de accesos, cumple un papel clave para fortalecer la gestión de la información sensible en organizaciones de distintos sectores y tamaños. Las investigaciones analizadas muestran que, aunque cada modelo —como RBAC, ABAC o Roles y Procesos— ofrece ventajas particulares, su efectividad real depende del equilibrio que logren entre seguridad, flexibilidad y facilidad de aplicación en el entorno de trabajo (Bian et al., 2024; Cao, 2022; Hathaliya y Tanwar, 2024; Mohanprasath et al., 2023; Vogel, 2016; Vu et al., 2018). De esta manera, las tendencias actuales apuntan hacia soluciones híbridas que combinan lo mejor de cada enfoque, brindando una gestión de accesos más adaptable y segura, pero también práctica y sostenible para las necesidades operativas y normativas de las empresas.

A continuación, se establecen criterios que servirán como base para la comparación de los modelos estudiados en el estado del arte, mostrados en la Tabla 2, basados en diversas características y funcionalidades.

Flexibilidad: evalúa la capacidad del modelo para adaptarse a distintos contextos, condiciones dinámicas y escenarios organizacionales cambiantes. Es de relevancia alta, y se califica de 0 a 5, donde valores más altos reflejan mayor adaptabilidad.

Facilidad de administración: mide el grado de simplicidad en la asignación, mantenimiento y ajuste de permisos dentro del modelo de control de accesos. Es de relevancia media, y se califica de 0 a 5, donde un valor mayor representa menor esfuerzo administrativo.

Seguridad y granularidad: determina el nivel de precisión en la definición de accesos y la capacidad de restringir privilegios de forma controlada y detallada. Es de relevancia muy alta, y se califica de 0 a 5, siendo las puntuaciones más altas indicativas de mayor robustez en seguridad.

Escalabilidad: analiza el rendimiento del modelo en organizaciones de gran tamaño o con estructuras complejas, considerando su capacidad de crecer sin perder eficiencia. Es de relevancia alta, y se califica de 0 a 5, siendo las puntuaciones más altas, las que reflejan un mejor desempeño en entornos masivos.

Alineación con procesos de negocio: considera el grado en que el modelo de control de accesos refleja y se integra con la lógica de los procesos operativos de la organización. Es de relevancia alta, y se califica de 0 a 5, siendo las puntuaciones más altas aquellas que muestran un mayor ajuste a la operatividad real.

Criterios	RBAC	RBAC+ABAC	Roles y procesos
Flexibilidad	2	3	2
Facilidad de administración	3	2	2
Seguridad y granularidad	2	3	3
Escalabilidad	3	3	2
Alineación con procesos	1	2	3
	11	13	12

Tabla 2. Comparación de las características de los estudios incluidos en el estado de arte

La elección del modelo híbrido propuesto según los resultados de la Tabla 2, responde a la necesidad de equilibrar flexibilidad, facilidad de administración, seguridad, escalabilidad y alineación con los procesos de negocio. En primer lugar, la combinación de RBAC y ABAC aporta reglas dinámicas basadas en atributos como ubicación, horario o dispositivo, lo que permite ajustar el acceso de manera contextual. A esto se suma el modelo de Roles y Procesos, que asegura que los permisos se otorguen en el momento adecuado del flujo operativo, garantizando la segregación de funciones y evitando que un mismo usuario concentre tareas incompatibles.

En segundo lugar, la facilidad de administración se ve reforzada porque RBAC simplifica la asignación inicial de permisos mediante roles, mientras que ABAC agrega un nivel adicional de filtros que, sin la estructura de roles, resultaría complejo de manejar. La incorporación de Roles y Procesos facilita la gestión al vincular los accesos con actividades de negocio ya conocidas por la organización, haciendo que el control sea comprensible para los equipos técnicos y de gestión.

En cuanto a seguridad y granularidad, el modelo híbrido maximiza la precisión al combinar condiciones contextuales de ABAC con la segregación propia de Roles y Procesos, lo que reduce accesos indebidos, previene fraudes y refuerza la trazabilidad de cada acción. En paralelo, la escalabilidad se sostiene en la estructura de roles de RBAC y en la transversalidad de reglas que aporta ABAC, mientras que el componente de procesos se aplica únicamente en etapas críticas, evitando sobrecargar todo el sistema.

Finalmente, este modelo ofrece la ventaja de alinear de forma más estrecha la seguridad con la lógica operativa real. RBAC por sí solo carece de conexión con los procesos, y aunque ABAC aproxima el control al contexto, es el modelo de Roles y Procesos el que garantiza que la protección se ajuste a cada fase del flujo de trabajo. En suma, esta evaluación respalda la propuesta de un modelo híbrido (RBAC + ABAC + Roles y procesos) reforzado con lineamientos de ISO/IEC 27001 para asegurar trazabilidad, control y consistencia en la segregación de funciones en *la Empresa*.

CAPÍTULO IV IMPLEMENTACIÓN

4.1. Introducción breve

Previo al diseño del nuevo modelo de segregación de funciones (SoD) y del sistema automatizado para su implementación, se realizó un diagnóstico integral del esquema vigente de gestión de accesos en SAP de *la Empresa*. El análisis reveló debilidades críticas como la inexistencia de un proceso formal para alta, revisión y baja de privilegios, ausencia de métricas objetivas, presencia de cuentas genéricas sin responsable y controles correctivos dependientes de revisiones manuales. Estas carencias generaban visibilidad limitada del riesgo, demoras en la mitigación de accesos indebidos y falta de trazabilidad en decisiones de asignación, lo que comprometía la eficacia de los controles exigidos por ISO/IEC 27001 y aumentaba la exposición a incidentes de seguridad. En respuesta, se desarrolló una propuesta alternativa al módulo SAP Access Control (*Compliance*), priorizando la eficiencia y el bajo costo de implementación.

A continuación, en la Tabla 3, se presenta la comparación entre el sistema desarrollado y el módulo oficial SAP Access Control (Compliance). Mientras la solución de SAP exige licencias adicionales, infraestructura dedicada y un equipo especializado, el sistema propuesto integra datos de SAP en un entorno de hoja de cálculo, reduciendo de manera significativa tanto los costos iniciales como los recurrentes. Pese a su simplicidad, conserva la capacidad de detectar conflictos en tiempo real, generar reportes trazables y alinearse con los controles ISO/IEC 27001. La propuesta destaca por su flexibilidad de personalización y por el uso de indicadores adaptados (% de privilegios excesivos corregidos y % de resolución de conflictos SoD), lo que la hace más accesible y funcional en organizaciones con restricciones presupuestales. No obstante, frente a SAP Access Control —que ofrece mayor escalabilidad y certificación oficial—, el sistema desarrollado presenta limitaciones en alcance multisistema y en aval formal, aunque resulta más viable para entornos donde se priorizan la eficiencia operativa y la continuidad del negocio.

Criterio	SAP Acces Control (Compliance)	Sistema desarrollado
Costo de implementación	Elevado: requiere licencias adicionales, infraestructura dedicada y equipo especializado.	Bajo: aprovecha entornos existentes (hojas de cálculo), sin costos de licencias adicionales.
Costo de operación	Recurrente y alto, asociado a mantenimiento, actualizaciones y soporte especializado.	Reducido: mantenimiento mínimo y adaptable a personal interno.
Complejidad de implementación	Alta: exige conocimientos avanzados en SAP y configuraciones extensas.	Media-baja: parametrización sencilla y rápida integración con datos de SAP.
Funcionalidad principal	Amplia: gestión integral de accesos, auditoría avanzada, integración nativa con otros módulos SAP.	Enfocada: detección de conflictos SoD, reportes trazables, control de accesos basado en RBAC.
Limitaciones	Elevado costo, rigidez y dependencia del proveedor	Escalabilidad limitada, no cuenta con certificación oficial.

Tabla 3. Comparación entre SAP Access Control (Compliance) y el sistema desarrollado

4.2. Diseño y desarrollo del modelo propuesto

4.2.1. Descripción funcional del sistema desarrollado

El núcleo de la solución se encuentra en un sistema desarrollado a medida, diseñada para gestionar de manera automatizada la segregación de funciones (SoD) y el control de accesos en el entorno actual de la empresa. Así, la estructura lógica del sistema refleja el modelo híbrido, en el cual los permisos se asignan a roles predefinidos y no directamente a los usuarios, lo que reduce la complejidad en la gestión y fortalece el control interno. Con este enfoque, se permite registrar y administrar los roles de usuario, identificar conflictos de funciones según las políticas de la empresa y generar reportes de auditoría para el seguimiento de accesos. Asimismo, produce un informe de segregación de funciones orientado a la interpretación por parte de la gestión empresarial, detallando información del usuario, contexto organizacional, identificación de riesgos y métricas de uso de transacciones. Todo ello se realiza en cumplimiento con los controles establecidos por la norma ISO/IEC 27001 según sus controles específicos.

4.2.2. Integración de lineamientos ISO/IEC 27001:2022

El sistema implementa controles específicos alineados con la norma ISO/IEC 27001:2022, especialmente los asociados con:

- A.5.12 – Clasificación de la información: identificación y etiquetado de datos sensibles para su adecuada protección.
- A.5.13 – Manejo de activos de información: aplicación de medidas de seguridad según la clasificación de la información.
- A.5.15 – Alta, modificación y baja de accesos de usuarios: control integral del ciclo de vida de credenciales y permisos.
- A.5.16 – Revisión de derechos de acceso de los usuarios: verificación periódica para detectar accesos obsoletos o innecesarios.
- A.5.17 – Gestión de credenciales secretas de autenticación: eliminación de cuentas genéricas o compartidas sin trazabilidad.
- A.5.18 – Acceso a la información y a los recursos de la información: asignación de accesos de acuerdo con necesidades de negocio y criterios de seguridad.
- A.5.19 – Segregación de tareas: separación de funciones incompatibles para mitigar riesgos de fraude o error.
- A.8.2 – Privilegios de acceso: asignación y revisión periódica de privilegios administrativos.
- A.8.10 – Eliminación o destrucción segura de información: prevención de exposición de datos tras su eliminación.
- A.8.24 – Protección de la información en tránsito: resguardo de datos durante su transmisión entre sistemas.
- A.8.25 – Protección de la información en reposo: aseguramiento de datos almacenados frente a accesos no autorizados.

Estos controles han sido adaptados al contexto de la empresa, garantizando que la asignación de roles y permisos cumpla con los principios de mínima autoridad y necesidad de conocer. A continuación, en la tabla 3 se muestran dichos controles y su correlación con las funciones del sistema.

Control ISO/IEC 27001:2022	Descripción del control	Funcionalidad específica del sistema
A.5.18 – Acceso a la información y a	Los accesos deben otorgarse según las	Configuración de matriz de roles y funciones vinculadas a transacciones SAP,

los recursos de la información	necesidades de negocio y criterios de seguridad.	con validación contra criterios de riesgo definidos.
A.5.15 – Alta, modificación y baja de accesos de usuarios	Controlar todo el ciclo de vida de credenciales y permisos.	Registro, revisión y actualización automatizada de accesos, con trazabilidad de modificaciones y revocaciones.
A.8.2 – Privilegios de acceso	Asignar y revisar privilegios administrativos periódicamente.	Reporte detallado de privilegios y funciones críticas asignadas, con posibilidad de auditoría y justificación por área responsable.
A.5.16 – Revisión de derechos de acceso de los usuarios	Revisar periódicamente los accesos para identificar cuentas obsoletas.	Ejecución de reportes para detectar usuarios con transacciones no acordes a su rol o sin actividad reciente.
A.5.17 – Gestión de credenciales secretas de autenticación	Evitar cuentas genéricas o compartidas sin trazabilidad.	Identificación de cuentas sin responsable asignado y recomendación de su desactivación.
A.5.12 – Clasificación de la información	Identificar y etiquetar datos sensibles.	Etiquetado de información crítica en reportes, distinguiendo funciones y transacciones de alto riesgo.
A.5.13 – Manejo de activos de información	Proteger datos según su clasificación.	Control de acceso diferenciado para datos y funciones según nivel de criticidad.
A.8.10 – Eliminación o destrucción segura de información	Evitar la exposición de datos eliminados.	Validación de accesos para asegurar que usuarios sin autorización no puedan recuperar datos eliminados.
A.8.24 – Protección de la información en tránsito	Proteger datos durante su transmisión.	Uso de entornos seguros para la extracción y carga de datos de SAP al sistema.
A.8.25 – Protección de la información en reposo	Proteger datos almacenados.	Repositorio seguro para almacenamiento de reportes generados, con acceso restringido.
A.5.19 – Segregación de tareas	Separar funciones incompatibles para reducir riesgos de fraude o error.	Generación automática de combinaciones de funciones (F1 vs F2) y detección de conflictos para impedir acumulación de funciones incompatibles.

Tabla 4. Correspondencia entre controles ISO/IEC 27001 y funcionalidades del sistema de análisis SoD

4.2.3. *Arquitectura y flujo de operación*

El flujo de trabajo propuesto para la gestión y análisis de segregación de funciones se articula en cinco etapas claramente definidas, que en conjunto configuran un proceso estructurado y trazable. En primer lugar, se desarrolla la **matriz de segregación de**

funciones presentada en la figura 6, construida de manera colaborativa con las distintas áreas de negocio —entre ellas Compras, Logística, Finanzas y Contabilidad—, donde se identifican los puntos críticos y riesgos operativos percibidos por cada frente. A partir de esta información, se transforma el insumo inicial en un modelo técnico que asocia roles, transacciones y objetos de autorización, estableciendo de forma explícita las combinaciones de funciones conflictivas (F1 frente a F2) que podrían generar vulnerabilidades en el control de accesos.

Figura 6. Matriz de segregación de funciones validada con criterios F1-F2.

Posteriormente, como se muestra en la figura 7, se ejecuta la etapa correspondiente a la **matriz generadora de funciones (F1 y F2)**, que recibe como entrada las transacciones efectivamente asignadas a cada usuario en el sistema SAP S/4HANA. En este módulo, las funciones y transacciones se vinculan inicialmente en las columnas A y B, mientras que en las columnas D a F se registran los usuarios junto con las transacciones que tienen habilitadas. Mediante la activación del botón *Ejecutar*, el sistema procesa la información y genera automáticamente la relación usuario-función-transacción, facilitando un mapeo integral del acceso real.

Figura 8. Reporte de combinaciones de funciones con conflictos detectados.

Nota. Captura posterior a la ejecución del “Generador”, mostrando las combinaciones obtenidas y la marcación de posibles conflictos de segregación de funciones.

La cuarta fase corresponde a la elaboración del **informe de segregación de funciones** mostrado en la figura 9, documento orientado a la interpretación por parte de la gestión empresarial, que presenta de manera estructurada los datos relevantes del trabajador, tales como usuario, nombre, función, departamento, empresa, holding, país, identificador de riesgo y valoración de las funciones implicadas, además de métricas de frecuencia de uso de las transacciones. Este informe traduce la complejidad técnica en un formato accesible para la toma de decisiones gerenciales, sin perder el rigor analítico que demanda la seguridad de la información.

ID	Nombre	Función	Departamento	Empresa	Holding	País	Proceso	Conflicto	Valoración	Func1	Descr Func1	Func2	Descr Func2	Func3	Descr Func3
00000001	GONZALEZ FLORES VISCARRA	ASISTENTE ADMINISTRATIVO	MANTENIMIENTO	RACIONALIZA CON EMPRESARIAL S.A. - ACP	Otros	Perú	OTC	OTC-004	Alto	PR02	Crear/Modificar pedidos de compra	ME21 (4206), ME21N (302), ME22 (302), ME21M (332)	Recepcionar pedidos adquiridos en el extranjero	MM02	MM02 (2645)
00000002	GUADALUPE NERY VANGUO VANGUO	AUXILIAR ADMINISTRATIVO	MANTENIMIENTO	RACIONALIZA CON EMPRESARIAL S.A. - ACP	Otros	Perú	OTC	OTC-008	Alto	AR03	Aplicar pagos a deudas de clientes	F-04 (1710), F-28 (1), F-28 (1), F-40 (1), F-82 (1)	Crear Facturas de Clientes (Contabilidad)	AR07	F-01 (309)
00000003	GUADALUPE NERY VANGUO VANGUO	AUXILIAR ADMINISTRATIVO	MANTENIMIENTO	RACIONALIZA CON EMPRESARIAL S.A. - ACP	Otros	Perú	OTC	OTC-008	Alto	AR06	Crear Notas de Crédito a Clientes (Contabilidad)	F-27 (1), F-81 (309)	Mantener el Maestro de Clientes	SD03	FD03 (38), FD03 (1)
00000004	GUADALUPE NERY VANGUO VANGUO	AUXILIAR ADMINISTRATIVO	MANTENIMIENTO	RACIONALIZA CON EMPRESARIAL S.A. - ACP	Otros	Perú	OTC	OTC-038	Alto	AR03	Aplicar pagos a deudas de clientes	F-04 (1710), F-28 (1), F-28 (1), F-40 (1), F-82 (1)	Mantener el Maestro de Clientes	SD03	FD03 (38), FD03 (1)
00000005	GUADALUPE NERY VANGUO VANGUO	AUXILIAR ADMINISTRATIVO	MANTENIMIENTO	RACIONALIZA CON EMPRESARIAL S.A. - ACP	Otros	Perú	OTC	OTC-030	Medio	SD03	Mantener el Maestro de Clientes	FD03 (38), FD03 (1)	Crear Facturas de Clientes (Contabilidad)	AR07	F-01 (309)
00000006	LUIS ALFREDO GUZMAN PAREDES	ASISTENTE ADMINISTRATIVO	JEFATURA DE OPERACIONES	RACIONALIZA CON EMPRESARIAL S.A. - ACP	Otros	Perú	OTC	OTC-007	Alto	AR05	Facturar pedidos de clientes	VPR1 (3811), VPR2 (170), VPR4 (1), ZSDPR03 (420)	Anular Facturas	AR08	VPR1 (3811)
00000007	LUIS ALFREDO GUZMAN PAREDES	ASISTENTE ADMINISTRATIVO	JEFATURA DE OPERACIONES	RACIONALIZA CON EMPRESARIAL S.A. - ACP	Otros	Perú	OTC	OTC-034	Alto	SD05	Crear / Modificar de Pedidos de ventas	VAR0 (7772), VAR2 (1438), VSD254 (1), FSD1003 (1)	Facturar pedidos de clientes	AR05	VPR1 (3811), VPR2 (170), VPR4 (1), ZSDPR03 (420)

Figura 9. Informe de SoD con identificación de riesgos y frecuencia de uso.

Nota. Captura del reporte final generado por el sistema, destacando las columnas con ID de riesgo y el número de veces que cada transacción fue utilizada en el periodo evaluado.

Finalmente, se lleva a cabo la **validación con el negocio**, en la que participan la empresa, la gerencia y el área operativa del trabajador involucrado, tal como se ve en la figura 10. En esta etapa, se revisa cada caso identificado, registrando en las columnas R y S tanto el estado como la justificación proporcionada por las partes responsables. Finalmente, este cierre asegura que cada hallazgo no solo sea técnicamente detectado, sino también analizado, documentado y, de ser necesario, gestionado con acciones correctivas oportunas y en cumplimiento con los controles establecidos por la norma ISO/IEC 27001.

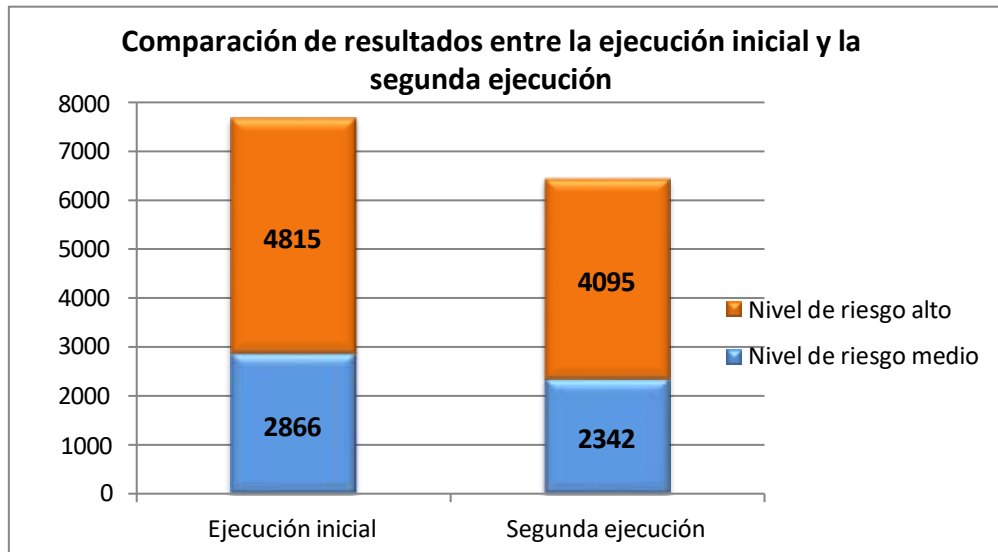


Figura 11. Comparación de resultados entre la ejecución inicial y la segunda ejecución

En la Figura 12 se observa el análisis del estado de los conflictos tras la respuesta de las áreas responsables evidenció que el 26 % de los casos de nivel de riesgo alto y el 16 % de los casos de nivel de riesgo medio fueron eliminados, mientras que el 37 % de los conflictos de nivel de riesgo alto y el 21 % de los de nivel de riesgo medio se mantienen por necesidades operativas justificadas. Estos resultados demuestran que, si bien el modelo facilita una reducción sustancial de accesos innecesarios, también preserva aquellas excepciones operativas debidamente documentadas, lo que refleja un balance entre seguridad y continuidad operativa, en concordancia con las mejores prácticas de seguridad de la información y con los controles establecidos en ISO/IEC 27001:2022, particularmente en los apartados A.5.15, A.5.18 y A.5.19.

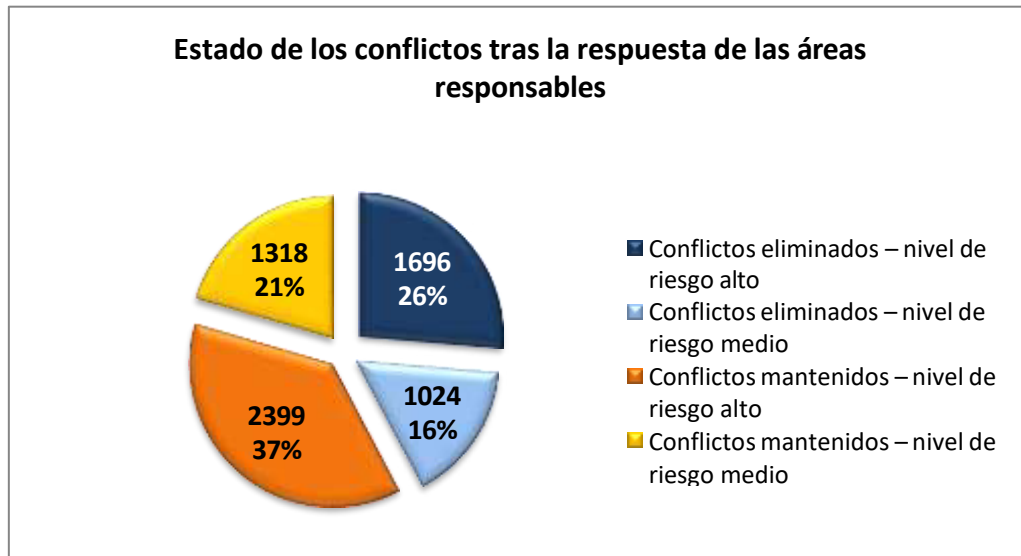


Figura 12. Estado de los conflictos tras la respuesta de las áreas responsables.

Además, la validación se midió mediante los siguientes **KPI definidos para la implementación**:

- **KPI 1: Porcentaje de cuentas con privilegios excesivos identificados y corregidos** (Figura 13)

El sistema permitió detectar usuarios con accesos no alineados a sus funciones reales y aplicar las correcciones necesarias. El objetivo definido fue mantener este indicador por debajo del **5%**, alineado con ISO/IEC 27001 (A.9.2 – Gestión de acceso de usuarios).



Figura 13. KPI 1: % de cuentas con privilegios excesivos

- **KPI 2: Número de conflictos de Segregación de Funciones (SoD) detectados vs. resueltos.** (Figura 14)

Se evaluó la proporción de conflictos detectados y efectivamente corregidos. El objetivo planteado fue alcanzar una **resolución superior al 90%**, indicador que refuerza la eficiencia del sistema frente a la permanencia de accesos indebidos.



Figura 14. KPI 2: % de conflictos de SoD resueltos

El uso de estos KPI permitió demostrar no solo la reducción en el número total de conflictos, sino también una **mejor capacidad de auditoría y control interno**, reflejada en mayor trazabilidad de decisiones, eliminación de cuentas innecesarias y menor tiempo de corrección (MTTR).

En conjunto, el análisis preliminar de costo-beneficio muestra que el sistema desarrollado internamente representó una alternativa significativamente más económica frente a la adquisición e implementación de un software especializado como SAP Access Control. Esto se refiere a que, mientras que la solución oficial demanda licencias adicionales, infraestructura y personal altamente especializado, la propuesta propia se construyó con talento interno y aprovechando herramientas ya disponibles, lo que redujo de forma considerable los costos iniciales y de operación. A ello se suma el beneficio indirecto derivado de incidentes evitados, como fraudes, duplicidad de pagos o accesos indebidos, los cuales hubiesen generado sanciones, auditorías adicionales y pérdida de confianza organizacional. Entonces, esta solución evidencia que una estrategia de seguridad diseñada internamente puede cerrar brechas críticas de seguridad con un nivel de inversión menor y un retorno más tangible en términos de continuidad operativa y reducción de riesgos.

Finalmente, si bien la implementación desarrollada ha demostrado ser efectiva al integrar controles de acceso mediante un sistema basado en Excel y macros, es necesario reconocer que, como oportunidad de mejora y evolución tecnológica, se proyecta una segunda fase orientada a la integración con plataformas más robustas, como SIEM o IAM corporativos, que permitan consolidar el monitoreo en tiempo real, automatizar alertas y establecer mayores niveles de control. Este avance no solo reforzaría la capacidad de respuesta ante incidentes de seguridad, sino que también garantizaría una integración más amplia con la infraestructura tecnológica de la empresa, asegurando continuidad, eficiencia y un alineamiento más sólido con los estándares internacionales de gestión de la seguridad de la información.

En resumen, como parte del análisis de impacto organizacional se evidenció que la implementación del sistema desarrollado no solo redujo en un 16.2% los conflictos de acceso y mejoró indicadores clave como la corrección de privilegios excesivos y la resolución de conflictos SoD, sino que también generó beneficios tangibles en la operación. Además, los usuarios clave percibieron mayor claridad en la asignación de roles, la trazabilidad fortaleció la confianza en las decisiones de seguridad y la reducción de cuentas innecesarias disminuyó las incidencias en mesa de ayuda. En ese sentido, este balance entre seguridad y continuidad operativa demuestra que el modelo no solo optimiza el control de accesos, sino que además contribuye a la eficiencia y usabilidad en la gestión diaria, fortaleciendo la cultura de control interno en la organización.

Capítulo V DISCUSIÓN, CONCLUSIONES Y RECOMENDACIONES

5.1. Discusión

El presente capítulo tuvo como propósito analizar los hallazgos derivados de la implementación de un modelo híbrido de control de accesos que integra RBAC, ABAC y Roles y Procesos en la empresa, contrastándolos con la literatura y con modelos aplicados en otros contextos. El análisis permitió identificar tensiones recurrentes en la gestión de accesos y, al mismo tiempo, evidenciar oportunidades de mejora sustentadas en experiencias comparativas.

En primer lugar, se observó la tensión entre eficiencia operativa y control de accesos. En la práctica, los usuarios tendían a solicitar privilegios adicionales para acelerar sus actividades, lo cual contravenía los principios de segregación de funciones (SoD). Esto coincide con lo señalado por Vogel (2016), quien advirtió que el éxito del RBAC depende de una adecuada ingeniería de roles, y con lo expuesto por Cao (2022), que destacó cómo la ausencia de validaciones rigurosas conduce a acumulaciones riesgosas. Frente a ello, la incorporación del enfoque de Roles y Procesos resultó clave para asegurar que cada autorización se otorgue en la fase correspondiente del flujo de trabajo, reduciendo la concentración de privilegios en un solo usuario y, por tanto, el riesgo de abuso.

En segundo término, se evidenció la insuficiencia de los controles manuales frente a la velocidad de los tecnológicos. Las revisiones periódicas que realizaba la empresa resultaban tardías e incapaces de detectar conflictos en tiempo real. La integración de una macro vinculada al ERP permitió superar esta limitación, en línea con lo observado por Vu et al. (2018), quienes subrayan la importancia de controles adaptativos en entornos dinámicos. Sin embargo, a diferencia de los modelos implementados en sectores como salud o farmacéutica (Hathaliya y Tanwar, 2024; Bian et al., 2024), donde se prioriza la granularidad extrema sobre la información sensible, en este caso se buscó un equilibrio más pragmático: contar con mecanismos ágiles y costo-efectivos que prevengan conflictos sin rediseñar la arquitectura de accesos.

Asimismo, la discusión puso en evidencia limitaciones en la madurez de la gestión de accesos: la falta de un modelo consolidado de roles, la existencia de criterios

fragmentados y una cultura débil de control interno. Tal situación se asemeja a lo planteado por Mohanprasath et al. (2023), quienes advierten que los modelos híbridos requieren ajustes permanentes y métricas confiables para evitar falsos positivos. En esta línea, la incorporación de indicadores objetivos como reducción del 16.2% en conflictos detectados, eliminación del 26% de riesgos altos y trazabilidad en la resolución de accesos, refuerza la pertinencia del modelo híbrido, pues combina la consistencia del RBAC, la flexibilidad contextual del ABAC y la trazabilidad propia de Roles y Procesos.

También se confirmó que el tamaño y el giro del negocio inciden en la aplicación de la SoD. Aunque la empresa no enfrenta regulaciones tan estrictas como en el sector financiero, el manejo de contratos de alto valor y activos críticos demanda controles equivalentes. Esto coincide con lo observado en el sector salud por Bian et al. (2024), donde un incumplimiento parcial de normas internacionales como la ISO/IEC 27001 compromete la continuidad operativa.

Por otra parte, la resistencia al cambio se identificó como un desafío recurrente. Algunos usuarios percibieron la segregación de funciones como una restricción a su autonomía, lo que pone de relieve que la sostenibilidad del modelo depende tanto de la tecnología como de estrategias de comunicación y capacitación. Este componente humano se convierte en un factor decisivo para lograr la aceptación y consolidación del modelo híbrido.

Finalmente, cabe destacar que SAP Access Control en S/4HANA constituye una solución avanzada y automatizada, capaz de acelerar los tiempos de detección y resolución de conflictos, además de ofrecer simulaciones de impacto previas a la aplicación de cambios (SAP, 2024; Answerthink, 2024). Sin embargo, su principal limitación radica en que prioriza la velocidad y la provisión automática, pero no ofrece un análisis profundo de las variables que originan los conflictos. En contraste, el modelo híbrido desarrollado en la empresa, si bien menos veloz en la ejecución, aporta un enfoque más específico y contextual: combina la capacidad técnica de la macro con la evaluación humana de especialistas, lo que permite comprender el trasfondo de los incidentes, proponer correcciones ajustadas a la realidad del negocio y garantizar un balance entre eficiencia, seguridad y alineación con los procesos organizacionales.

5.2. Conclusiones

- La investigación evidenció brechas en la gestión de accesos de la empresa, como acumulación de funciones, controles manuales ineficaces, baja madurez en roles y resistencia al cambio, lo que incrementaba los riesgos de seguridad.
- El modelo híbrido que integra RBAC, ABAC y Roles y Procesos demostró ser más efectivo que los enfoques individuales, al combinar simplicidad en la administración, granularidad contextual y alineación con los flujos críticos del negocio.
- La validación del sistema desarrollado mostró que la integración de controles automatizados y reglas dinámicas permite reducir riesgos, garantizar cumplimiento normativo (ISO/IEC 27001) y generar indicadores objetivos que fortalecen la trazabilidad y la auditoría.
- Como aporte práctico, la propuesta ofrece a la empresa una herramienta costo-efectiva y adaptable que mejora la segregación de funciones y protege la información crítica. En el plano académico, se constituye como un modelo replicable para organizaciones intermedias que buscan equilibrar eficiencia, seguridad y sostenibilidad en la gestión de accesos.

5.3. Recomendaciones

- Se recomienda que futuras investigaciones incluyan una validación cruzada con stakeholders como auditores externos y jefes de área. Esto permitirá contrastar la efectividad del modelo más allá del plano técnico, fortaleciendo su legitimidad y asegurando mayor alineación con las necesidades del negocio y las prácticas de control interno.
- Se sugiere implementar un plan de madurez en la gestión de accesos de la *Empresa*: en el corto plazo, consolidar la definición de roles y su integración con procesos críticos; en el mediano, ampliar con atributos dinámicos (ABAC) para mayor granularidad; y en el largo, evolucionar hacia modelos Zero Trust con integración a plataformas IAM corporativas.
- Se recomienda formalizar un proceso integral de gobernanza de accesos que incorpore auditoría continua, revisiones periódicas y métricas estratégicas de seguridad (p. ej., porcentaje de conflictos SoD corregidos, tiempo medio de

resolución y reducción de cuentas inactivas), fortaleciendo la trazabilidad y el cumplimiento con la ISO/IEC 27001.

- Se propone consolidar el uso del sistema desarrollado como alternativa costo-efectiva frente a SAP Access Control, documentando beneficios en términos de eficiencia y alineación normativa para reforzar su legitimidad como solución corporativa sostenible.
- Se sugiere implementar programas de capacitación y sensibilización dirigidos a usuarios clave y responsables de procesos, con el fin de reducir la resistencia al cambio y fortalecer la cultura de seguridad de la información y control interno.
- Se recomienda establecer un plan de evolución tecnológica que contemple la integración progresiva con sistemas de monitoreo más robustos (SIEM) y con plataformas de gestión de identidades (IAM), asegurando escalabilidad, resiliencia y preparación ante futuros requerimientos regulatorios y tecnológicos.

REFERENCIAS

Aftab, M. Hamza, A., Oluwasanmi, A., Xuyun, N., Sarfraz, M., Shehzad, D., Qin, Z., Rafiq, A. (2022). Traditional and Hybrid Access Control Models: A Detailed Survey, Security and Communication Networks, 12, 65671–65693. <https://doi.org/10.1155/2022/1560885>

Axiomatics (23 de julio, 2018). *Intro to Attribute Based Access Control (ABAC)*. Disponible en: <https://axiomatics.com/blog/intro-to-attribute-based-access-control-abac>

Bian, Aoao; Han, Dezhi; Cui, Mingming; Li, Dun Medical, Record Information Storage Scheme Based on Blockchain and Attribute Roles-Based Access Control, (2024), *Computer Science and Information Systems*, 21(3), pp. 807–830, <https://doi.org/10.2298/CSIS231002019B>

Bowman, K. (2025). SAP Acces Control: Key Capabilities and How to Use Them to Implement SoD, *Pathlock*, 25 de junio de 2025. Disponible en https://pathlock.com/learn/sap-access-key-capabilities-and-how-to-use-them-to-implement-sod/?utm_source=chatgpt.com

Cao, R., Research on RBAC Based Role Access Control in Financial MIS (2022), Proceedings - 6th International Conference on Wireless Communications and Applications, pp. 147–150. <https://doi.org/10.1109/ICWCAPP57292.2022.00043>

Congreso de la República del Perú (2011). *Ley N.º 29733 – Ley de Protección de Datos Personales*, Diario Oficial El Peruano. <https://cdn.www.gob.pe/uploads/document/file/272360/Ley%20N%C2%BA%2029733.pdf.pdf?v=1618338779>

e-Governance Academy, *National Cyber Security Index (NCSI) 2023 – Peru Profile*. (2023). Tallinn, Estonia: NCSI, 2023. Disponible en: <https://ncsi.ega.ee>

European Union Agency for Cybersecurity (ENISA). (2022). *Guidelines on Security Measures for Information Assets*. Recuperado de <https://www.enisa.europa.eu>

Fischer-Hellman, P. (2012). *Information flow based security control beyond RBAC: how to enable fine-grained security policy enforcement in business processes beyond limitations of role-based access control (RBAC)*. Springer Vieweg. <https://doi.org/10.1007/978-3-8348-2618-3>

Fong, P. (2011). Relationship-based access control: protection model and policy language. *Association for Computing Machinery*, pp. 191–202. <https://doi.org/10.1145/1943513.1943539>

Hathaliya J.J., Tanwar S., Role and attribute-based access control scheme for decentralized medicine supply chain, (2024), *Journal of Information Security and Applications*, p. 85. <https://doi.org/10.1016/j.jisa.2024.103851>

Hernández-Sampieri, R. y Mendoza, C. (2018). Metodología de la investigación. Las ruta cuantitativa, cualitativa y mixta. Mc Graw Hill Education.

Hu, V. C., Ferraiolo, D. F., Chandramouli, R., & Kuhn, D. R. (2020). *Guide to Attribute Based Access Control (ABAC) Definition and Considerations*. NIST Special Publication, pp. 800-162. <https://doi.org/10.6028/NIST.SP.800-162>

Huang, D., Dong, Q., & Zhu, Y. (2020). *Attribute-Based Encryption and Access Control*. Springer. <https://doi.org/10.1201/9781351210607>

IBM Security, *Cost of a Data Breach Report 2023*. IBM Corporation (2023). [En línea]. Disponible en: <https://www.ibm.com/reports/data-breach>

Indenhaus (31 de mayo, 2017). *How to Successfully Introduce Role Based Access Control into a Group Environment*. Disponible en: <https://idenhaus.com/how-integrate-role-based-access-control-group-environment/>

ISACA, *COBIT 2019 Framework: Governance and Management Objectives*, Rolling Meadows, IL: Information Systems Audit and Control Association, 2020.

ISACA. (2021). *Implementing a Risk-Based Approach to Data Protection: A Practical Guide*. Rolling Meadows, IL: Information Systems Audit and Control Association.

ISO/IEC. (2022). *ISO/IEC 27001:2022 – Information security, cybersecurity and privacy protection – Information security management systems – Requirements*. Geneva, Switzerland: International Organization for Standardization.

ISO/IEC. (2020). *ISO/IEC 27701:2020 – Security techniques – Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management*. Geneva, Switzerland: International Organization for Standardization.

Jyosthna P.M.; M.i, A. V.; Teja, M. S.; Ray, S. K.; Kumar, B.Y. S., Enhancing Security and Flexibility with Combined RBAC and ABAC Access Control Models (2024), Proceedings of the 2024 10th International Conference on Communication and Signal Processing, ICCSP 2024, pp. 576–581, DOI: 10.1109/ICCSP60870.2024.10543482

Kayes, A.S.M.; Rahayu, W.; Dillon, T.; Chang, E.; Han, J. (2019). Context-aware access control with imprecise context characterization for cloud-based data resources. *Future Gener. Comput. Syst.* Pp. 93, 237–255. <https://doi.org/10.1016/j.future.2018.10.036>

Kessem, L. (30 de julio, 2025). Cost of a Data Breach Report: Navigating the AI rush without sidelining security,” *IBM X-Force*. Disponible en: <https://www.ibm.com/think/x-force/2025-cost-of-a-data-breach-navigating-ai>

Konathala, K. (28 de mayo, 2024). Integrating SAP Access Control as part of your S/4HANA Public/Private Cloud and On-Premises Implementations, *Answerthink*. Disponible en: https://www.answerthink.com/2024/05/28/integrating-sap-access-control/?utm_source=chatgpt.com

Mohamed, A., Auer, D., Hofer, D. & Kueng, J. (2024). Comparison of Access Control Approaches for Graph-Structured Data. *Cryptography and Security*. <https://doi.org/10.48550/arXiv.2405.20762>

National Institute of Standards and Technology (NIST). (2010). *Guide to Protecting the Confidentiality of Personally Identifiable Information (PII)* (NIST Special Publication 800-122). Gaithersburg, MD: U.S. Department of Commerce. Disponible en: <https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-122.pdf>

National Institute of Standards and Technology (2020). *Security and Privacy Controls for Information Systems and Organizations*, NIST SP 800-53 Rev. 5, Gaithersburg, MD: U.S. Department of Commerce. <https://doi.org/10.6028/NIST.SP.800-53r5>

National Institute of Standards and Technology (2020). *Zero Trust Architecture* (Special Publication 800-207). Gaithersburg, MD: National Institute of Standards and Technology. <https://doi.org/10.6028/NIST.SP.800-207>

Organización de las Naciones Unidas. (2023). Informe de los Objetivos de Desarrollo Sostenible. Disponible en: https://unstats.un.org/sdgs/report/2023/The-Sustainable-Development-Goals-Report-2023_Spanish.pdf?_gl=1*1swr32b*_ga*NTcxNTkxNzIwLjE3NDUyODE0OTQ.*_ga_TK9BQL5X7Z*MTc0NTI4MTQ5NC4xLjEuMTc0NTI4MTY0NS4wLjAuMA

Pal, S., & Jadidi, Z. (2021). Protocol-Based and Hybrid Access Control for the IoT: Approaches and Research Opportunities. *Sensors*, 21(20), 6832. <https://doi.org/10.3390/s21206832>

Sánchez, D. (14 de noviembre, 2022) *Tipos de Control de Acceso Físico y sus Componentes*, *ITA Tech (blog)*. Disponible en: <https://ita.tech/tipos-de-control-de-acceso-fisico-y-componentes>

Santos-Olmo, A., Sánchez, L., Caballero, I., Camacho, S., & Fernández-Medina, E. (2016). La importancia de la cultura de la seguridad en las PYMES frente a la correcta gestión de la seguridad de sus activos. *Future Internet*, 8 (3), p. 30. <https://doi.org/10.3390/fi8030030>

Vogel, M., Implementing role-based access control - How we can do it better (2006). ISSE 2006 - Securing Electronic Business Processes: Highlights of the Information Security

Solutions Europe 2006 Conference, pp. 176–185. https://doi.org/10.1007/978-3-8348-9195-2_19

Vu, Thi-Huong-Giang.;Trinh, Tuan-Dat; Tran, Trung-Hieu, Authorization Model for Microservice-Based ERP Software, (2024), *Lecture Notes in Networks and Systems*, pp. 497–506. https://doi.org/10.1007/978-981-97-5504-2_59

Zapata, B., Fernández, J. & Toval, A. (2015). Seguridad en la computación en la nube: un estudio de mapeo. *Computer Science and Information Systems*, 12, pp. 161-184. <https://doi.org/10.2298/CSIS140205086C>

ANEXOS

Anexo A.

Análisis de conflictos de acceso por empresa y departamento

User	Blot	Nombr	Cargo	Departament	Holding	Conflicto Ejecución inicial (Alto)	Conflicto Ejecución inicial (Alto)	Conflicto Segunda ejecución (Alto)	Conflicto Segunda ejecución (Medio)	Conflicto Eliminados (Alto)	Conflicto Eliminados (Medio)	Conflicto Mantenidos (Alto)	Conflicto Mantenidos (Medio)	Conflicto Mantenidos (Medio)	Pendiente respuest
AABANTO	7	A.M.A.M	OFICINA	COMERCIAL	Azucareras	3	0	1	0	0	0	1	0	1	0
AAGURRE	23	A.A.A.A	CONTADOR	CONTABILIDAD	Perú	6	3	5	2	0	0	5	2	0	0
AALVAREZ	25	A.A.A.A	ANALISTA	GERENCIA DE PRESUPUESTOS	Perú	1	0	1	0	1	0	0	0	0	0
AAMESQUI	14	A.F.A.F	ASISTENTE DE TESORERÍA	CORPORATIVO - STAFF	Otros negocios	4	1	4	0	1	0	3	0	0	0
AAMPUDIA	7	A.A.A.A	JEFE DE DEPARTAMENT	PRODUCCION	Azucareras	1	0	1	0	0	0	1	0	1	0
DO	1A	A.E.A.E	GENERAL	GENERAL -	Cartones	7	8	0	0	0	0	0	0	0	0
AATICONA	5E	A.A.A.A	ASISTENTE ADMINISTRATIVO	CONTROL DE CALIDAD -	Cementerías	2	1	1	1	0	1	1	0	0	0
AAZUNIGA	5L	A.A.A.A	OPERADOR DE PRODUCCIÓN	LOGÍSTICA Y ENSACADO -	Cementerías	3	0	3	0	2	0	1	0	0	0
ABARANDI	8	A.C.A.C	SECRETARIA	GERENCIA DE VENTAS -	Alimentos - Perú	1	1	0	1	0	1	0	0	0	0
ABPACHEC	8	A.P.A.P	ADMINISTRADOR ZONAL	ADMIN. ZONAL ICA -	Alimentos - Perú	1	1	0	1	0	0	0	1	0	0

Nota. Por motivos de extensión, se muestra únicamente una sección del análisis de conflictos por empresa y departamento, extraída de la macro original que consolida la totalidad de datos evaluados.

Anexo B

Análisis de conflictos por holding según cada empresa

Holding	Conflictos Ejecución inicial (Alto)	Conflictos Ejecución inicial (Medio)	Conflictos Segunda ejecución (Alto)	Conflictos Segunda ejecución (Medio)	Conflictos Eliminados (Alto)	Conflictos Eliminados (Medio)	Conflictos Mantenidos (Alto)	Conflictos Mantenidos (Medio)	Conflictos por atender
Alimentos - Perú	262	146	242	129	78	27	164	102	25
Alimentos - Países	404	256	256	140	175	115	81	25	4
Azucareras	129	43	106	35	0	0	106	35	141
Azucareras	117	67	103	52	0	0	103	52	155
Cementeras	66	52	56	42	28	26	28	16	2
Alimentos - Perú	24	20	21	20	8	5	13	15	16
Azucareras	100	67	91	65	0	0	91	65	156
Cementeras	67	42	55	28	30	22	25	6	5
Alimentos - Países	85	55	84	56	14	21	70	35	15
Alimentos - Perú	658	367	516	313	232	151	284	162	175
Alimentos - Perú	13	5	9	4	3	2	6	2	0
Alimentos - Perú	38	23	35	22	17	10	18	12	19
Alimentos - Perú	18	7	14	6	6	1	8	5	0

Nota. Por motivos de extensión, se muestra únicamente una sección del análisis de conflictos por holding según cada empresa, extraída de la macro original que consolida la totalidad de datos evaluados.

Anexo C

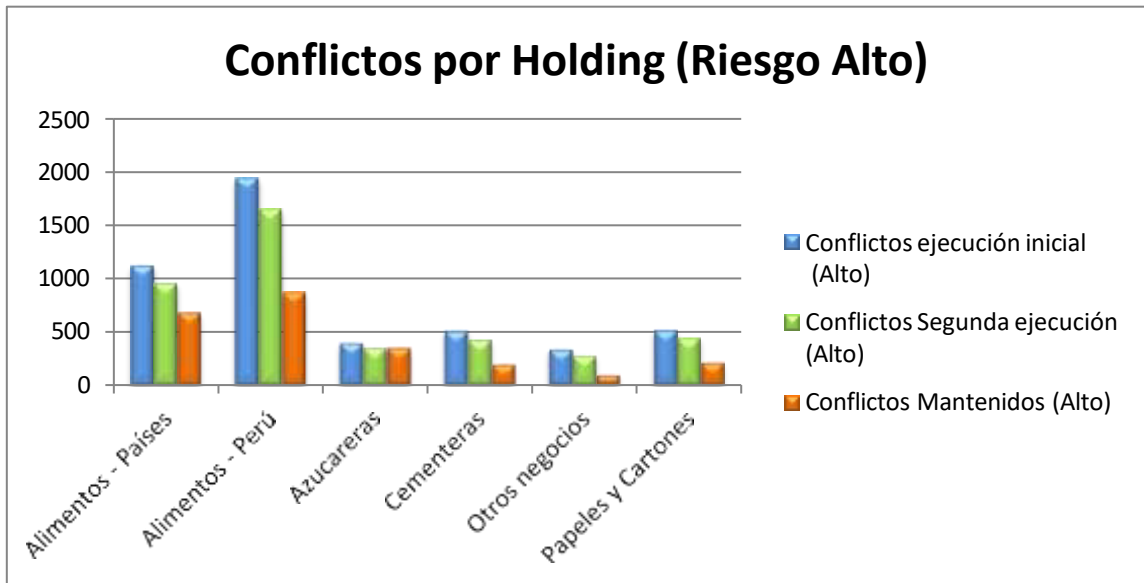
Análisis de conflictos por holding según los usuarios

Holding	Usuarios Ejecución inicial (Total)	Usuarios Ejecución inicial (Alto)	Usuarios Ejecución inicial (Medio)	Usuarios Segunda ejecución (Total)	Usuarios Segunda ejecución (Alto)	Usuarios Segunda ejecución (Medio)	Usuarios sin conflicto (Total)	Usuarios sin conflicto (Alto)	Usuarios sin conflicto (Medio)	Usuarios que mantienen conflictos(T otal)	Usuarios que mantienen conflictos (Alto)	Usuarios que mantienen conflictos (Medio)	Conflictos pendientes
Alimentos - Perú	34	31	29	39	37	27	21	21	18	37	35	24	18
Alimentos - Países	46	46	41	42	42	37	38	37	30	30	28	15	4
Azucareras	64	62	20	57	53	13	0	0	0	57	53	13	57
Azucareras	52	49	25	48	42	23	0	0	0	48	42	23	48
Cementeras	24	24	16	24	22	15	16	11	12	19	18	5	2
Alimentos - Perú	3	3	2	2	2	2	1	1	1	2	2	2	1
Azucareras	9	9	6	9	9	6	0	0	0	9	9	6	9
Cementeras	13	13	10	13	13	6	9	8	5	11	11	4	4
Alimentos - Países	11	11	8	13	13	10	6	5	5	13	13	9	3
Alimentos - Perú	136	136	112	140	99	110	65	60	45	127	77	89	51
Alimentos - Perú	3	3	3	3	1	3	1	1	1	3	1	2	0
Alimentos - Perú	7	7	7	7	6	6	5	4	3	5	5	5	4

Nota. Por motivos de extensión, se muestra únicamente una sección del análisis de conflictos por holding según los usuarios, extraída de la macro original que consolida la totalidad de datos evaluados.

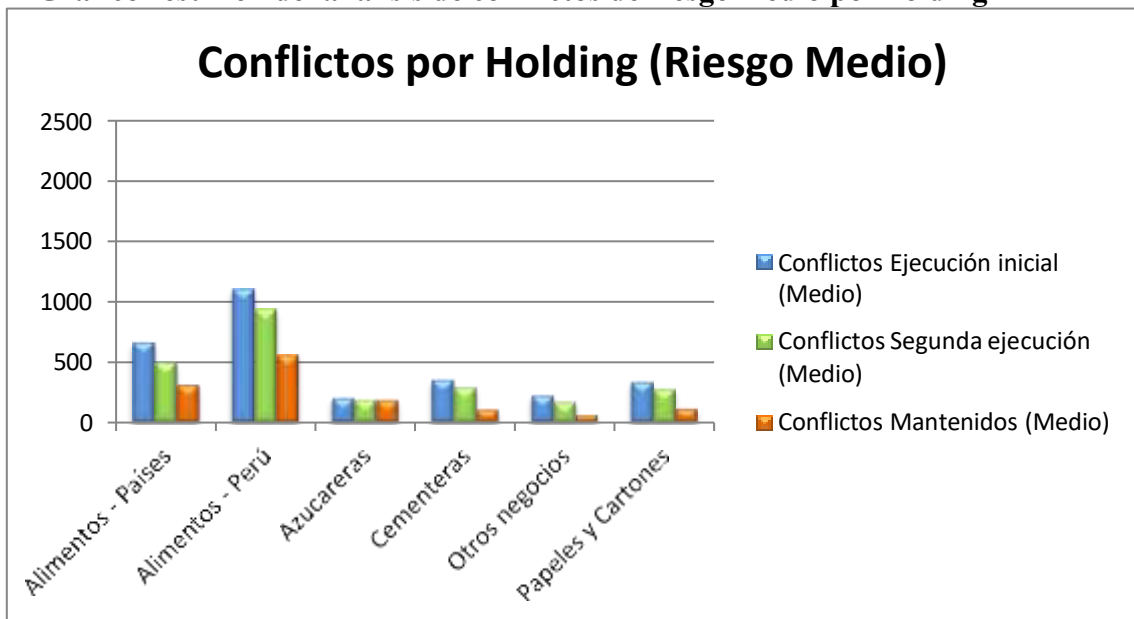
Anexo D.

Gráfico resumen del análisis de conflictos de riesgo alto por holding



Anexo E.

Gráfico resumen del análisis de conflictos de riesgo medio por holding



Anexo F.

Gráfico resumen del análisis de conflictos por holding

Usuarios con conflicto por Holding

