ANÁLISIS DE LOS RIESGOS EN LA IMPLEMENTACIÓN DE AUTOMATIZACIONES EN EL PROCESO DE DISPUTAS DE LA ORGANIZACIÓN AMRIZE

TRABAJO DE GRADO PARA OPTAR POR EL TÍTULO DE

Administradora de Empresas

Presentado por:

JULIANA ANDREA CASTILLO DIAZ

Asesor Temático:

MARTIN ALONSO MORA RENDÓN

Asesora Metodológico:

ISIS MIOSOTIS ALVAREZ FLOREZ

UNIVERSIDAD AUTÓNOMA LATINOAMERICANA

FACULTAD DE ADMINISTRACIÓN DE EMPRESAS

MEDELLIN

2025

Resumen

El proceso de *Disputes* de AMRIZE, organización pública resultado de la escisión de Holcim en Estados Unidos y Canadá, ha incorporado diversas automatizaciones orientadas a mejorar la eficiencia operativa, reducir errores manuales y tiempos de procesamiento. Sin embargo, la implementación de estas herramientas ha generado riesgos operativos, tecnológicos, normativos y organizacionales que pueden afectar la continuidad del proceso, la integridad de la información y el cumplimiento regulatorio. Este trabajo analiza los riesgos inherentes a tales automatizaciones mediante un enfoque mixto que combina valoración cualitativa y cuantitativa, integrando criterios del marco COSO ERM y la ISO 31000. A partir del diagnóstico, se evalúan quince riesgos priorizados según probabilidad e impacto, y se diseñan controles y respuestas estratégicas orientadas a su mitigación, aceptación, transferencia o eliminación. Finalmente, se propone un plan de mejora estructurado bajo la metodología PHVA, el cual define actividades, responsables, tiempos y mecanismos de seguimiento para fortalecer la estabilidad técnica, el cumplimiento normativo y la sostenibilidad operativa del proceso en AMRIZE.

Palabras clave: Automatización, Proceso, Riesgo, Disputas, Errores, Organización Pública.

Abstract

The Disputes process at AMRIZE, a public organization resulting from the spin-off of Holcim in the United States and Canada, has incorporated several automation tools aimed at improving operational efficiency, reducing manual errors, and shortening processing times. However, the implementation of these technologies has introduced operational, technological, regulatory, and organizational risks that may affect process continuity, data integrity, and regulatory compliance. This study analyzes the risks inherent to these automations through a mixed methodological approach that combines qualitative and quantitative assessments, integrating the principles of the COSO ERM framework and ISO 31000. Based on this diagnostic, fifteen risks are evaluated and prioritized according to their probability and impact, and strategic controls and response actions are designed to mitigate, accept, transfer, or eliminate

them. Finally, an improvement plan is proposed under the PDCA methodology, defining activities, responsibilities, timelines, and monitoring mechanisms to strengthen technical stability, regulatory compliance, and operational sustainability within AMRIZE's automated Disputes process.

Keywords: Automation, Process, Risk, Disputes, Errors, Public Organization.

Agradecimientos

A Dios, por la fortaleza y la claridad otorgadas durante este proceso académico y personal.

A mi familia y pareja, por su apoyo incondicional, por acompañar cada meta y por ser el motor que impulsa mi crecimiento profesional, por su ejemplo de disciplina y dedicación, y quienes con su cariño y motivación han hecho posible este logro.

A Valentina Mesa, por su apoyo incondicional y su capacidad de escuchar con paciencia en los momentos de mayor crisis e incertidumbre.

A mis asesores, Martín Alonso Mora Rendón e Isis Miosotis Álvarez Flórez, por su guía, orientación, retroalimentación y compromiso en la construcción metodológica y técnica de este trabajo.

A la empresa AMRIZE, especialmente al equipo de *Disputes*, por facilitar el acceso a la información, por la disposición para participar en entrevistas y discusiones, y por permitir que este análisis aporte a la consolidación de un modelo de gestión de riesgos robusto y aplicable a los procesos automatizados.

Finalmente, agradezco a todos quienes, de manera indirecta, contribuyeron con su apoyo, conocimientos o palabras de aliento para la culminación de este trabajo de grado.

Tabla de Contenido

Índice de Tablas

Índice de Figuras

Glosario

1. ***Accountability* (Responsabilidad demostrada)**: Deber de evidenciar cumplimiento en protección de datos con políticas, controles, DPIA, auditorías y registros. (SIC, ISO 31000).
2. ***Algorithmic bias* (Sesgo algorítmico)**: Resultado discriminatorio por diseño/datos de un algoritmo.
3. ***BCP/Business Continuity* (Continuidad del negocio)**: Capacidad de operar procesos críticos ante interrupciones.
4. ***Breach notification* (Notificación de brechas)**: Deber de avisar incidentes de seguridad a autoridades/titulares.
5. **CI/CD (Continuous Integration/Delivery)**: Prácticas de ingeniería para liberación continua con control.
6. **Cifrado en tránsito/en reposo**: Protección criptográfica de datos en movimiento / almacenados.
7. **CPGs (CISA Cybersecurity Performance Goals)**: Metas mínimas transversales de ciberseguridad.
8. ***Failover:*** Modo de respaldo cuando el componente principal falla.
9. ***Firewall:*** Control de tráfico de red según políticas de seguridad.
10. **IIoT (Industrial IoT)**: Conectividad de sensores/actuadores en industria.
11. ***Logs inmutables:*** Registros inviolables de actividades de bots/usuarios.
12. **Notificación a RNBD**: Reporte de incidentes en 15 días hábiles.
13. ***Ransomware:*** Programa maligno que cifra activos y exige pago.
14. **SAP-RPA (Integración)**: Flujos automatizados que interactúan con SAP (logs, SoD, cifrado).
15. ***Segregation of Duties (SoD):*** Separación de funciones para evitar fraude/error (SIC/NIST; mención en SAP/RPA).
16. **Servicios IaaS/PaaS/SaaS**: Modelos de nube.

Introducción

La transformación digital ha impulsado a las organizaciones a incorporar tecnologías de automatización como herramientas clave para optimizar sus operaciones, mejorar la eficiencia y fortalecer la trazabilidad de la información. En este contexto, AMRIZE, empresa pública estadounidense surgida tras la escisión del negocio norteamericano de Holcim, ha integrado diversas automatizaciones dentro del proceso de *Disputes* del ciclo *Order to Cash* (O2C). Dichas automatizaciones han permitido agilizar tareas operativas, reducir errores manuales y aumentar la consistencia de los datos procesados; no obstante, también han introducido riesgos técnicos, operativos, legales y organizacionales que requieren ser gestionados de manera sistemática.

Considerando la criticidad del proceso de *Disputes* en la conciliación de cuentas, la validación de información tributaria y la resolución de discrepancias que afectan directamente el flujo de caja de la organización, se vuelve indispensable analizar los riesgos inherentes a las automatizaciones implementadas. En línea con los principios de la gestión moderna del riesgo, este trabajo identifica, evalúa y prioriza los eventos que pueden afectar la continuidad, confiabilidad y cumplimiento normativo del proceso, integrando tanto marcos teóricos como referentes legales aplicables al entorno corporativo de AMRIZE.

La investigación se desarrolla bajo un enfoque mixto y se fundamenta en herramientas metodológicas como el análisis cualitativo y cuantitativo del riesgo, la simulación mediante el método de Monte Carlo, el marco COSO ERM y la ISO 31000. Inicialmente, se caracteriza el proceso de *Disputes* y se describen las automatizaciones implementadas, identificando sus puntos críticos. Posteriormente, se evalúan quince riesgos mediante matrices de probabilidad e impacto, y se define para cada uno una estrategia de tratamiento basada en criterios de mitigación, aceptación, transferencia o evitación. Finalmente, se diseña un plan de acción estructurado bajo el ciclo PHVA, el cual integra actividades, tiempos, responsables y mecanismos de monitoreo que permiten fortalecer la gobernanza tecnológica, la seguridad operativa y la sostenibilidad del proceso automatizado.

De esta manera, el trabajo aporta un modelo integral de gestión del riesgo aplicable a las automatizaciones del proceso de *Disputes* y contribuye a que estas no solo generen eficiencia, sino también confianza, cumplimiento y continuidad operativa en un entorno sujeto a exigencias regulatorias y auditorías permanentes.

1. Formulación

La etapa de formulación constituye la primera fase en el desarrollo del plan de mejoramiento, y se lleva a cabo mediante una descripción del contexto organizacional de AMRIZE, así como de la caracterización del proceso de *Disputes* y de los desafíos generales asociados a la implementación de automatizaciones. Con base a esto, se construye el planteamiento del problema y su respectiva justificación, articulado con los objetivos tanto general como específicos y la base metodológica del estudio. De manera complementaria, el marco referencial y el marco legal consolidan los fundamentos conceptuales y normativos que sustentan el trabajo, permitiendo en conjunto una explicación y estructuración del proceso de formulación.

1.2. Planteamiento del Problema

North America Shared Services en adelante AMRIZE, es una empresa de los Estados Unidos que surge en junio 2025 tras el resultado de la escisión de Holcim, e iniciando su cotización en la Bolsa de Nueva York. Con más de 19.000 empleados, 1.000 plantas en EE. UU y Canadá, es hoy el principal productor de cemento en Norteamérica y uno de los líderes en soluciones de construcción en líneas de infraestructura, comercial, residencial, entre otros.

El nombre AMRIZE, resulta de la combinación de dos conceptos: "ambición" y "ascenso" (*rising* en inglés). "*Am*" representa el compromiso de la futura empresa con el alto rendimiento y la innovación para responder a las mayores ambiciones de sus clientes. "*Rize*" simboliza el impulso de la compañía por liderar el avance de la construcción en Norteamérica, dando forma a edificios e infraestructuras esenciales que mejoran la calidad de vida (Holcim, 2025).

La estructura funcional de AMRIZE está conformada por un modelo de seis torres con funciones propias de cada una. La torre de *Order to Cash* (O2C), gestiona el ciclo completo del ingreso de cara al cliente: desde la facturación del producto vendido en planta hasta la cobranza y el servicio al cliente. Dentro de ésta, el proceso de *Disputes* se encarga de investigar las

discrepancias de los pagos y reclamos que requieran validación de datos, revisión documental en SAP como soportes de pago, facturas, entre otros con el único objetivo de conciliar las cuentas de los clientes en las diferentes regiones de EE. UU. con el fin de mantener las cuentas limpias.

En el siglo XXI, la transformación digital ha impulsado a las organizaciones, tanto privadas como públicas, a incorporar herramientas de automatización con el fin de optimizar sus procesos, reducir costos operativos y mejorar la eficiencia operacional. En ese sentido, la automatización de procesos (*RPA*) y otras tecnologías emergentes se han convertido en aliados clave para el procesamiento de tareas repetitivas y de alto volumen en diferentes áreas organizacionales.

El auge de la integración de tecnologías de automatización de procesos mediante *robots* de *software* (*Robotic Process Automation* - *RPA*-), han venido en crecimiento en los últimos años, siendo fundamental en empresas que demandan procesamiento de alto volumen de tareas operativas y bajo margen de error. La *RPA* tiene la capacidad de automatizar operaciones dentro de las organizaciones de manera eficiente no sólo en tiempo, sino también reduciendo errores manuales y liberando el personal para tareas analíticas (*Hall*, 2024). No obstante, también se advierte que entre el 30% y el 50% de la implementación de las mismas fallas por falta de una planificación estratégica, resistencia al cambio, problemas de alineación entre áreas, así como también falta de seguimientos y de controles internos (*Reuters*, 2025).

Consciente de la importancia de la innovación, *AMRIZE* promueve la automatización de múltiples procesos, integrando tecnología en su operación para responder a las exigencias del mercado y a los avances en inteligencia artificial y nuevas tecnologías. Desde el proceso de *Disputes*, se ha iniciado la integración de la *RPA*, con el propósito de automatizar tareas repetitivas como creación de créditos para impuestos, por ajustes de precios en materiales, créditos para refacturación, generación de información desde transacciones de SAP, generación de respuestas estandarizadas, automatización de informes actualizados en tiempo real, entre otros. Sin embargo, la implementación de sistemas de *RPA* a la integración de la cotidianidad de tareas, conlleva múltiples riesgos clasificados como operacionales, tecnológicos, legales o riesgos reputacionales y que pueden conducir a pérdidas económicas.

En ese sentido, según Arnanz (2021), los sistemas automatizados pueden introducir sesgos, discriminaciones involuntarias o falta de transparencia si no se implementan protocolos robustos de auditoría, supervisión y control humano y algorítmico. Además, Barrio y Silóniz (2024) destacan los retos al auditar sistemas *RPA* en el sector público, entre ellos el acceso seguro a datos, la integridad y el seguimiento de incidentes.

Dado el manejo de datos sensibles en múltiples canales de interacción desde el proceso de *Disputes,* se hace necesaria la realización de auditorías en tiempo real y la necesidad de trazabilidad jurídica para prevenir sesgos operativos y garantizar el cumplimiento de normativas frente a las automatizaciones que se han implementado.

Es importante identificar, caracterizar, categorizar, gestionar y evaluar los riesgos asociados, que permitan tener un plan de manejo o protocolo de *failover,* definido como un "modo de funcionamiento de respaldo en el que las funciones de un componente de sistema son asumidas por componentes del sistema secundario cuando el componente principal no está disponible" (Instituto Nacional Electoral, 2020), de manera estructurada.

Por lo tanto, este trabajo de grado se propone responder a la pregunta: ¿cómo diseñar e implementar un marco de gestión integral de los riesgos identificados con las automatizaciones mediante *RPA* en el proceso de Disputas de *AMRIZE*, garantizando tanto la eficiencia operativa como el cumplimiento normativo y la preservación de la confianza interna y externa?

1.2. Justificación

La gestión efectiva de los diferentes riesgos identificados en la implementación de automatizaciones es importante para garantizar el cumplimiento de los objetivos organizacionales, más aún desde la mirada pública. Su relevancia se fundamenta tanto en el entorno interno como en el contexto global. Para *AMRIZE*, líder en el sector de materiales de construcción en Norteamérica, la incorporación de *RPA* en el proceso de *Disputes*, no sólo representa un avance en la integración con sistemas tecnológicos que buscan la eficiencia en todos los procesos y que se alinean con los objetivos estratégicos como organización, sino que

también representa una transformación que impacta directamente a la continuidad operativa, protegiendo la confianza de sus grupos de interés (*skateholders*), pero también su reputación como empresa pública que debe cumplir con la normatividad exigida en los Estados Unidos y la acción en todas sus mejoras internas no sólo implementando sistemas de mejora operacional sino teniendo un plan de acción frente a los riesgos que pueda representar, es decir, anticipando los escenarios posibles con planes de respuesta.

La implementación de automatización en el proceso de *Disputes* de *North America Shared Services* - AMRIZE representa una oportunidad significativa para aumentar la eficiencia y reducir tiempos de resolución. Sin embargo, esta transformación también conlleva riesgos que pueden afectar directamente la continuidad, calidad y seguridad de los procesos. Las operaciones en AMRIZE deben estar regidas por altos estándares de transparencia, fiabilidad y cumplimiento normativo. Por ello, es imprescindible analizar de forma anticipada y sistemática los riesgos asociados a la automatización en este proceso.

Se evidencia que la automatización de procesos puede optimizar recursos, reducir errores y acelerar los tiempos de respuesta, mejorando indicadores de áreas (Rojas, 2023), sin embargo, también expone a riesgos si no se acompaña de un marco robusto de gestión y control, como la pérdida de continuidad de procesos clave en el área, la exposición a sanciones regulatorias y el deterioro de la reputación corporativa (ASF, 2014).

En ese sentido, el análisis de los diferentes riesgos de las automatizaciones en el proceso de *Disputes* y su correcto plan de gestión, puede convertir los desafíos actuales en oportunidades de optimización organizacional. Tal como lo menciona la Guía de Autoevaluación de Riesgos (ASF, 2014), la identificación temprana de amenazas, junto con la definición de niveles de tolerancia y planes de continuidad, fortalece la capacidad de respuesta de las organizaciones ante eventos o escenarios inesperados. Este principio es clave en la empresa AMRIZE, donde el volumen de transacciones diarias, la criticidad de la información y el impacto directo de cada proceso en otras áreas y como tal en el flujo de caja, requieren de una operación ininterrumpida y confiables para los grupos de interés.

Adicionalmente, implementar un marco de gestión y evaluación de riesgos desde el ámbito operativo, tecnológico, legal y reputacional, ofrece una ventaja competitiva frente a otras empresas del mismo sector, que se traduce a mayor capacidad para garantizar el cumplimiento normativo como organización pública de los Estados Unidos, reducir vulnerabilidades tecnológicas, prevenir sesgos en procesos automatizados y mantener la confianza de clientes e inversionistas. Como señala Blahusiakova (2023), las empresas que han adoptado la automatización con estrategias de gestión de riesgos bien estructuradas no sólo optimizan procesos, sino que también elevan su competitividad y capacidad de adaptación en entornos de cambio acelerado influidos por la tecnología.

En consecuencia, este estudio es crucial para el proceso de *Disputes* de la empresa AMRIZE, ya que permite establecer un marco metodológico la gestión de los riesgos asociados a las automatizaciones, sino que también asegure que la inversión en *RPA* se traduzca en beneficios sostenibles y medibles para la organización.

1.3. Objetivos

1.3.1. General

Analizar los riesgos inherentes en la implementación de procesos de automatización en el proceso de Disputas y su incidencia en la empresa AMRIZE como organización pública de los Estados Unidos de Norte América.

1.3.2. Específicos

- Evaluar los riesgos en los procesos automatizados dentro del proceso de Disputas de la empresa AMRIZE mediante una metodología de análisis de riesgos.
- Definir los controles sobre el impacto o la probabilidad de los riesgos identificados en los procesos automatizados dentro del proceso de Disputas de la empresa AMRIZE.

- Diseñar el plan de acción para el seguimiento y control de los riesgos en los procesos automatizados dentro del proceso de Disputas de la empresa AMRIZE.

1.4. Alcance

El presente trabajo de grado comprende el proceso de valoración de los riesgos identificados en la organización, incluyendo la recopilación y análisis de la información, la estimación cualitativa y/o cuantitativa de la probabilidad de ocurrencia y el impacto potencial de cada riesgo, considerando factores internos y externos que puedan incidir en su materialización.

Asimismo, se elaborará la matriz de riesgos, como instrumento que permita clasificar y jerarquizar los riesgos en función de su nivel de criticidad, facilitando su trazabilidad y control. Además, se diseñará el mapa de calor como representación gráfica que muestre de manera visual la distribución de los riesgos en relación con su probabilidad e impacto, y que sirva como herramienta estratégica para la priorización de acciones y la asignación eficiente de recursos en pro de su control.

En tal sentido, el alcance de este trabajo incluye la sistematización de la información de riesgos hasta la entrega de los productos finales: matriz de riesgos y mapa de calor, alineados con los objetivos del sistema de gestión de la organización, la metodología de riesgos y los marcos normativos y estándares internacionales aplicables a la organización AMRIZE.

1.5. Marco de Referencia

El presente marco de referencia se estructura en dos ejes fundamentales. En primer lugar, se aborda el referente teórico donde se exponen los conceptos, modelos y enfoques más relevantes en torno a la automatización de procesos, la gestión del riesgo y su evolución conceptual, con el fin de comprender las bases conceptuales y técnicas que sustentan la

investigación. En segundo lugar, se desarrolla el referente legal, que examina el marco normativo nacional e internacional aplicable a los procesos de automatización y gestión de riesgos.

1.5.1. Referente teórico

El referente teórico se orienta a exponer los fundamentos de la automatización de procesos y su impacto en la gestión empresarial, transformando las operaciones y la toma de decisiones. Asimismo, aborda la evolución del concepto de riesgo y su papel en la estrategia organizacional, desde las dimensiones tecnológicas, operativas, legales y reputacionales. Integra, además, marcos y herramientas como la Simulación Monte Carlo, los indicadores claves de riesgo y el modelo COSO ERM, que ofrecen una base conceptual y metodológica para comprender los desafíos y oportunidades que la gestión de riesgos plantea en los actuales entornos corporativos.

La automatización de procesos se entiende como la aplicación de tecnologías digitales que permiten ejecutar tareas rutinarias de manera eficiente y con menor margen de error, liberando tiempo para labores de mayor valor estratégico (Aguirre & Rodríguez, 2017). En este contexto, la Automatización Robótica de Procesos (*RPA*) se ha consolidado como una herramienta clave, al utilizar robots de software que replican acciones humanas sobre sistemas informáticos, agilizando la gestión operativa y aumentando la trazabilidad de los procesos (Van der Aalst et al., 2018).

De forma complementaria, surge la Automatización de Procesos Humanos (RHA), orientada a integrar tecnologías inteligentes – como inteligencia artificial y aprendizaje automático – que no sólo reemplazan tareas repetitivas, sino que ayudan a los equipos en actividades que requieren análisis. Este enfoque, conocido como automatización cognitiva, implica rediseños organizacionales y nuevos retos en materia de gestión de riesgos y gobernanza digital (Willcocks et al., 2017).

En este contexto, la automatización se entiende como el proceso mediante el cual las actividades humanas son asistidas o sustituidas por sistemas tecnológicos capaces de operar con mínima intervención manual. Su propósito no se limita a aumentar la eficiencia operativa, sino

que también busca reducir errores, optimizar recursos y fortalecer la capacidad de respuesta ante entornos cambiantes. Así, la automatización se convierte en un elemento clave para la gestión moderna del riesgo, al permitir una mayor anticipación y control sobre los procesos, integrando herramientas que transforman la manera en que las organizaciones perciben, analizan y enfrentan las amenazas o contingencias.

El riesgo ha estado presente en la humanidad desde los primeros intercambios con el entorno, vinculado inicialmente a amenazas físicas y visibles. Según Mejía (2011), la raíz etimológica del término en varios idiomas alude a un obstáculo o amenaza concreta cuya superación dependía de la anticipación y la preparación (p.25). Con el tiempo, este significado se amplió para abarcar cualquier evento o condición que pudiera afectar de manera positiva o negativa, el logro de los objetivos individuales, sociales o empresariales.

La teoría económica moderna introduce una distinción fundamental entre el riesgo y la incertidumbre. Para Knight (1921), citado por Mejía (2011), el riesgo hace referencia a aquellas situaciones en las que los resultados futuros son inciertos, pero las probabilidades de ocurrencia pueden estimarse o medirse, lo que permite la aplicación de modelos estadísticos o probabilísticos. En contraste, la incertidumbre implica una falta total o parcial de información, donde las probabilidades no pueden conocerse ni cuantificarse de manera objetiva (p. 27). Esta diferencia entre ambos conceptos es clave para la gestión organizacional: cuando se trata de riesgos medibles, es posible aplicar modelos probabilísticos y herramientas cuantitativas; en cambio, frente a la incertidumbre, se requieren aproximaciones como el análisis de escenarios o la prospectiva estratégica. Stulz (2006), advierte que confundir ambas categorías puede conducir a fallos críticos en la gestión.

En la concepción contemporánea, el riesgo no se limita a una connotación negativa. Lam (2014), plantea que “el riesgo es el equilibrio entre arte y ciencia, y su gestión adecuada puede transformarlo en una oportunidad para crear valor” (p. 14). Esta perspectiva implica que la gestión de riesgos empresariales o en inglés *Enterprise Risk Management (ERM)* no sólo busca mitigar pérdidas potenciales, sino también potenciar la capacidad de una organización para identificar y aprovechar oportunidades estratégicas. Hopkin (2018) lo define como “el efecto de

la incertidumbre sobre los objetivos" (p.75), destacando que dicho efecto puede ser tanto positivo como negativo.

La gestión de riesgos, por tanto, requiere un enfoque integral que considere varias dimensiones que pueden estar interrelacionadas entre sí. En el plano tecnológico, los riesgos se definen como la probabilidad de que la digitalización, la inteligencia artificial o el *big data* generen vulnerabilidades en los sistemas, fallos en la gestión de datos o exposición a ciberataques. Según Naim (2022), si bien la inteligencia artificial potencia el análisis de costos, la evaluación de riesgos y la toma de decisiones estratégicas, su aplicación sin una gobernanza de datos adecuada introduce amenazas como sesgos algorítmicos y brechas de seguridad (p.56).

En la dimensión operativa, los riesgos operativos corresponden a la posibilidad de disrupciones en la continuidad de los procesos, alteraciones en la calidad de los productos y servicios o fragilidades en la resiliencia de las cadenas de suministro. La incorporación de tecnologías como la automatización de procesos empresariales (BPA) y la automatización robótica de procesos (RBA), al reducir la intervención humana, expone a las organizaciones a riesgos de carácter sistémico, vulnerabilidades tecnológicas y amenazas cibernéticas que comprometen la estabilidad operativa y la seguridad de los datos (Robinson, 2022).

Desde el plano legal y regulatorio, los riesgos se entienden como la posibilidad de incumplir los marcos normativos nacionales e internacionales, lo que expone a las organizaciones a sanciones, restricciones y afectaciones reputacionales. Lam (2014), enfatiza que "el cumplimiento normativo es parte esencial de la gestión de riesgos y debe integrarse en la estrategia" (p.149), pues no se trata de un requisito aislado, sino de un elemento que afecta la sostenibilidad de la organización.

Por último, en la dimensión organizacional, los riesgos se definen como aquellos vinculados con la capacidad de la empresa para establecer un apetito de riesgo, definido por Hopkin (2018) como "la cantidad y tipo de riesgo que una organización está dispuesta a asumir para alcanzar sus objetivos" (p.150), concepto que debe traducirse en políticas y prácticas definidas y claras en todos los niveles jerárquicos. En ese sentido, Mejía et al. (2024) afirman que, una cultura de gestión de riesgos sólida conlleva a la promoción de la transparencia, el

reporte a tiempo de incidentes y la participación desde todos los niveles de la organización (p.133). En contraste, las culturas organizacionales reactivas tienden a ocultar los problemas, agravando sus consecuencias.

Es por esto que, al hablar de las etapas de la gestión del riesgo, la identificación de los riesgos constituye la primera etapa, pues de su exhaustividad depende la efectividad de las fases posteriores. Mejía et al. (2024) señalan que la identificación debe ser "sistemática, documentada y con participación de todos los niveles de la organización" (p.110), para ello, entre las herramientas usadas se destacan la lluvia de ideas o *brainstorming*, que fomenta la generación de posibles riesgos; el análisis causa-efecto, que permite identificar raíces de problemas mediante el diagrama de *Ishikawa*; las entrevistas y encuestas a expertos internos y externos y las inspecciones físicas para detectar riesgos *in situ* (p.p. 111-119).

Stulz (2006), enfatiza que "los mayores fracasos en la gestión de riesgos provienen de no identificar o no reconocer la verdadera naturaleza de los riesgos asumidos" (p-8). La identificación de los riesgos no es un ejercicio único, sino un proceso continuo, ya que el entorno interno y externo cambia constantemente, generando nuevas amenazas y oportunidades.

Tras la identificación, la evaluación de riesgos busca determinar su importancia y priorizar su tratamiento. Existen dos enfoques principales: la valoración cualitativa, que utiliza escalas subjetivas de probabilidad e impacto, escalas que pueden ser definidas como bajo, medio o alto, y la cuantitativa, que se respalda en datos y modelos estadísticos. Para Hopkin (2018), aunque la valoración cualitativa es más rápida y económica, esta puede carecer de precisión si no usa criterios claros y consensuados como base (p.143). Por su parte, la valoración cuantitativa, aunque más demandante en términos de datos y recursos, permite estimaciones más exactas y útiles en riesgos financieros y de mercado.

Para la modelación de riesgos, la simulación Monte Carlo permite simular la variabilidad de múltiples factores de manera simultánea, generando una distribución probabilística de resultados (Anderson, 2024, p. 213). Esta técnica, además, permite realizar análisis de sensibilidad para identificar las variables con mayor impacto, facilitando la priorización de medidas de mitigación. Adicionalmente, herramientas como *Oracle Crystal Ball* integran estas

capacidades en entornos accesibles como hojas de cálculo, ampliando su aplicación a contextos corporativos diversos, puesto que permite modelar miles de posibles escenarios y su impacto en flujos de caja de proyectos o áreas específicas de las empresas.

En la misma línea, el marco COSO ERM (*Committee of Sponsoring Organizations of the Treadway Commission*, 2017) es un enfoque integral de gestión de riesgos que involucra no sólo a la junta directiva de una organización, sino también a la alta gerencia y todo el personal de diferentes áreas, promoviendo una participación activa en la identificación, evaluación y respuesta ante riesgos, facilitando la alineación del riesgo con la estrategia empresarial, la integración entre crecimiento y rendimiento, la mejora en la toma de decisiones, el uso eficiente de recursos, etc.

De acuerdo con su marco metodológico, el COSO ERM (Sánchez, 2015, p. 45) amplía la perspectiva al situar la gestión de riesgos como parte de la gobernanza y la estrategia, articulando ocho componentes interrelacionados, los cuales son el entorno interno (que define la cultura y estructura de la organización), el establecimiento de objetivos (que permite anticipar eventos que afecten su cumplimiento), la identificación de eventos (que distingue entre oportunidades y amenazas), la evaluación de riesgos (que analiza probabilidad e impacto desde la perspectiva inherente y residual), la respuesta a riesgos (que define acciones para evitarlos, aceptarlos, mitigarlos o transferirlos), las actividades de control (que aseguran la ejecución de respuestas), la información y comunicación (que garantiza el flujo oportuno y efectivo de datos), y la supervisión y control (que evalúa y ajusta el proceso de manera continua). Lam (2014) subraya que "COSO ERM ayuda a alinear el apetito de riesgo con la estrategia y a mejorar la toma de decisiones" (p. 67), algo fundamental y relevante en entornos de alta volatilidad; además, clasifica los objetivos organizacionales en cuatro categorías: estratégicos, operativos, financieros y de cumplimiento normativo, para garantizar de esta manera, que la gestión de los riesgos abarque de manera integral todas las áreas críticas de la empresa (Leeland, 2024).

Paralelamente, al hablar de la gestión de riesgos, es importante incorporar indicadores clave de riesgo (*Key Risk Indicators*) que permitan monitorear variables críticas para la organización. Estos indicadores, integrados en paneles de control o *dashboards* y vinculados a

sistemas de alerta temprana, facilitan la detección de desviaciones antes de que se materialicen en pérdidas significativas.

En definitiva, el riesgo es una condición inherente a cualquier actividad humana y organizacional. Su gestión entendida como un proceso sistemático, estructurado y adaptado al contexto, permite no sólo prevenir pérdidas, sino también identificar y aprovechar oportunidades estratégicas.

La evolución conceptual desde una visión estrictamente defensiva hacia un enfoque integral y orientado a la creación de valor refleja el cambio en la naturaleza de los entornos económicos, tecnológicos y sociales. Es en estos entornos caracterizados por la interdependencia global y la velocidad de cambio donde la gestión de riesgos deja de ser una función aislada para convertirse en un componente esencial de la estrategia corporativa.

1.5.2. Referente legal

El tránsito de AMRIZE hacia operaciones inteligentes mediante la implementación de automatizaciones, robótica, *IIoT*, control avanzado de procesos y analítica de datos, está enmarcado en un contexto normativo sólido que garantice la seguridad, transparencia y cumplimiento en cada etapa. Este marco está orientado por el gobierno corporativo, la ciberseguridad, la seguridad industrial, la protección de datos y la normativa nacional e internacional que regula tanto el funcionamiento interno de la organización como su interacción con el mercado global.

En este contexto, la condición de AMRIZE como emisor en la Bolsa de Nueva York, impone exigencias adicionales en materia de controles internos, divulgación de la información y gestión de riesgos, mientras que a su vez la operación en Colombia incorpora la obligación de cumplir con normas locales en protección de datos, gestión documental y delitos informáticos. Así, se genera un entramado normativo entre el nivel federal, estatal, internacional y nacional, que constituye la base sobre la cual se deben desarrollas las automatizaciones y procesos digitales de la organización.

Tabla 1. Principal normatividad aplicable a procesos de automatización en AMRIZE.

Ley / Norma / Regulación	Objeto	Relación
Sarbanes–Oxley Act (SOX) (EE. UU.)	Establece reglas de control interno sobre la información financiera y certificación de procesos.	Obliga a diseñar, probar y certificar controles, también en procesos automatizados de Amrize.
SEC Rules (10-K y 8-K) (EE. UU.)	Exige divulgar la gestión de riesgos cibernéticos y reportar incidentes de ciberseguridad de forma inmediata.	Vincula la automatización con el deber de transparencia y revelación oportuna al mercado.
NYSE Timely Disclosure Policy (EE. UU.)	Garantiza la publicación simultánea de información material.	Requiere coordinar divulgaciones para evitar asimetrías en entornos con procesos automatizados.
NIST Cybersecurity Framework 2.0 y NIST SP 800-82 (EE. UU.)	Proveen lineamientos para ciberseguridad y sistemas de control industrial (OT).	Sirven de guía técnica para proteger procesos de automatización en entornos críticos (PLCs, SCADA, IIoT).
FTC Act / Políticas de IA y Consumo (EE. UU.)	Prohíbe prácticas engañosas relacionadas con el uso de IA.	Exige transparencia en automatizaciones cognitivas y algoritmos de Amrize.
CFAA – Computer Fraud and Abuse Act (EE. UU.)	Sanciona el acceso y uso indebido de sistemas informáticos.	Aplica a Amrize en automatizaciones y bots que operen con datos o sistemas en EE. UU., reforzando obligaciones de ciberseguridad.
ISO/IEC 27001:2022 (Internacional)	Define requisitos para un Sistema de Gestión de Seguridad de la Información (SGSI).	Asegura que los procesos automatizados de Amrize cumplan estándares internacionales de seguridad y reduzcan vulnerabilidades.
Ley 1581 de 2012 (Colombia)	Regula la protección de datos personales y principios de tratamiento.	Aplica a todo proceso automatizado que manipule datos personales en el SSC de Colombia.
Decreto 1074 de 2015 (Colombia)	Reglamenta la Ley 1581 e introduce el principio de Responsabilidad Demostrada.	Exige inventarios de datos, auditorías y controles en flujos de RPA/IA.
Circular Externa 002 de 2018 (SIC) (Colombia)	Define países con nivel adecuado de protección de datos.	Habilita transferencias de datos EE. UU.–Colombia bajo reglas específicas.
Ley 527 de 1999 (Colombia)	Reconoce validez de mensajes de datos y documentos electrónicos.	Sustenta la autenticidad de logs y evidencias generadas por bots.
Ley 1273 de 2009 (Colombia)	Tipifica delitos informáticos y protege la información y datos.	Obliga a prevenir accesos indebidos, sabotaje o interceptación en sistemas automatizados.
Ley 222 de 1995 (Colombia)	Regula sociedades comerciales y responsabilidades de administradores.	Exige a la dirección de Amrize actuar con diligencia en decisiones sobre automatización y gestión de riesgos.
Decreto 620 de 2020 (Colombia)	Establece lineamientos de gobierno digital y ciberseguridad.	Obliga a integrar principios de interoperabilidad, seguridad y privacidad en los procesos automatizados de Amrize.

Fuente. Elaboración propia a partir de revisión bibliográfica.

El marco legal aplicable a AMRIZE demuestra la necesidad de articular de manera coherente regulaciones internacionales, federales, estatales y nacionales que inciden directamente en el diseño y operación de procesos automatizados. Esta normatividad no solo garantiza la protección de los inversionistas y la transparencia en los mercados financieros, sino que también salvaguarda la seguridad de los trabajadores, la privacidad de los datos personales y la integridad de los sistemas tecnológicos en los que se soporta la organización.

En este sentido, la gestión de riesgos se convierte en un componente esencial para la sostenibilidad de AMRIZE. La incorporación de marcos como *SOX, NIST, FTC, FCPA*, así como la legislación colombiana en materia de datos y ciberseguridad, permite que la transición hacia operaciones inteligentes se realice con estándares de cumplimiento robustos. Esto fortalece la confianza de los grupos de interés, reduce vulnerabilidades legales, tecnológicas y reputacionales, y asegura que la automatización contribuya a la eficiencia operativa y a su vez al alineamiento estratégico y ético de la compañía.

1.6. Metodología

1.6.1. Enfoque

Este estudio adopta un enfoque mixto, en el que hacen parte del proceso las perspectivas cualitativa y cuantitativa. Según Creswell y Plano Clark (2018), los métodos mixtos permiten integrar la profundidad interpretativa de los enfoques cualitativos con la capacidad de generalización y análisis estadístico de los enfoques cuantitativos. Esta articulación facilita comprender los fenómenos con una perspectiva holística, mejorando la validez de los resultados y garantizando un análisis más completo frente a la problemática planteada.

1.6.2. Estrategia

La estrategia se centra en la formulación de un plan de mejoramiento, concebido como un instrumento de gestión sistemático orientado a reducir brechas de desempeño, corregir deficiencias y fortalecer capacidades organizacionales mediante acciones estructuradas, medibles y sostenibles en el tiempo. De acuerdo con Chiavenato (2017), un plan de mejoramiento traduce los diagnósticos en propuestas concretas de acción, estableciendo objetivos, metas, responsables y mecanismos de seguimiento que contribuyen a la generación de valor y al fortalecimiento de la sostenibilidad institucional.

En el marco de este ejercicio, el plan de mejoramiento se sustenta en tres ejes interdependientes que guían el proceso de transformación. El primero corresponde a la mejora continua y la calidad total, principios que aseguran un proceso permanente de innovación y perfeccionamiento, con el propósito de incrementar el valor entregado a los diferentes grupos de interés. Según López (2005), la calidad total trasciende el cumplimiento normativo y se convierte en un enfoque estratégico que impulsa la innovación y la creación de valor. El segundo eje se relaciona con la gestión del riesgo, la cual, bajo los lineamientos de la norma ISO 31000:2018, reconoce la incertidumbre como un factor inherente a la operación y promueve mecanismos de anticipación frente a posibles amenazas (ISO, 2018). Finalmente, el tercer eje se fundamenta en la automatización de procesos, entendida como un habilitador clave para optimizar tiempos, reducir errores y garantizar trazabilidad. Tal como señalan Mihi y Rivera (2009), las tecnologías de automatización fortalecen la capacidad de adaptación de las organizaciones y potencian su competitividad en entornos cambiantes.

De esta manera, la estrategia planteada trasciende la simple corrección de fallas puntuales, para consolidarse como un modelo integral de gestión caracterizado por su enfoque proactivo, resiliente y orientado a la excelencia organizacional.

1.6.3. Método

El ciclo PHVA (Planear–Hacer–Verificar–Actuar) constituye el método adoptado para estructurar el proceso de mejora organizacional. Propuesto inicialmente por Shewhart y popularizado por Deming, este ciclo se ha consolidado como un referente de gestión de la calidad, al promover la estandarización de actividades bajo una lógica de retroalimentación constante, lo que garantiza aprendizaje organizacional y mejora continua (Castillo, 2019).

En su fase inicial, Planear, se formulan los objetivos, se definen indicadores de desempeño y se establecen acciones correctivas fundamentadas en la evidencia disponible, lo que asegura un punto de partida sólido. Posteriormente, en la fase Hacer, se implementan las acciones planificadas, apoyadas por procesos automatizados que reducen la probabilidad de error humano y mejoran la eficiencia operativa. La tercera fase, Verificar, consiste en la comparación de los resultados obtenidos frente a las metas definidas, utilizando métricas digitales y tableros de control que facilitan un monitoreo en tiempo real. Finalmente, la fase Actuar implica la adopción de medidas de ajuste y la institucionalización de las mejores prácticas, cerrando así un ciclo que no solo corrige desviaciones, sino que también fortalece la gestión del conocimiento.

En este sentido, la metodología PHVA, al ser iterativa y flexible, no se limita a la solución de problemas específicos, sino que permite instaurar un modelo de innovación permanente. Tal como señalan Salazar, Martínez y Ruiz (2020), la aplicación rigurosa de este ciclo fomenta resiliencia organizacional, incrementa la capacidad de adaptación y consolida un marco de mejora sostenible en el tiempo.

1.6.4. Técnicas para la recolección y análisis de la información

El diseño metodológico integra diversas técnicas de recolección y análisis de información, para garantizar confiabilidad, validez y una visión integral del fenómeno estudiado. Estas herramientas permiten capturar información documental, empírica y prospectiva, así como organizar e interpretar los datos obtenidos de manera sistemática.

En cuanto a la recolección de información, se emplea la revisión documental que constituye un análisis crítico y sistemático de literatura académica, normativa y técnica, y la cual proporciona el marco teórico y contextual necesario para sustentar la investigación y orientar la interpretación de los hallazgos (Arias, 2012). A su vez, las entrevistas semiestructuradas representan un instrumento cualitativo que combina preguntas guías con la flexibilidad necesaria para indagar percepciones y significados, favoreciendo la comprensión de los fenómenos estudiados (Kvale, 2011). En complemento, las encuestas estructuradas permiten recopilar información estandarizada de carácter cuantitativo (Creswell & Creswell, 2018). También se incluye el método Delphi, concebido como una técnica prospectiva que, mediante consultas iterativas a expertos, permite generar consensos sobre escenarios futuros, riesgos emergentes o temas estratégicos (Linstone & Turoff, 2002).

Finalmente, se incorpora el uso de Crystal Ball, que es una prueba simulada a partir de una información cuantitativa y que aplica el método de Monte Carlo para modelar riesgos y evaluar escenarios bajo condiciones de incertidumbre, fortaleciendo la capacidad de predicción y el análisis de sensibilidad (Savage, 2014).

Respecto a las técnicas de análisis de la información, se adoptan herramientas que facilitan la interpretación, organización y priorización de los datos. El mapa de riesgos se utiliza como una representación visual que permite identificar, clasificar y jerarquizar los riesgos de manera clara, apoyando la toma de decisiones estratégicas en contextos de incertidumbre (Hopkin, 2018). Por su parte, las matrices de información constituyen instrumentos analíticos que organizan los datos en estructuras comparativas, lo que posibilita detectar patrones, establecer relaciones y reconocer vacíos relevantes para la investigación (Mejía, 2011).

En conjunto, estas técnicas integran evidencia cualitativa y cuantitativa, lo que no solo refuerza la confiabilidad del proceso analítico, sino que también permite construir conclusiones sólidas y fundamentadas, capaces de responder con mayor rigor a los objetivos planteados en el estudio.

1.6.5. Consideraciones éticas

Este proyecto se desarrolla en cumplimiento del artículo 15 de la Constitución Política de Colombia y la Ley 1581 de 2012, garantizando el derecho a la intimidad, la protección de datos personales y el respeto a la privacidad. Todas las fases del estudio se realizan bajo consentimiento informado, con medidas de confidencialidad y anonimización, priorizando la ética, la transparencia y la responsabilidad profesional; la información obtenida se empleará únicamente con fines académicos y será divulgada solo con autorización expresa de *North America Shared Services* – AMRIZE.

2. Plan de Mejora

La segunda fase del trabajo, correspondiente al Plan de Mejora, se estructura a partir del diagnóstico del proceso de *Disputes* junto con la descripción de las automatizaciones implementadas en el mismo, identificando sus ventajas y puntos críticos. A partir de esto, se desarrolla el análisis del proceso, en el que se clasifican y describen los riesgos asociados a cada automatización. Posteriormente, se realiza la evaluación de los riesgos, combinando valoraciones cualitativas y cuantitativas para determinar la probabilidad de ocurrencia y el impacto en USD en el flujo de caja en la continuidad operativa del proceso. Con esto, se plantea la reformulación del proceso mediante la definición de respuesta al riesgo bajo los criterios de aceptación, mitigación, transferencia o evitación. De esta manera, se formulan las estrategias de mitigación y el esquema de manejo, monitoreo y revisión de controles, consolidando así un plan de mejora integral para el proceso de *Disputes* y sus automatizaciones.

2.1. Diagnóstico del proceso

Amrize es una empresa independiente con sede en Estados Unidos que nació tras la escisión completa del negocio norteamericano de Holcim en junio de 2025 operando como una empresa pública o *public company*[1] que cotiza en bolsa bajo el símbolo "AMRZ" en la Bolsa de Nueva York. Esta separación le permite enfocarse exclusivamente en ofrecer soluciones para la construcción en el mercado de Norteamérica (Canadá y Estados Unidos), que incluyen agregado, concreto, asfalto y cemento.

En ese sentido, North America Shared Services se dedica a la prestación de servicios compartidos para AMRIZE. Su función principal consiste en centralizar y estandarizar los procesos administrativos, financieros y contables de las distintas

[1] En Estados Unidos, una *public company* es una sociedad cuyas acciones se ofrecen y negocian públicamente en mercados de valores, y que está sujeta a requisitos de registro y divulgación de información financiera ante la *Securities and Exchange Commission* (SEC), debiendo cumplir obligaciones periódicas de reporte, auditoría y transparencia (Encyclopaedia Britannica, 2026; *U.S. Securities and Exchange Commission*, 2025).

divisiones de la empresa, optimizando la eficiencia operativa, el control interno y la trazabilidad de la información.

AMRIZE opera con un enfoque orientado a la excelencia operativa y la mejora continua, integrando tecnologías digitales, automatización y metodologías globales de gestión como *RPA* y *Six Sigma*, para garantizar la consistencia en la ejecución de procesos transversales críticos. Su estructura funcional está organizada en "torres" que agrupan actividades afines, entre las que se destacan: *Order to Cash* (O2C), *Procure to Pay* (P2P), *Record to Report* (R2R), *Hire to Retire* (H2R), Seguridad (IT), *Internal Control*, *People* y *Strategy and Performance*.

Dentro de AMRIZE, la torre *Order to Cash* (O2C) es un pilar esencial para convertir órdenes comerciales en ingresos liquidados y sostenibles. En este ciclo, el área de Disputas tiene un rol fundamental: recibir, investigar y resolver discrepancias en cuentas de clientes —sea por errores en factura, variaciones en precios, cantidades o descuentos— garantizando que lo facturado coincida con lo cobrado y que los estados contables sean precisos para que puedan cerrarse.

Este proceso es transversal. Disputas interactúa constantemente con otras funciones de O2C como *Credit, Billing*, *Cash Application*, *Customer Data* y *Customer Service*, asegurando que cada decisión o ajuste se alinee con los demás actores del ciclo. De este modo, el proceso de disputas en AMRIZE tiene como propósito investigar y resolver las diferencias que se presentan en los saldos de los clientes, asegurando la conciliación correcta de las cuentas. A través de análisis precisos y resultados verificables, el área contribuye a mantener la transparencia y exactitud de la información financiera, fortaleciendo el control interno y la confiabilidad de los registros contables dentro del ciclo O2C.

El área de Disputas en AMRIZE ha desarrollado un conjunto de automatizaciones orientadas a mejorar la eficiencia, precisión y trazabilidad de sus operaciones dentro del ciclo *Order to Cash* (O2C). Estas herramientas han sido diseñadas para reducir la carga operativa de los analistas, minimizar errores humanos y agilizar la resolución de

diferencias en cuentas de clientes, especialmente en tareas que implican validaciones tributarias, notas crédito o débito, categorización de disputas y extracción masiva de información desde SAP. En total, se han implementado ocho automatizaciones que integran Excel, SAP, *RPA* y *Google Sheets*. Su selección responde a que estos procesos son los de mayor volumen, recurrencia y complejidad técnica dentro del área, por lo que su automatización permite garantizar resultados más uniformes y controlados.

No obstante, pese a los avances tecnológicos alcanzados, el análisis operativo del área de Disputas en AMRIZE evidencia la existencia de diversos puntos críticos que afectan la continuidad, confiabilidad y trazabilidad de los procesos dentro del ciclo *Order to Cash* (O2C). Si bien la automatización ha permitido reducir errores manuales y optimizar tiempos, aún persisten riesgos asociados tanto a factores técnicos como organizacionales que inciden directamente en la eficiencia y en la integridad de la información financiera.

Entre las principales situaciones identificadas se encuentran las fallas en macros y los errores en la información procesada, generados por deficiencias en la programación o en la configuración de las fórmulas utilizadas en Excel. Estas fallas interrumpen la ejecución de procesos automatizados, ocasionan reprocesos y pérdida de tiempo, afectando la productividad general del área. A su vez, las diferencias entre la información obtenida en SAP y la reportada por las herramientas automatizadas reflejan inconsistencias en consultas o parámetros configurados, lo que puede derivar en errores contables y observaciones en auditorías internas o externas.

Asimismo, se presenta la carga incompleta de datos como consecuencia de parámetros erróneos en las consultas de SAP, que generan omisiones en la información clave para la gestión de disputas. Este riesgo adquiere mayor relevancia cuando las omisiones involucran valores tributarios o comprobantes legales, ya que podrían dar lugar a incumplimientos normativos. En el mismo sentido, la validación incorrecta de jurisdicciones fiscales, tasas y códigos tributarios (*tax rate, city, county o district*) representa un riesgo recurrente derivado de *layouts* desactualizados o configuraciones erróneas, que pueden generar sanciones, reprocesos y ajustes retroactivos.

Por otro lado, la dependencia del conocimiento individual de ciertos analistas evidencia la falta de documentación técnica y de planes de respaldo en los procesos automatizados. Cuando el dominio del procedimiento recae en pocas personas, la rotación de personal o la ausencia temporal de un experto genera vulnerabilidad operativa y discontinuidad en las tareas críticas. Esta situación se agrava ante la ausencia de métricas de desempeño (*KPI*) que permitan medir objetivamente los beneficios de las automatizaciones, los ahorros en tiempo o la reducción de errores, lo que impide realizar un seguimiento efectivo de la eficiencia alcanzada.

En materia tecnológica, se identifican riesgos asociados a la corrupción de archivos por falta de controles en el uso de programas externos o versiones no autorizadas de software, exponiendo la información sensible a pérdida o manipulación indebida. De igual manera, la escalabilidad limitada de las automatizaciones constituye un obstáculo para la integración futura con otras áreas, incrementando los costos de migración y reduciendo la capacidad de adaptación frente a nuevas exigencias operativas o regulatorias.

A nivel normativo, el incumplimiento internacional de estándares de control y reporte financiero se relaciona con el desconocimiento o la falta de actualización frente a las normas aplicables, como la Ley Sarbanes–Oxley o las disposiciones fiscales locales. Esta brecha puede derivar en sanciones, restricciones operativas o pérdida de certificaciones corporativas. En cuanto a la continuidad operativa, la ausencia de planes de contingencia ante caídas de sistema, fallas de macros o interrupciones del *RPA* expone al área a la paralización de procesos y a la dependencia de soluciones improvisadas por parte de los empleados.

Adicionalmente, la automatización parcial de trabajos manuales sin políticas claras de transición tecnológica genera inseguridad laboral y resistencia al cambio, afectando la moral del equipo y ralentizando la adopción de nuevas herramientas. A ello se suma el uso de infraestructura externa no controlada, como la instalación de complementos o programas de fuentes no verificadas, que eleva el riesgo de ciberataques y pérdida de control sobre la información.

Otro punto crítico es la pérdida de trazabilidad para auditorías, derivada de la falta de registros o bitácoras en los procesos automatizados, lo cual dificulta el seguimiento de decisiones y la verificación de cumplimiento. Finalmente, los bloqueos y protecciones débiles en Excel permiten la manipulación no autorizada de celdas y fórmulas, comprometiendo la exactitud de los resultados financieros y generando potenciales observaciones o sanciones durante revisiones fiscales.

En conjunto, estos riesgos reflejan la necesidad de fortalecer la gobernanza tecnológica, la documentación de procesos y la capacitación del personal técnico, asegurando que las automatizaciones no solo incrementen la eficiencia operativa, sino que también garanticen la sostenibilidad, la seguridad de la información y la confiabilidad del ciclo O2C en entornos sujetos a auditorías permanentes. Bajo esta perspectiva, las siguientes secciones describen en detalle las automatizaciones implementadas en el área de Disputas de AMRIZE, sus objetivos operativos, flujos funcionales y riesgos específicos o generales asociados a cada una.

2.2. Análisis del proceso

El análisis del proceso se desarrolla mediante la revisión detallada de cada automatización implementada en el área de *Disputes*, describiendo su funcionamiento, los flujos operativos asociados y las interacciones con herramientas como SAP, Excel, *RPA* y las otras utilizadas. Esta revisión permite comprender cómo se ejecutan actualmente las tareas automatizadas, cuáles son sus dependencias técnicas y operativas, y qué situaciones generan interrupciones, reprocesos o pérdida de trazabilidad. A partir de este diagnóstico se identifican los puntos críticos del proceso, lo que constituye la base para avanzar hacia la identificación de los riesgos inherentes a cada automatización.

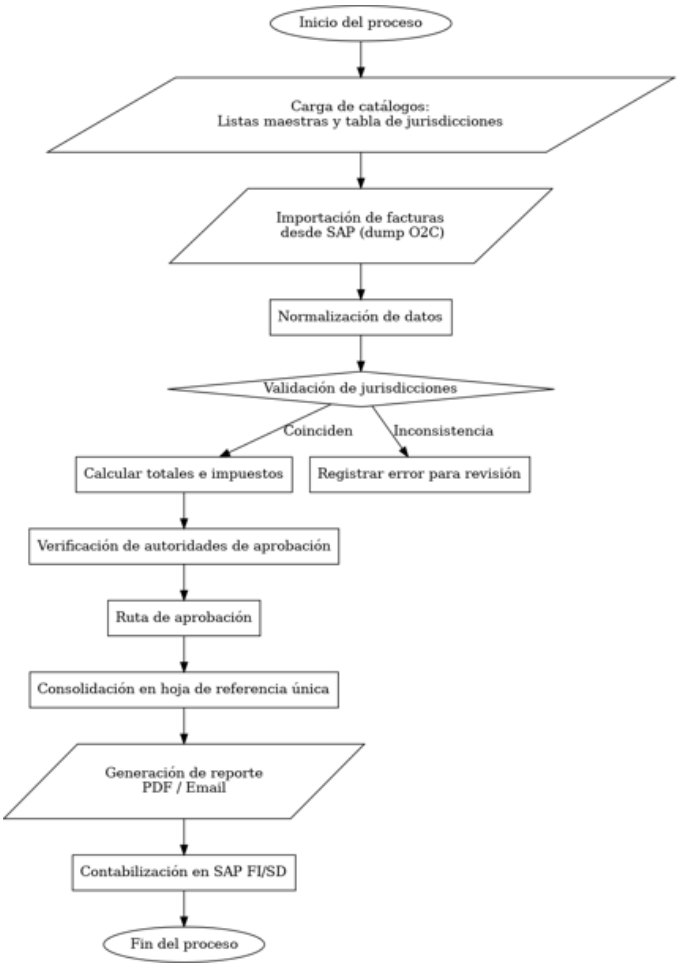
Identificación de los riesgos

La identificación de los riesgos se realiza caracterizando, para siete de las automatizaciones implementadas en Disputas, las vulnerabilidades técnicas, operativas, normativas y de trazabilidad que afectan su desempeño. Este ejercicio permite reconocer riesgos comunes, como fallas en macros, inconsistencias en datos extraídos de SAP, desactualización de bases, ausencia de documentación y dependencia del conocimiento individual, así como riesgos específicos asociados a cada una. La identificación sistemática de estos eventos proporciona el insumo necesario para su posterior evaluación y para la formulación de estrategias de control y mejora.

2.2.1. Validación O2C FI Tax Form USA– AMRIZE:

La automatización de Validación O2C FI *Tax Form* USA tiene como propósito verificar los impuestos de una o varias facturas mediante la extracción directa de información desde SAP. Las macros de Excel estandarizan los datos y los cruzan con una hoja de jurisdicciones que contiene los códigos autorizados para cada región de Estados Unidos, asegurando que los campos de *City, County y District* coincidan correctamente. Si se detecta un error, el sistema marca la celda en rojo e indica el valor correcto, lo que garantiza precisión en la determinación tributaria. En este proceso, uno de los riesgos más comunes es la desactualización de la base de jurisdicciones o la pérdida de validación cuando los códigos cambian en SAP.

Figura 1. Flujograma de automatización Validación O2C FI Tax Form USA - AMRIZE



Fuente. Elaboración propia con Chat GPT a partir de prompt y archivos de Excel.

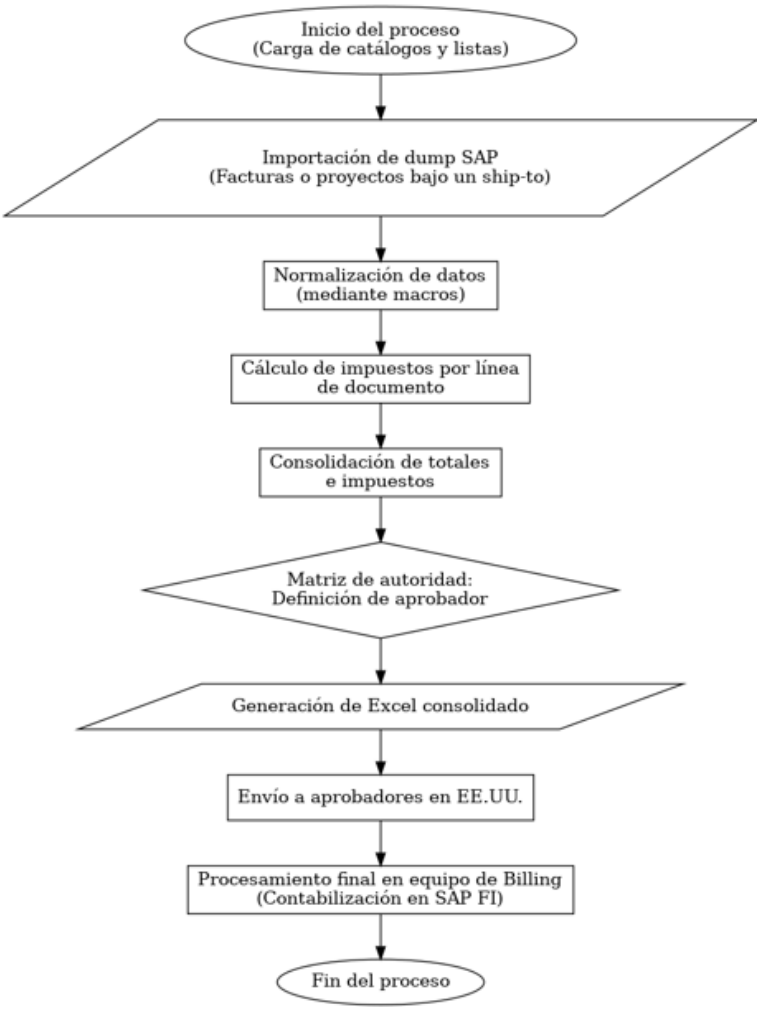
2.2.2. FI Tax Debit and Credit Form USA– AMRIZE:

La FI *Tax Debit and Credit Form* USA automatiza la generación de notas crédito o débito relacionadas con impuestos de facturas o proyectos específicos. A partir del *dump* exportado de SAP, las macros consolidan los datos, calculan los impuestos por línea y

definen automáticamente los aprobadores de acuerdo con la matriz de autoridad establecida. El resultado es un archivo final listo para revisión y aprobación por parte de los equipos de Estados Unidos. Cabe resaltar que, para los débitos fiscales, las aprobaciones deben ser otorgadas por el *Credit Manager* designado a la región y el *Tax Team*, solicitada mediante correo electrónico; mientras que en los créditos fiscales, la aprobación está dada por niveles de acuerdo con los montos del crédito: de USD 0.00 hasta USD 1,500.00 aprueba sólo el *Credit Manager* designado a la región y si es mayor a estos montos o mayor a 6 meses, se requiere tanto aprobación del *Credit Manager* como del *Tax Team*, aprobación que también se solicita mediante correo electrónico.

Los riesgos más relevantes en esta automatización están relacionados con la posibilidad de errores en la matriz de autoridad, duplicación de notas o fallas en el flujo de envío automático a los aprobadores.

Figura 2. Flujograma de automatización FI Tax Debit and Credit Form USA– AMRIZE.



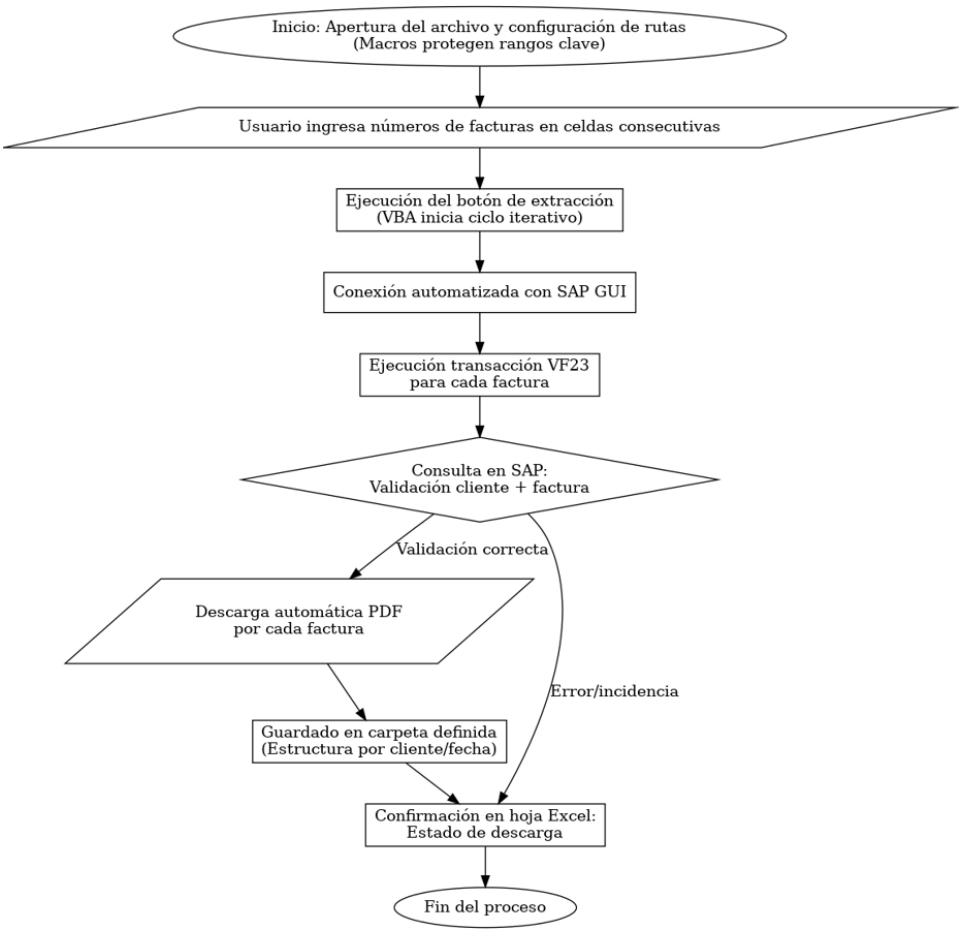
Fuente. Elaboración propia con Chat GPT a partir de prompt y archivos de Excel.

A diferencia de la anterior automatización, esta realiza todo el proceso de rellenar la información que debe ir en la forma, mientras que la descrita anteriormente sólo realiza una validación en el código de jurisdicción para determinar de acuerdo con una lista, si el nombre de la *City*, *County* o *District* coincide con la región y la ubicación del proyecto.

2.2.3. Extracción de facturas en masivo con VF23 USA- AMRIZE:

La extracción masiva de facturas VF23 USA permite descargar múltiples facturas en PDF con un solo clic, mediante un ciclo automatizado que ejecuta la transacción VF23 en SAP para cada número listado. La herramienta valida que cada factura corresponda al cliente correcto y almacena los archivos en carpetas organizadas, registrando los resultados en Excel. No obstante, este proceso puede verse afectado por caídas de conexión, omisión de facturas o saturación del sistema si se ejecutan varios procesos en simultáneo.

Figura 3. Flujograma de automatización VF23 USA- AMRIZE USA– AMRIZE



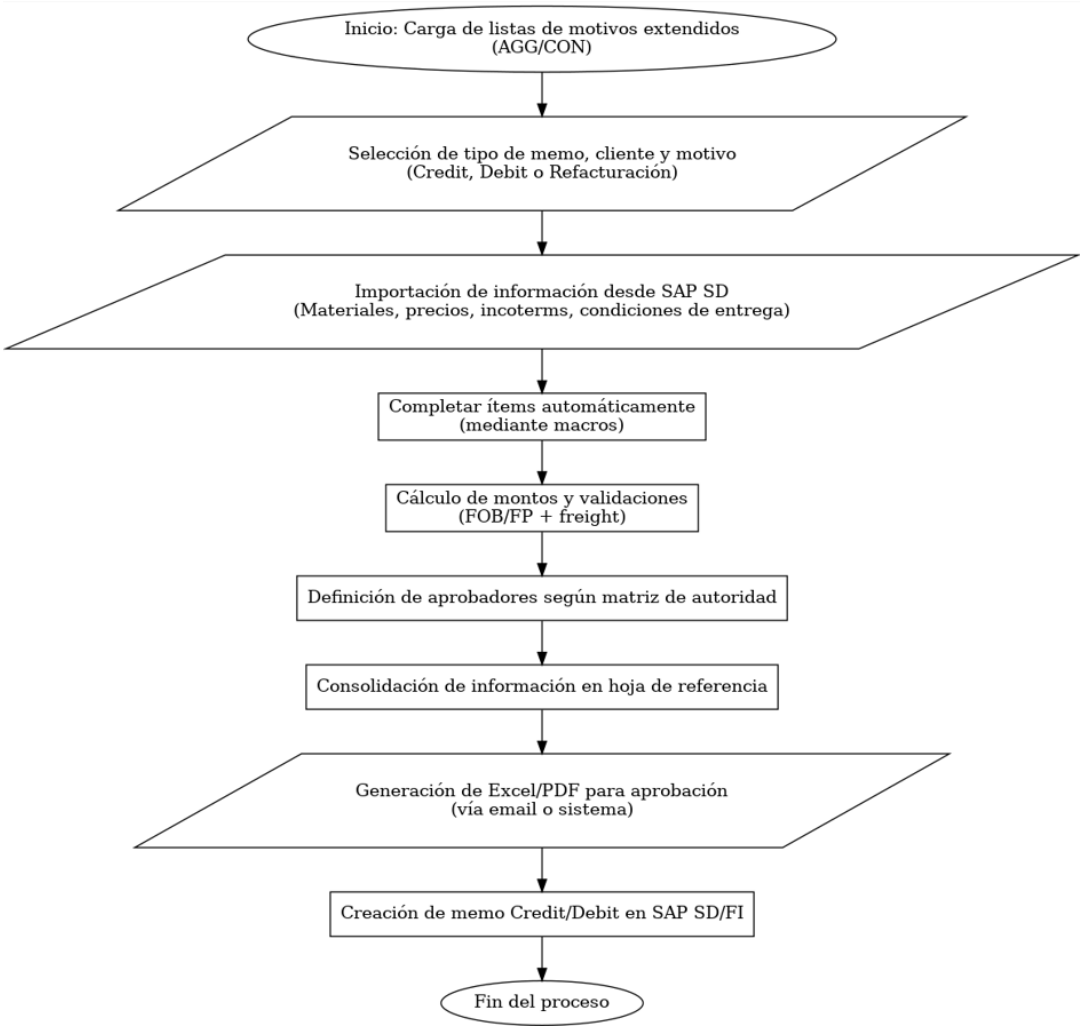
Fuente. Elaboración propia con Chat GPT a partir de prompt y archivos de Excel.

2.2.4. O2C SD Credit or Debit Form USA – AMRIZE:

El formato automatizado O2C SD *Credit or Debit Form* USA facilita la creación de notas crédito o débito por errores en precios, clientes, entregas o calidad del producto. El sistema importa información desde SAP SD, completa los campos de manera automática y realiza validaciones lógicas que aseguran coherencia entre materiales, precios e incoterms. Además, consulta la matriz de autoridad para asignar los aprobadores correspondientes; en ésta, existen 4 niveles de aprobación según los montos y según la región de Estados Unidos: de USD 0 a USD 1,000.00, de USD 1,001.00 a USD 25,000.00, de USD 25,001.00 a USD 100,000.00, y finalmente mayor a USD 100,001.00.

Los riesgos principales en este proceso se relacionan con parámetros erróneos en la selección del tipo de memo, desactualización de aprobadores o inconsistencias en los cálculos automáticos cuando los formatos importados no siguen el estándar.

Figura 4.Flujograma de automatización SD Credit or Debit Form USA – AMRIZE.



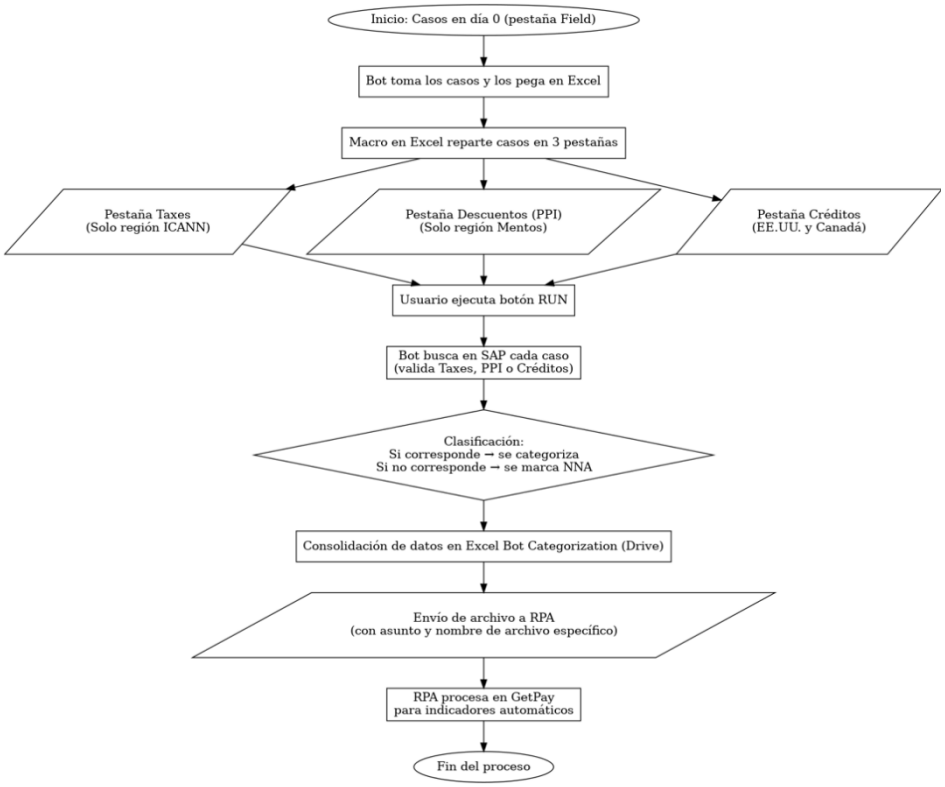
Fuente. Elaboración propia con Chat GPT a partir de prompt y archivos de Excel.

2.2.5. BOT USA – AMRIZE:

El BOT USA – Amrize es una de las herramientas más representativas del avance tecnológico del área. Este sistema clasifica automáticamente los casos de *short payments* del día 0 en categorías como *Taxes*, *Discounts/PPI* y *Credits*, distribuyéndolos en diferentes pestañas dentro de un archivo de Excel. Luego, el proceso se conecta con SAP y finalmente con *RPA*, que completa la categorización automática en *GetPaid*. Gracias a ello, se reduce la carga

operativa y se mejora la eficiencia diaria de los analistas. Sin embargo, existen riesgos derivados de errores en la configuración del BOT, pérdida de registros durante el envío al *RPA* o duplicación de casos por ejecuciones simultáneas.

Figura 5. Flujograma de BOT USA – AMRIZE.



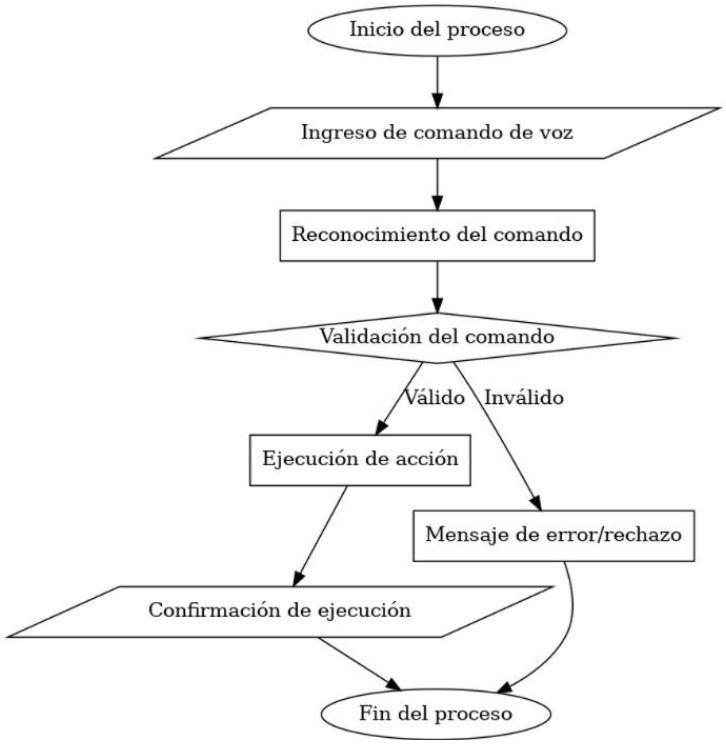
Fuente. Elaboración propia con Chat GPT a partir de prompt y audio de entrevista.

2.2.6. Comando de Voz – Inicia USA – AMRIZE:

La automatización por Comando de Voz – Inicia USA representa un avance en accesibilidad y rapidez de ejecución. El sistema responde a una instrucción de voz definida (“INICIA”) y, tras validar que la orden sea legítima y coincida con un comando autorizado, ejecuta la acción en SAP o Excel. Este proceso permite reducir tiempos en tareas rutinarias, aunque puede verse afectado por

riesgos como activaciones involuntarias, reconocimiento erróneo de voz o brechas de seguridad si no se restringe adecuadamente el acceso.

Figura 6. Flujograma de automatización Comando Voz - Inicia USA – AMRIZE.



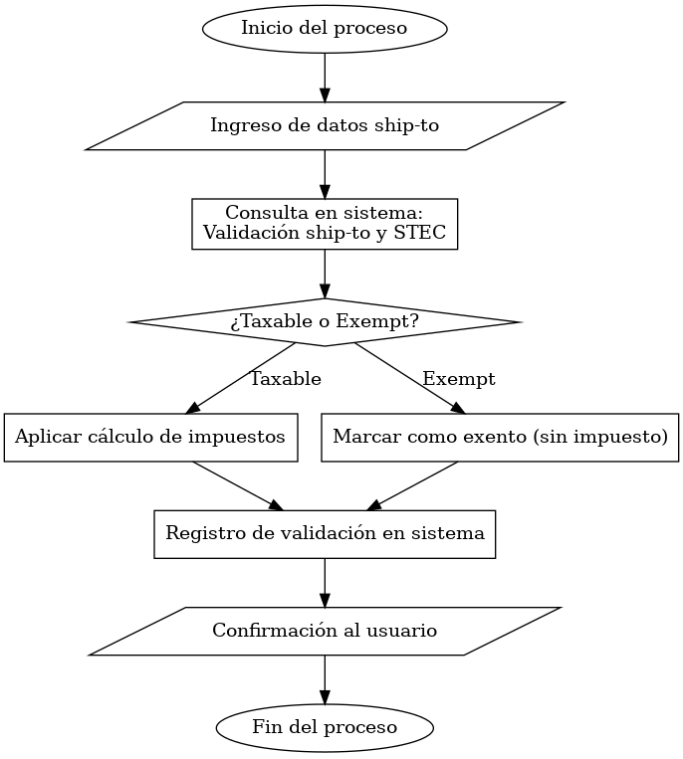
Fuente. Elaboración propia con Chat GPT a partir de prompt y audio de entrevista.

2.2.7. Validación de ship-to y STEC taxable or exempt USA – AMRIZE:

Finalmente, la automatización Validación de Ship-to y STEC *Taxable* or *Exempt* USA consulta una base de datos para determinar si un proyecto pertenece a una jurisdicción gravada o exenta y si cuenta con un documento STEC válido que soporte la exoneración de impuestos. En caso de ser *taxable*, se aplican los cálculos de impuestos extraídos de la FICUST TAX y los resultados se documentan en un archivo para su aprobación por Billing. Los

riesgos más frecuentes incluyen errores de clasificación por datos incompletos, falta de actualización de la base de STEC o aplicación incorrecta de créditos fiscales.

Figura 7. Flujograma de automatización validación de ship-to y STEC taxable or exempt USA – AMRIZE.



Fuente. Elaboración propia con Chat GPT a partir de prompt y audio de entrevista.

En términos generales, las automatizaciones comparten riesgos comunes como la dependencia de macros locales y versiones de Excel sin control de cambios, la exposición a ciberseguridad por el manejo de archivos con información sensible, la sobrecarga del sistema SAP por ejecuciones simultáneas, y las limitaciones en la capacitación del personal para interpretar errores automatizados. También se identifican riesgos de interrupciones en la conexión

con SAP o fallas en los entornos *RPA*, que pueden comprometer la continuidad operativa y retrasar la gestión de disputas.

De manera particular, la automatización FI *Tax Form* presenta riesgos de inconsistencias por errores en la validación de jurisdicciones o códigos desactualizados; FI *Tax Debit* and *Credit Form* puede generar duplicidad en notas o errores en aprobaciones si la matriz de autoridad no está actualizada; VF23 enfrenta riesgos de omisión o descarga incompleta de facturas ante fallas en conexión o secuencias mal definidas; SD *Credit* or *Debit Form* puede verse afectada por parámetros erróneos o cálculos incorrectos cuando el *dump* de SAP no sigue el formato estándar; el BOT de *GetPaid* puede presentar errores en la categorización de casos o pérdida de registros durante la transferencia a *RPA*; la automatización por Comando de Voz enfrenta riesgos de activación involuntaria o reconocimiento inexacto de órdenes; y la Validación de *Ship-to* y STEC puede registrar errores de clasificación o aplicar créditos incorrectos si la base de datos no se encuentra actualizada.

En este contexto, la relación entre el proceso de automatizaciones en Disputas y la problemática planteada radica en la necesidad de asegurar la confiabilidad y continuidad operativa de los sistemas automatizados dentro del ciclo O2C. Si bien las automatizaciones han reducido significativamente los tiempos de respuesta y los errores manuales, su implementación ha evidenciado nuevos desafíos asociados a la dependencia tecnológica, la estandarización de procesos y la capacitación del personal. Las fallas en los entornos *RPA*, la falta de control sobre cada versión y la limitada gestión de incidentes técnicos generan cuellos de botella que afectan la trazabilidad de las operaciones, lo cual es importante para una organización como AMRIZE sujeta a continuas auditorias.

Adicionalmente, es importante mencionar que estas dinámicas pueden generar indirectamente fenómenos de estrés tecnológico, entendido como el impacto negativo derivado del uso intensivo de tecnologías de la información, especialmente cuando existen sobrecargas del sistema, fallas en los procesadores o demoras en los desarrollos y aplicaciones, lo cual afecta el desempeño organizacional y la eficiencia operativa (Tarafdar et al., 2014).

Por tanto, la problemática central no radica en la ausencia de automatización, sino en la necesidad de fortalecer la gobernanza tecnológica y los controles operativos que garanticen su correcto funcionamiento y sostenibilidad a largo plazo, reduciendo la exposición a riesgos sistémicos y previniendo fenómenos de estrés tecnológico asociados a la sobrecarga, complejidad y dependencia de los sistemas automatizados.

Evaluación de los riesgos identificados

La evaluación de los riesgos identificados se lleva a cabo clasificando cada riesgo según su probabilidad de ocurrencia y su impacto operacional, financiero, regulatorio y legal, utilizando tanto insumos del equipo de *Disputes* como la variación del flujo de caja del trimestre julio–septiembre de 2025. Para ello, se asignan valoraciones cualitativas y cuantitativas expresadas en porcentajes de afectación, permitiendo determinar cuáles eventos representan amenazas significativas para la operación y el ciclo O2C, especialmente en el marco de cumplimiento de controles internos sobre información financiera exigidos por la normativa SOX. Este proceso evidencia la magnitud real de los riesgos y facilita priorizar aquellos que requieren acciones inmediatas frente a los que pueden mantenerse bajo monitoreo.

Este proceso implica, además, analizar los eventos identificados que podrían afectar el cumplimiento de los objetivos de la empresa, y comprender qué situaciones de los quince riesgos representan una amenaza, cómo podrían incidir en los resultados del flujo de caja de la organización y en qué medida dichos riesgos interactúan entre sí, influyendo en los procesos y en la operatividad de *Disputes*.

Para esto, se asigna a cada riesgo una valoración cualitativa que permite clasificarlo en uno de los niveles establecidos: Alto, Medio o Bajo y cuantitativa que permite asignar un porcentaje de afectación en el flujo de caja de la empresa – el cual se toma desde julio 2025 hasta el mes de septiembre 2025 -. Ambas valoraciones se definen

mediante reunión con el equipo de *Disputes* teniendo en cuenta cada riesgo evaluado y el nivel de incertidumbre vinculado a posibles eventos futuros.

Tabla 2. Niveles de evaluación cualitativa de los riesgos identificados en los procesos de automatización de Disputas.

Riesgo Bajo	Se presenta cuando la probabilidad de una pérdida esperada es inferior al nivel promedio, considerando tanto la exposición como los factores de incertidumbre asoaciados a eventos futuros.
Riesgo Medio	Corresponde a situaciones en las que la probabilidad de pérdida se ubica en un punto cercano al promedio, con un nivel típico de exposición e incertidumbre que no se desvía de lo habitual.
Riesgo Alto	Se caracteriza por una probabilidad de pérdida considerablemente mayor, derivada de una exposición elevada y de un alto grado de incertidumbre respecto a lo que pueda ocurrir en el futuro.

Fuente. Elaboración propia.

En el análisis cualitativo de los riesgos identificados se tiene que, la operación del área presenta un riesgo alto por la dependencia de macros y automatizaciones en Excel. La inestabilidad de estas herramientas hace que cualquier falla pueda detener el proceso, generar reprocesos y afectar la confiabilidad de la información en etapas críticas de cierre. Por el contrario, el riesgo de diferencias entre SAP y la información automatizada es bajo, gracias a los controles y validaciones cruzadas implementadas.

Por otro lado, los errores asociados a información doblemente validada representan un riesgo moderado, pues generan reprocesos y retrasos, aunque sin impactos operativos severos. La carga incompleta desde SAP se clasifica como baja, dado que ocurre con poca frecuencia y cuenta con verificaciones adicionales. No obstante, la validación incorrecta de impuestos o

jurisdicciones fiscales constituye un riesgo alto por sus implicaciones normativas y sancionatorias.

La dependencia del conocimiento individual es un riesgo alto debido a la falta de documentación técnica, lo que compromete la continuidad operativa. Del mismo modo, la ausencia de métricas que permitan medir el desempeño de las automatizaciones se considera riesgo alto, ya que limita la detección oportuna de fallas y la demostración de beneficios del proceso.

La posible corrupción de archivos por uso de herramientas externas representa un riesgo moderado, mientras que la baja escalabilidad de ciertas automatizaciones es un riesgo bajo que afecta más la proyección futura que la operación actual. El incumplimiento de estándares internacionales, como SOX, se evalúa como moderado gracias a los controles vigentes; sin embargo, la falta de planes de contingencia constituye un riesgo alto por su impacto directo ante caídas del sistema o fallas masivas.

La resistencia al cambio y el uso de infraestructura no autorizada son ambos riesgos altos, ya que pueden afectar la adopción de mejoras, exponer la operación a amenazas cibernéticas y comprometer la integridad de la información. Asimismo, la pérdida de trazabilidad en automatizaciones se clasifica como moderada, mientras que la manipulación indebida de celdas en Excel es otro riesgo moderado que puede alterar cálculos y conciliaciones.

En conjunto, la evaluación cualitativa evidencia riesgos tecnológicos, operativos y legales que en varios casos alcanzan niveles altos, lo que exige reforzar la automatización, la documentación, la seguridad, los indicadores de desempeño y la gestión del cambio para asegurar la estabilidad y confiabilidad del proceso en AMRIZE.

En ese mismo sentido, desde el análisis cuantitativo, complementario al cualitativo, se permite estimar el impacto financiero potencial de cada riesgo sobre el flujo de caja, permitiendo dimensionar en términos monetarios la afectación real que pueden generar fallas operativas, tecnológicas o legales. Para este ejercicio, se analizaron las variaciones y movimientos del flujo de caja entre junio y septiembre de 2025, asignando a cada riesgo un porcentaje de impacto y su equivalencia en millones de USD.

Tabla 3. Niveles de evaluación cuantitativa de los riesgos identificados en los procesos de automatización de Disputas en relación con el Flujo de Caja de AMRIZE.

Valoración Cuantitativa			
Cuenta de Flujo de Caja 2025	**Justificación**	**(%)**	**($ USD)**
Net cash used in operating activities - "Other items, net"	Retrasos y reprocesos internos afectan el flujo operativo.	0,70%	-$ 3,15
Changes in operating assets and liabilities - Accounts receivable, net	Inconsistencias provocan retrasos en acreditaciones y reprocesos por confirmación de información.	0,50%	-$ 4,25
Operating activities – Other items, net	Causa reprocesos y correcciones que reducen eficiencia operativa.	0,60%	$ 0,35
Operating activities –Accounts payable / Accounts receivable	Puede generar registros pendientes o incorrectos que afectan salidas o entradas de efectivo.	0,20%	-$ 1,64
Operating activities – Other liabilities	Sanciones o ajustes fiscales afectan salidas operativas o provisiones.	1,00%	-$ 1,96
Operating activities – Other items, net	Vulnerabilidad operativa ante ausencias o rotación, afectando el flujo operativo.	0,10%	$ 0,06
Operating activities – Other items, net	Dificulta monitoreo del gasto y eficiencia, generando variaciones no controladas.	0,80%	$ 0,47
Operating activities – Other assets	Pérdida o reposición de archivos afecta activos operativos y tiempo de procesamiento.	1,00%	-$ 0,91
Investing activities – Purchases of property, plant and equipment	Aumenta CAPEX no planeado o costos de licencias e inversiones no contempladas.	0,30%	-$ 1,34
Operating activities – "Other liabilities"	Sanciones o ajustes fiscales afectan salidas operativas o provisiones.	1,00%	-$ 1,96
Operating activities – Other items, net	Incrementa costos imprevistos ante incidentes; impacto directo en flujo operativo.	1,00%	$ 0,59
Operating activities – Other items, net	Ajustes de personal y costos transitorios que reducen el flujo operativo.	0,50%	$ 0,30
Investing activities – Acquisitions, net of cash acquired o Operating activities	Pérdida de control sobre infraestructura afectan inversiones y flujos e implica inversiones adicionales no contempladas o no autorizadas previamente.	0,60%	-$ 0,47
Operating activities – Other liabilities	Genera ajustes y reprocesos contables que afectan pasivos operativos.	0,40%	-$ 0,78
Operating activities – Other items, net	Riesgo de manipulación o error que deriva en flujos operativos erráticos.	0,30%	$ 0,18

Fuente. Elaboración propia a partir del Flujo de Caja de AMRIZE del trimestre de julio 2025 a septiembre 2025.

Estos resultados evidencian que varios riesgos, clasificados como altos en la valoración cualitativa, también presentan impactos relevantes en términos monetarios. Los retrasos y reprocesos derivados de fallas en macros representan uno de los impactos más relevantes, con una afectación estimada del 0,70%, equivalente a -3,15 USD, lo cual confirma su clasificación como riesgo alto debido a su potencial para detener el proceso, alterar la secuencia operativa y comprometer los tiempos de cierre. De manera similar, las inconsistencias en la conciliación de cuentas por cobrar y por pagar - originadas en errores dentro de las automatizaciones - muestran variaciones entre 0,50% y 0,20%, con impactos que oscilan entre -4,25 USD y -1,64 USD, reflejando vulnerabilidades contables que deterioran la confiabilidad de la información financiera y exponen al proceso a reprocesos continuos.

En materia fiscal, las sanciones o ajustes originados en validaciones incorrectas de impuestos alcanzan un impacto del 1,00%, equivalente a -1,96 USD, lo que confirma el carácter crítico de este riesgo debido a las implicaciones legales y sancionatorias. A nivel operativo, la ausencia de métricas y controles sobre el desempeño de las automatizaciones genera afectaciones cercanas al 0,50%, con un impacto aproximado de 0,30 USD, evidencia la persistencia de ineficiencias estructurales que limitan la capacidad de monitoreo y mejoramiento continuo.

Otros riesgos, como la pérdida o corrupción de archivos por manipulación o uso de herramientas externas, muestran impactos entre -0,91 USD y -0,78 USD, ubicándose en un nivel moderado, afecta la trazabilidad y obliga a procesos adicionales de revisión. Por su parte, los aumentos no previstos en costos o CAPEX asociados a fallas tecnológicas o necesidades de sustitución de infraestructura registran una afectación del 0,30%, equivalente a -1,34 USD, lo que evidencia su incidencia directa sobre la planificación financiera y la estabilidad presupuestal de la empresa.

Finalmente, la manipulación indebida de celdas y otros errores humanos presentan impactos del orden del 0,30%, con valores cercanos a 0,18 USD, lo cual refuerza su clasificación como riesgo moderado, especialmente por su capacidad de alterar cálculos, comprometer conciliaciones y generar desviaciones en la información operativa.

En conjunto, los porcentajes cuantitativos muestran que los riesgos más significativos en valor monetario coinciden con aquellos que afectan directamente los procesos críticos de *Disputes*: macro dependencia, controles fiscales, reprocesos contables y dependencias individuales de conocimiento técnico. Aunque los montos pueden parecer unitariamente moderados, la frecuencia y acumulación de estos eventos durante el ciclo trimestral pueden representar afectaciones relevantes a la eficiencia operativa y al costo total del proceso.

En definitiva, los riesgos tecnológicos y operativos representan las mayores amenazas, seguidos por los riesgos normativos y fiscales, mientras que los riesgos asociados a escalabilidad, carga incompleta o variaciones menores en automatizaciones presentan impactos más bajos. En consecuencia, se evidencia la necesidad de reforzar las automatizaciones, la seguridad en

archivos, la mitigación de reprocesos, la documentación técnica, y los controles de calidad para garantizar la estabilidad y confiabilidad del proceso en AMRIZE.

2.3. Reformulación del proceso

La reformulación del proceso corresponde a la etapa en la que los riesgos priorizados se traducen en decisiones estratégicas para su tratamiento. Esta, se desarrolla a partir de los resultados de la evaluación, definiendo para cada riesgo la respuesta más adecuada según su nivel de criticidad. Mediante la matriz de probabilidad e impacto, se determina si los riesgos deben ser aceptados, mitigados, evitados o transferidos, integrando criterios técnicos, operativos y financieros. A partir de esta clasificación, se estructuran las acciones de mejora y controles orientados a fortalecer el uso de las automatizaciones, disminuir los reprocesos y asegurar la continuidad operativa de *Disputes*.

2.3.1. Respuesta

La etapa de respuesta al riesgo busca determinar la estrategia más adecuada para cada evento identificado, considerando su relevancia operativa (análisis cualitativo) y su potencial efecto financiero (análisis cuantitativo). Para ello, se aplica una metodología combinada en la que la probabilidad de ocurrencia cualitativa se integra con el nivel de impacto cuantitativo. Este enfoque permite clasificar cada riesgo y asignar la respuesta correspondiente de acuerdo con su criticidad.

La probabilidad fue categorizada en tres niveles (alta, media y baja) con base en la frecuencia histórica del evento y la sensibilidad operativa del proceso. Paralelamente, el impacto fue determinado mediante los porcentajes de afectación cuantitativa, los cuales se agruparon en impacto bajo (0 % – 0,30 %), medio (0,31 % – 0,70 %) y alto (≥ 0,71 %). La

combinación de ambos factores permitió ubicar cada riesgo dentro de la matriz probabilidad–impacto y determinar la respuesta adecuada según los criterios institucionales: ignorar, aceptar, mitigar/transferir o evitar.

Tabla 4. Mapa de calor de los riesgos identificados en las automatizaciones de Disputas.

		Respuesta			
		Ignorar	**Aceptar**	**Mitigar (Transferir)**	**Evitar**
Probabilidad	**Alta**		R2		R5
			R6		
			R14		
	Media	R3	R15	R10	
			R13		
			R11		
			R7		
			R12	R1	
	Baja	R9		R8	
		R4			
		Bajo	**Medio**	**Alto**	
		Impacto			

Fuente. Elaboración propia a partir de cruces de Probabilidad x Impacto para cada riesgo.

Los riesgos clasificados con impacto medio y probabilidad alta, como R1, R7, R10, R11 y R13, fueron definidos como riesgos a mitigar, dado que pueden generar interrupciones operativas, reprocesos y desviaciones que requieren intervención estructural para reducir su materialización. El riesgo R8, con probabilidad media e impacto alto, también fue asignado a mitigación debido a la posibilidad de afectación significativa por corrupción o pérdida de archivos.

Los riesgos con impacto y probabilidad altos, como R5, fueron categorizados como riesgos a evitar, en tanto representan una amenaza crítica con implicaciones normativas y sancionatorias que exceden el umbral aceptable de exposición.

De otro lado, los riesgos con impacto y probabilidad medios, tales como R3, R11, R12, R14 y R15, se clasificaron como riesgos aceptables, ya que su ocurrencia puede gestionarse dentro de las capacidades operativas sin requerir intervenciones extraordinarias. Asimismo, los riesgos con probabilidad alta, pero impacto bajo, como R6, y aquellos con probabilidad baja e impacto medio, como R2, también se consideraron aceptables por su efecto limitado sobre los resultados del proceso.

Los riesgos con probabilidad e impacto bajos, tales como R4 y R9, fueron clasificados como riesgos a ignorar debido a su baja relevancia operativa y su efecto marginal sobre la continuidad del proceso.

La respuesta al riesgo obtenida evidencia una adecuada priorización basada en criterios objetivos y medibles. La metodología permitió identificar riesgos críticos que requieren intervención inmediata (mitigar o evitar) y diferenciar aquellos que pueden ser asumidos por la operación sin afectar la estabilidad del proceso. En consecuencia, la asignación final de estrategias se sustenta en un análisis integrado que combina información cuantitativa del flujo de caja con la valoración cualitativa de la probabilidad, garantizando coherencia metodológica y una gestión del riesgo alineada con las mejores prácticas organizacionales.

2.4. Estrategias de mitigación

Las estrategias de mitigación se desarrollan como continuidad del proceso de identificación, evaluación y reformulación de los riesgos, y constituyen la fase en la que las decisiones definidas en la matriz probabilidad e impacto se transforman en acciones orientadas a reducir la exposición del área de *Disputes*. A partir de los riesgos priorizados, se establecen controles, medidas preventivas y ajustes operativos que permiten fortalecer

la estabilidad de las automatizaciones y asegurar la integridad de los procesos. Esta etapa, además, da paso al esquema de manejo, monitoreo y revisión, mediante el cual se garantiza el seguimiento sistemático de los riesgos, la actualización de los controles implementados y la mejora continua del desempeño operativo y tecnológico del área.

2.4.1. Manejo de los Riesgos, Monitoreo y Revisión de Controles

La etapa de manejo, monitoreo y revisión corresponde al proceso mediante el cual las respuestas definidas para cada riesgo se convierten en acciones concretas orientadas a asegurar su control y seguimiento permanente. Esta fase permite que las decisiones tomadas -Aceptar, Mitigar, Evitar o Ignorar- se apliquen de manera organizada y proporcional al nivel de exposición identificado, fortaleciendo así la estabilidad operativa y la confiabilidad del proceso de automatizaciones de *Disputes*.

Tabla 5. Manejo, monitoreo y revisión de los riesgos.

Riesgo	Manejo propuesto	Monitoreo	Revisión
R1	Revisión periódica del código, pruebas estructuradas y documentación de macros.	Seguimiento mensual del desempeño de la macro y reportes de errores.	Revisión trimestral del código por parte del responsable técnico o automatización.
R2	Reforzar conciliaciones SAP–macro y estandarizar parámetros de extracción.	Verificación de variaciones inesperadas en conciliaciones.	Revisión bimestral de criterios de extracción y consistencia de datos.
R3	Validaciones previas, auditoria interna del archivo y claridad en lógica aplicada.	Control de alertas por valores atípicos y errores recurrentes.	Revisión semestral de estructura del archivo y reglas de negocio implementadas.
R4	Seguimiento básico a cargas de datos, sin nuevos controles.	Monitoreo eventual cuando se actualicen fuentes o estructuras.	Revisión anual para confirmar que el riesgo sigue siendo de baja incidencia.
R5	Eliminación del riesgo mediante ajustes tributarios, doble verificación y soporte del área fiscal.	Verificación continua de cambios normativos aplicables.	Revisión trimestral de configuraciones fiscales en SAP.
R6	Documentación formal y transferencia de conocimiento.	Monitoreo del cumplimiento de manuales y disponibilidad de versiones actualizadas.	Revisión semestral de la documentación técnica y rotación de personal clave.
R7	Implementación de indicadores operativos y de calidad.	Seguimiento mensual de KPIs de reprocesos, tiempos y errores.	Revisión trimestral del tablero de control y ajuste de indicadores.
R8	Políticas de seguridad documental, controles de integridad y uso de repositorios corporativos.	Monitoreo de accesos, modificaciones y patrones inusuales en archivos.	Revisión semestral de medidas de seguridad y estructura de almacenamiento.
R9	Monitorear la escalabilidad ante aumentos futuros de carga.	Evaluación periódica del volumen procesado y tiempos de ejecución.	Revisión anual de la capacidad técnica de automatizaciones.
R10	Fortalecer controles SOX, trazabilidad y auditorías internas.	Monitoreo de cumplimiento SOX en actividades clave.	Revisión semestral o según auditoría interna.
R11	Crear planes de contingencia, respaldos y rutas de recuperación.	Verificación mensual del estado de respaldos y tiempos de recuperación.	Revisión anual del plan de continuidad y pruebas de contingencia.
R12	Capacitación cruzada, identificación de roles críticos y soporte alterno.	Seguimiento del plan de capacitación y disponibilidad de reemplazos.	Revisión anual del mapa de capacidades y dependencias operativas.
R13	Aplicación estricta de políticas de TI, restricción de software externo y monitoreo de accesos.	Monitoreo continuo de uso de herramientas autorizadas.	Revisión trimestral de directrices de TI y cumplimiento.
R14	Registros automatizados, control de versiones y documentación del flujo.	Seguimiento del registro de eventos y trazabilidad de cambios.	Revisión semestral de logs y consistencia de versionamiento.
R15	Validaciones automáticas, revisión entre pares y protección de celdas críticas.	Monitoreo frecuente de errores manuales detectados en validaciones.	Revisión trimestral del diseño

Fuente. Elaboración propia a partir de análisis de información.

El análisis de la tabla anterior evidencia que los riesgos técnicos como R1, R2 y R3 requieren fortalecer controles, estandarizar parámetros y documentar procesos; los riesgos críticos de naturaleza normativa, como R5 y R10, exigen eliminar la causa raíz mediante ajustes fiscales y cumplimiento SOX; mientras que riesgos operativos como R6, R7, R11 o R12 se abordan mediante documentación, indicadores de desempeño, planes de continuidad y capacitación cruzada. Para riesgos de seguridad y trazabilidad —R8, R13 y R14— se priorizan controles de integridad, políticas de TI y registros automatizados. Riesgos de baja relevancia como R4 y R9 se mantienen bajo monitoreo periódicamente sin necesidad de acciones adicionales, y aquellos derivados de intervención manual, como el R15, se controlan mediante validaciones automáticas y revisión entre pares. Cada acción se complementa con esquemas de monitoreo y revisión periódica que permiten detectar desviaciones y ajustar los controles de forma oportuna.

Este tratamiento se complementa con mecanismos de monitoreo continuo y revisiones programadas que aseguran la actualización de controles, la detección temprana de desviaciones y la mejora continua del sistema. En conjunto, el manejo, monitoreo y revisión consolidan la respuesta al riesgo como un proceso dinámico que fortalece la capacidad operativa del área, reduce la probabilidad de fallas críticas y garantiza la alineación con los requisitos técnicos y normativos establecidos.

3. Plan de Acción propuesto con Diagrama de Gantt

3.1. Objetivo

El objetivo del plan de acción es llevar a cabo las actividades definidas en el proceso de reformulación, estableciendo tiempos, responsables y controles que permitan ejecutar de manera ordenada y verificable las acciones de mejora para fortalecer la estabilidad, seguridad, trazabilidad y continuidad de las automatizaciones del proceso de *Disputes* en AMRIZE.

3.2. Alcance

Este plan integra las categorías de riesgo previamente priorizadas y transforma cada actividad en tareas programadas dentro de un cronograma realista y ejecutable, facilitando el monitoreo de avances y el cierre de brechas operativas y tecnológicas, desde cinco categorías definidas en la fase de reformulación del riesgo: Controles técnicos y de calidad del código, Controles tributarios y de cumplimiento, Gestión documental y trazabilidad, Gestión operativa y desempeño, y Gestión de seguridad y Talento Humano.

3.3. Diagrama de Gantt

El plan de acción se presenta mediante el Diagrama de Gantt, ya que permite estructurar las actividades del plan de acción de manera secuencial y organizada, clasificándolas por categorías y mostrando la duración estimada de cada tarea en semanas. Su diseño facilita la visualización del orden de ejecución, la identificación de los periodos de mayor carga operativa, el seguimiento del avance mediante la columna de cumplimiento y la detección temprana de desviaciones a través de los retrasos registrados.

Tabla 6. Diagrama de Gantt propuesto.

CATEGORÍA 1	ACTIVIDAD	TAREA	RESPONSABLE DE LA TAREA	CANTIDAD DE TRABAJO EN SEMANAS		
				ESTIMAR	COMPLETADO	RETRASO
1. Controles técnicos y de Calidad del Código	1.1 Revisión periódica del código, pruebas estructuradas y documentación de macros.	Documentar pasos, funciones y dependencias	Analista de Automatización, Supervisora, Desarrollador y Revisor Técnico	12		12
		Revisar sintaxis y lógica del código				
		Ejecutar pruebas unitarias y pruebas de regresi				
		Actualizar control de versiones				
		Registrar incidentes y cambios en repositorio				
	1.2 Reforzar información SAP–macro y estandarizar parámetros de extracción.	Revisar fuentes SAP	Especialista en SAP, Desarrollador Macros y Analista de Disputes	6		6
		Ajustar parámetros de descarga y filtros				
		Estandarizar columnas y formatos de				
		Probar información SAP manual VS SAP				
	1.3 Validaciones previas, auditoría interna del archivo y claridad en la lógica aplicada.	Revisar reglas del negocio o limitantes	Auditor interno, Analista Técnico y Equipo de Disputes	3		3
		Implementar validaciones automáticas				
		Auditar fórmulas críticas				
		Asegurar coherencia y confiabilidad en información de apoyo				
	1.4 Validaciones automáticas, revisión entre pares y protección de	Añadir validaciones en tiempo real	Analista de Automatización y Desarrollador	5		5
		Establecer revisión por pares antes del uso				
		Proteger celdas clave				
	1.5 Seguimiento básico a cargas de datos, sin nuevos controles.	Monitorear dumps SAP periódicamente	Analista de Automatización, Equipo de Disputes y Desarrollador	48		48
		Registrar inconsistencias detectadas				
		Informar hallazgos de manera mensual al Team Lead				

CATEGORÍA 2	ACTIVIDAD	TAREA	RESPONSABLE DE LA TAREA	CANTIDAD DE TRABAJO EN SEMANAS		
				ESTIMAR	COMPLETADO	RETRASO
2. Controles Tributarios, Normativos y de Cumplimiento	2.1 Eliminación del riesgo mediante ajustes tributarios, doble verificación y soporte del área fiscal.	Verificar datos tributarios (jurisdicciones, STEC, tax rate)	Especialista fiscal y Equipo de Disputes	4		4
		Validar cálculos tributarios con área fiscal				
	2.2 Fortalecer controles SOX, trazabilidad y auditorías internas.	Revisar controles SOX aplicables a O2C y a las automatizaciones	Auditor SOX, Supervisora y Analista de Disputes	10		10
		Garantizar evidencias y logs del proceso				
		Preparar documentación para auditoría				

CATEGORÍA 3	ACTIVIDAD	TAREA	RESPONSABLE DE LA TAREA	CANTIDAD DE TRABAJO EN SEMANAS		
				ESTIMAR	COMPLETADO	RETRASO
3. Gestión Documental, Conocimiento y	3.1 Documentación formal y transferencia de conocimiento.	Crear manuales técnicos y operativos	Equipo Disputes, Desarrollador	8		8
		Registrar decisiones de diseño				
		Realizar sesiones de transferencia al equipo				
	3.2 Políticas de seguridad documental, controles de integridad y uso de repositorios corporativos.	Migrar archivos a repositorios seguros	Desarrollador y IT de la organización	12		12
		Implementar permisos de acceso				
		Controlar integridad (hashing / versioning)				
	3.3 Registros automatizados, control de	Activar logs automatizados	Desarrollador y Analista	12		12
		Configurar sistemas de control de versiones				

Trazabilidad	versiones y documentación del flujo.	Configurar sistemas de control de versiones	Técnico	12		12
		Documentar flujos y excepciones				
	3.4 Definición de controles y gestión de riesgos del proceso automatizado	Identificar riesgos del proceso impactado (Disputes).	Desarrollador, IT, Supervisora y Control Interno	12		12
		Definir controles preventivos y detectivos asociados.				
		Documentar matriz de riesgos y controles (incluye impacto SOX si aplica).				
		Diseñar plan de continuidad y procedimiento ante fallas, validando alineación con estándares SAP.				
CATEGRORÍA 4	**ACTIVIDAD**	**TAREA**	**RESPONSABLE DE LA TAREA**	**CANTIDAD DE TRABAJO EN SEMANAS**		
				ESTIMAR	**COMPLETADO**	**RESTRASO**
4. Gestión Operativa y Mejora del Desempeño	4.1 Implementación de indicadores operativos y de calidad.	Definir KPIs	Supervisora	4		4
		Crear dashboards				
		Establecer periodicidad de medición				
	4.2 Monitorear la escalabilidad ante aumentos futuros de carga.	Probar automatización en escenarios de alta y baja carga	Analista RPA, Desarrollador y Equipo Disputes	12		12
		Medir tiempos de ejecución				
		Ajustar tiempos, loops y consultas				
	4.3 Crear planes de contingencia, respaldos y rutas de recuperación.	Esteblecer back ups de macros y bots	Desarrollador, Equipo IT, Analista RPA	5		5
		Definir rutas de recuperación				
		Probar failover manual				
CATEGORÍA 5	**ACTIVIDAD**	**TAREA**	**RESPONSABLE DE LA TAREA**	**CANTIDAD DE TRABAJO EN SEMANAS**		
				ESTIMAR	**COMPLETADO**	**RESTRASO**
5. Gestión de Seguridad y Talento Humano	5.1 Capacitación cruzada, identificación de roles críticos y soporte alterno.	Mapear roles críticos	Recursos Humanos, Supervisora	5		5
		Asignar suplencias				
		Realizar capacitaciones internas				
	5.2 Aplicación estricta de políticas de TI, restricción de software externo y monitoreo de accesos.	Validar cumplimiento de políticas IT	IT Team, Supervisora	10		10
		Bloquear softwares externos no autorizados				
		Configurar monitoreo de accesos y alertas				

Fuente. Elaboración propia a partir de plantilla de Excel.

3.3.1 Categorías

En la Categoría 1, correspondiente a los controles técnicos y la calidad del código, se concentra el mayor esfuerzo del plan. La revisión periódica del código (12 semanas) y el reforzamiento SAP–macro (6 semanas) representan los hitos principales, complementados por actividades de validación y auditoría interna (3 a 5 semanas) y por el seguimiento continuo de cargas de datos, que se extiende durante 48 semanas debido a su naturaleza operativa. Estas acciones, programadas mayoritariamente en los primeros trimestres, resultan esenciales para mitigar los riesgos asociados a la macro dependencia y a las fallas en la extracción y procesamiento de información.

La Categoría 2, orientada al control tributario y normativo, incorpora tareas especializadas como la verificación fiscal (4 semanas) y el fortalecimiento de los controles SOX y la trazabilidad del proceso (10 semanas). Su ejecución se articula con las

auditorías internas y externas, asegurando el cumplimiento de los requisitos regulatorios y corporativos.

En la Categoría 3, centrada en la gestión documental y la trazabilidad, se incluyen la elaboración de documentación técnica, la migración a repositorios seguros y la activación de registros automatizados y controles de versión. Estas actividades, con duraciones entre 8 y 12 semanas, garantizan la integridad de la información, la conservación del conocimiento y el cumplimiento de las directrices de auditoría y TI.

La Categoría 4, vinculada con la gestión operativa y el desempeño, incorpora acciones claves para el monitoreo y la continuidad del proceso, como la implementación de indicadores (4 semanas), las pruebas de escalabilidad (12 semanas) y la creación de planes de contingencia y recuperación (5 semanas). Su orden respeta la secuencia del ciclo PHVA, avanzando desde la definición de métricas hasta la validación operativa y la preparación para escenarios críticos.

Finalmente, la Categoría 5, relativa a la seguridad y al talento humano, contempla actividades fundamentales para la sostenibilidad del proceso, entre ellas la capacitación cruzada (5 semanas) y la aplicación de políticas de TI (10 semanas). Estas acciones consolidan la estabilidad del recurso humano y refuerzan el cumplimiento de estándares de ciberseguridad.

3.3.2. Actividades (desde el ciclo PHVA)

El plan se estructura bajo la metodología PHVA, lo que asegura una secuencia lógica y orientada a la mejora continua. En Plan (Planear) se ubican actividades de diagnóstico y definición, como la revisión del código (1.1), los ajustes tributarios (2.1), la documentación del proceso (3.1) y la definición de indicadores (4.1).

La fase Do (Hacer) comprende la ejecución operativa: reforzar SAP–macro (1.2), migrar archivos a repositorios seguros (3.2) y realizar pruebas de escalabilidad (4.2).

En Check (Verificar) se integran auditorías, controles SOX, validaciones automáticas y controles de versión (actividades 1.3, 2.2 y 3.3).

Finalmente, Act (Actuar) agrupa acciones de ajuste, continuidad y fortalecimiento, como los planes de recuperación (4.3) y la capacitación cruzada (5.1), asegurando la retroalimentación y estabilización del proceso.

3.3.3. Responsables

La ejecución involucra a múltiples actores. El área funcional del proceso O2C - Disputes (coordinador y jefe de torre O2C), que identifica la necesidad, define el proceso, establece las reglas de negocio y determina los puntos de control requeridos, así como la validación inicial del diseño. El equipo técnico (desarrolladores y analistas RPA y de automatización) se encarga del desarrollo, pruebas y mantenimiento; SAP y Disputes validan la información y los parámetros funcionales; Supervisores y Team Leads realizan el seguimiento y autorizan ajustes; Auditoría interna, SOX y fiscal verifican el cumplimiento normativo; TI y Seguridad administran accesos, repositorios y políticas de ciberseguridad; y Recursos Humanos gestiona la capacitación y el soporte del conocimiento.

3.3.4. Fecha de inicio y de cierre

El plan de acción inicia en la primera semana del ciclo operativo anual, desde donde se activan las actividades técnicas, de control y documentación conforme al cronograma del Diagrama de Gantt. Esto permite una distribución ordenada del trabajo y la priorización de las tareas críticas en las etapas iniciales.

El cierre se establece para la última semana del ciclo anual, una vez finalizadas las actividades técnicas, normativas y operativas, y verificada la efectividad de los controles y la trazabilidad. Esta fase concluye con la revisión del ciclo PHVA, la documentación de lecciones y retroalimentación y la preparación del proceso para el siguiente periodo de

mejora continua, teniendo en cuenta que hay actividades con mayor duración que otras, en términos de semanas.

3.3.5. Controles y Seguimiento

El seguimiento del plan se apoyará en indicadores de avance (estimado, completado y retraso), así como en indicadores de efectividad del control, los cuales serán definidos y formalizados en conjunto con el equipo funcional, técnico y de control interno, de acuerdo con las necesidades del proceso impactado y el nivel de riesgo identificado, permitiendo evaluar no solo la ejecución sino la funcionalidad real de los controles implementados. La supervisión mensual del *Team Lead* y del Auditor SOX refuerza la validez técnica y normativa del proceso. Asimismo, se establece un plan de contingencia que define acciones ante fallas del *bot*, desviaciones significativas o incumplimiento de controles, en alineación con las metodologías de gestión de riesgos aplicadas. Las revisiones periódicas del código, los logs automáticos y el ciclo PHVA garantizan mejora continua y trazabilidad.

En síntesis, el diagrama de Gantt evidencia que el plan de acción está organizado de manera estructurada, gradual y coherente con las prioridades del proceso de *Disputes*. La secuencia en tiempo facilita la ejecución ordenada de las tareas, asegura la integración de los controles técnicos, normativos y operativos, y permite un seguimiento claro del avance y los retrasos. La distribución equilibrada de actividades entre áreas técnicas, fiscales, documentales y de talento humano demuestra una planificación integral que fortalece la estabilidad del proceso y garantiza que las mejoras se implementen de forma sostenible y alineada con la metodología de mejora continua.

4. Recomendaciones

Para asegurar la correcta ejecución del Plan de Mejora, se recomienda, en primer lugar, consolidar una estructura clara de gobernanza que defina responsables, procesos y mecanismos de seguimiento. Esto permitirá una implementación ordenada y reducirá la dispersión operativa entre empleados o la concentración de tareas en ciertas personas.

Se sugiere priorizar las actividades críticas del plan especialmente las relacionadas con estabilidad técnica, cumplimiento SOX y trazabilidad, ya que constituyen la base para garantizar la confiabilidad del proceso y mitigar los riesgos identificados. La ejecución debe apoyarse en controles robustos, documentación actualizada y validaciones constantes que aseguren consistencia en los resultados y minimicen errores.

Asimismo, es fundamental fortalecer la gestión del talento mediante capacitación y transferencia de conocimiento, reduciendo dependencias individuales y asegurando continuidad operativa.

Finalmente, se recomienda mantener un monitoreo permanente a través de indicadores clave y revisiones periódicas, permitiendo ajustar oportunamente el plan, anticipar desviaciones y consolidar una cultura de mejora continua en el proceso de *Disputes*. Este enfoque garantizará que las acciones ejecutadas no solo resuelvan necesidades actuales, sino que preparen al área para desafíos futuros con mayor preparación operativa.

5. Conclusiones

El análisis desarrollado permitió evaluar de manera integral los riesgos asociados a las automatizaciones del proceso de *Disputes*, identificando quince riesgos con impacto operativo, tecnológico y normativo. La combinación de valoración cualitativa y cuantitativa permitió dimensionar su efecto real sobre la continuidad del proceso y sobre el flujo de caja, en coherencia con los principios de Hopkin, Mejía y el marco COSO ERM.

Asimismo, se definieron los controles y respuestas para cada riesgo, estructurados bajo criterios de evitar, mitigar, aceptar o ignorar, lo que permitió asignar acciones proporcionales a su nivel de criticidad. Esta clasificación fortalece la gobernanza del proceso y asegura cumplimiento con los requerimientos normativos y fiscales que aplican a AMRIZE como organización pública en los Estados Unidos.

Del mismo modo, se diseñó un plan de acción robusto, basado en el ciclo PHVA, que integra actividades técnicas, documentales, normativas y operativas, con responsables y tiempos definidos. Este plan proporciona una ruta clara para la mejora continua, la trazabilidad y la sostenibilidad del proceso automatizado.

En conjunto, los resultados permiten concluir que, aunque AMRIZE ha avanzado en la adopción de automatizaciones, estas requieren un marco más sólido de control, documentación y seguimiento. El análisis evidencia que una gestión de riesgos articulada, alineada con marcos teóricos como COSO ERM y las tendencias de automatización (*RPA*), es indispensable para garantizar que las automatizaciones contribuyan efectivamente a la eficiencia operativa, la calidad de la información y el cumplimiento regulatorio.

Referencias Bibliográficas

Aguirre, S., & Rodríguez, A. (2017). Automation in business processes and its impact on productivity. Proceedings of the International Conference on Business and Information. https://www.researchgate.net/publication/319343356_Automation_of_a_Business_Process_Using_Robotic_Process_Automation_RPA_A_Case_Study

Anderson, D. R. (2014). An introduction to management science: Quantitative approaches to decision making (14th ed.). Cengage Learning. https://nibmehub.com/opac-service/pdf/read/Business%20Risk%20Management%20Models%20and%20Analysis%20-Edward%20J.%20Anderson.pdf

Arnanz, A. (2021). Decisiones automatizadas: Problemas y soluciones jurídicas. *Revista de Derecho Público: Teoría y Método, 3*(1), 85–127. https://doi.org/10.37417/RPD/vol_1_2021_535

Auditoría Superior de la Federación (ASF). (2014). *Guía de autoevaluación de riesgos en el sector público*. Auditoría Especial de Tecnologías de Información, Comunicaciones y Control. https://www.asf.gob.mx/

Barrio, J., & Silóniz, A. (2024). Auditoría de procesos robotizados: Retos y oportunidades en el sector público. *Revista de Contabilidad y Auditoría Pública, 30*(2), 45–68. https://asocex.es/wp-content/uploads/2024/11/art-BARRIO.pdf

Blahušiaková, M. (2023). Business process automation – New challenges to increasing the efficiency and competitiveness of companies. *Strategic Management, 28*(3), 18–33. https://doi.org/10.5937/StraMan2300038B

California Privacy Protection Agency. (2023–2024). CCPA/CPRA regulations. California Privacy Protection Agency. https://cppa.ca.gov/

Castillo, L. E. (2019). El modelo Deming (PHVA) como estrategia competitiva para realzar el potencial administrativo. Universidad Militar Nueva Granada.

https://repository.umng.edu.co/server/api/core/bitstreams/c6908a00-bc53-44d5-b402-d0779d159872/content

CISA. (2025, agosto). *Cross-sector cybersecurity performance goals*. Cybersecurity and Infrastructure Security Agency. https://www.cisa.gov/cross-sector-cybersecurity-performance-goals

CISA. (2023, marzo 21). *CISA releases updated cybersecurity performance goals*. Cybersecurity and Infrastructure Security Agency. https://www.cisa.gov/news-events/alerts/2023/03/21/cisa-releases-updated-cybersecurity-performance-goals

Committee of Sponsoring Organizations of the Treadway Commission. (2017). Enterprise risk management—Integrating with strategy and performance. COSO. https://static.poder360.com.br/2023/09/Diretriz-Enterprise-Risk-Management-Coso-2017.pdf

Congreso de la República de Colombia. (2012, 17 de octubre). *Ley estatutaria 1581 de 2012. Por la cual se dictan disposiciones generales para la protección de datos personales*. Diario Oficial. https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=49981

Congreso de la República de Colombia. (2008). *Ley 1266 de 2008: Régimen de habeas data financiero*. Congreso de Colombia. https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=34334

Congreso de la República de Colombia. (2009). *Ley 1273 de 2009: Delitos informáticos*. Congreso de Colombia. https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=34893

Constitución Política de Colombia [Const. Pol. Colom.]. (1991). Artículo 15. https://colombia.justia.com/nacionales/constitucion-politica-de-colombia/titulo-ii/capitulo-1/

Creswell, J. W., & Plano Clark, V. L. (2018). *Designing and conducting mixed methods research* (3.ª ed.). SAGE Publications. https://books.google.com.co/books?id=FnY0BV-q-hYC&printsec=frontcover&source=gbs_atb#v=onepage&q&f=false

eCFR. (2025, Agosto). *17 CFR § 229.106 (Item 106) – Cybersecurity*. Electronic Code of Federal Regulations. https://www.ecfr.gov/current/title-17/chapter-II/part-229/subpart-229.100/section-229.106

eCFR. (2025, Agosto). *40 CFR Part 63, Subpart LLL – NESHAP Portland Cement*. Electronic Code of Federal Regulations. https://www.ecfr.gov/current/title-40/chapter-I/subchapter-C/part-63/subpart-LLL

eCFR. (2025, Agosto). *40 CFR Part 98, Subpart H – Cement production*. Electronic Code of Federal Regulations. https://www.ecfr.gov/current/title-40/chapter-I/subchapter-C/part-98/subpart-H

EEOC & DOJ. (2022). *The Americans with Disabilities Act and the use of software, algorithms, and AI to assess job applicants and employees*. U.S. Equal Employment Opportunity Commission. https://www.eeoc.gov/

Eldridge, S. (2026, 14 de febrero). *Public Company*. *Encyclopedia Britannica*. https://www.britannica.com/money/public-company

FCC. (s. f.). *Equipment authorization – Supplier's declaration of conformity/certification (Part 15)*. Federal Communications Commission. https://www.fcc.gov/

Flechsig, C., Anslinger, F., & Lasch, R. (2022). Robotic process automation in purchasing and supply management: A multiple case study on potentials, barriers, and implementation. *Journal of Purchasing & Supply Management, 28*(1), Article 100718. https://doi.org/10.1016/j.pursup.2021.100718

FTC. (2023). Keep your AI claims in check. Federal Trade Commission. https://www.ftc.gov/business-guidance/blog/2023/03/keep-your-ai-claims-check

García, M., Quispe, C., & Ráez, L. (2003). Mejora continua de la calidad en los procesos. Industrial Data, 6(1), 89-94. https://www.redalyc.org/pdf/816/81606112.pdf

Hall, L. (2024). *Transforming accounting: Robotic Process Automation in the accounting environment* [Tesis doctoral, Virginia Commonwealth University]. VCU Scholars Compass. https://scholarscompass.vcu.edu/etd

Hernández, R., Fernández, C., & Baptista, P. (2014). *Metodología de la investigación* (6.ª ed.). McGraw-Hill Education. https://www.esup.edu.pe/wpcontent/uploads/2020/12/2.%20Hernandez,%20Fernandez%20y%20Baptista-metodolog%C3%ADa%20Investigacion%20Cientifica%206ta%20ed.pdf

Holcim. (2025, 21 de febrero). El negocio de Holcim en Norteamérica se llamará Amrize tras la prevista escisión. *Holcim España*. https://www.holcim.es/el-negocio-en-norteamerica-se-llamara-amrize

Hopkin, P. (2018). Fundamentals of risk management: Understanding, evaluating and implementing effective risk management (5th ed.). Kogan Page. https://unidel.edu.ng/focelibrary/books/Fundamentals%20of%20Risk%20Management_%20Understanding,%20evaluating%20and%20implementing%20effective%20risk%20management%20(%20PDFDrive%20).pdf

Instituto Nacional Electoral. Unidad Técnica de Servicios de Informática. (2020, 4 de febrero). *Procedimiento de failover: Sistema de representantes de partidos políticos y candidaturas independientes*. Instituto Nacional Electoral. https://repositoriodocumental.ine.mx/xmlui/bitstream/handle/123456789/117610/ccoe-se23092020-p3-5-Acdo.pdf

ISO. (2018). ISO 31000:2018. Gestión de riesgos – Directrices. International Organization for Standarization. https://www.ramajudicial.gov.co/documents/5454330/14491339/Norma.ISO.31000.2018.Espanol.pdf/cb482b2c-afd9-4699-b409-0732a5261486

Lam, J. (2014). Enterprise risk management: From incentives to controls (2nd ed.). Wiley. https://students.aiu.edu/submissions/profiles/resources/onlineBook/X9P8W6_Enterprise%20Risk%20Management.pdf

Leland, A. (2024, junio 20). *Fundamentals of the COSO Framework: Building blocks for integrated internal controls*. AuditBoard. https://auditboard.com/blog/coso-framework-fundamentals?utm_source=chatgpt.com

López, R. (2005). La calidad total en la empresa moderna. Perspectivas, 8(2), 67-81. https://www.redalyc.org/pdf/4259/425942412006.pdf

Naim, M. (2022). La revancha de los poderosos: Cómo los autócratas están reinventando la política en el siglo XXI. Debate. https://americanjournal.org/index.php/ajbmeb/article/view/37/26

National Association of Attorneys General. (s. f.). *State data breach notification laws – Overview*. NAAG. https://www.naag.org/

Navas, W., Catota, V., & Ramírez, S. (2023). Calidad Total. Herramienta para crear valor. Religación Press. https://press.religacion.com/index.php/press/catalog/view/49/140/286

NIST. (2022). *SP 800-82 Rev. 3: Guide to industrial control systems (ICS) security*. National Institute of Standards and Technology. https://csrc.nist.gov/publications/detail/sp/800-82/rev-3/final

NIST. (2024). *Cybersecurity framework 2.0*. National Institute of Standards and Technology. https://www.nist.gov/cyberframework

NIST. (2025). *Executive Order 14110 rescinded: AI policy resources*. National Institute of Standards and Technology. https://www.nist.gov/artificial-intelligence

NYC Department of Consumer and Worker Protection. (s. f.). *Automated employment decision tools law (Local Law 144)*. City of New York. https://www.nyc.gov/assets/dca/downloads/pdf/workers/144

NYSE. (2025). *Listed company compliance guidance memo*. New York Stock Exchange. https://www.nyse.com/publicdocs/nyse/regulation/nyse/Compliance_Guidance_Memo.pdf

NYSE. (s. f.). *Regulation – Timely disclosure policy (Market Watch)*. New York Stock Exchange. https://www.nyse.com/regulation

Mejía, J. (2011). Fundamentos de administración de riesgos. Editorial Universidad del Rosario. https://editorial.eafit.edu.co/index.php/editorial/catalog/download/633/1226/2636?inline=1

Mejía, J., Núñez, C., Villanueva, M., & Jaraba, J. (2024). Gestión integral del riesgo empresarial. Ecoe Ediciones. https://editorial.eafit.edu.co/index.php/editorial/catalog/book/633

Mihi, A., & Rivera, H. (2009). El mejoramiento continuo. Universidad del Rosario. https://repository.urosario.edu.co/server/api/core/bitstreams/2e438b69-6536-418b-b213-98558d4035ae/content

Ministerio TIC. (2018). *Guía de computación en la nube: Lineamientos de contratación y gestión de riesgos*. Ministerio de Tecnologías de la Información y las Comunicaciones. https://normograma.mintic.gov.co/mintic/docs/guiacomputacionenlanube.pdf

OSHA. (s. f.). *29 CFR 1910.212 – General requirements for all machines*. Occupational Safety and Health Administration. https://www.osha.gov/laws-regs/regulations/standardnumber/1910/1910.212

Reuters. (2024). *Illinois passes BIPA damages limit, overview of biometrics litigation*. Reuters. https://www.reuters.com/legal/transactional/illinois-passes-bipa-damages-limit-overview-biometrics-litigation-2024-08-29

Reuters. (2025, 28 de marzo). Holcim targets M&A deals to fuel growth following Amrize spin off. *Reuters*. https://www.reuters.com/business/holcim-target-ma-deals-fuel-growth-following-amrize-spin-off-2025-03-28/

Robinson, C. L., & Chan, D. Y. (2022). *Potential Risks Inherent in Robotic Process Automation. Journal of Vincentian Social Action*, 6(2), Article 11. scholar.stjohns.edu/jovsa/vol6/iss2/11

Rojas, P. A. (2023). *La influencia de la Robotic Process Automation en la función de la gestión financiera en las empresas* [Trabajo de grado, Pontificia Universidad Javeriana]. Repositorio Institucional PUJ. https://repository.javeriana.edu.co/items/b855239f-1832-4e0b-98e3-a7054b0367d3

Salazar, J., Mora, N., Romero, W., & Ollague, J. (2020). Diagnóstico de la aplicación del ciclo PHVA según la ISO 9001:2015 en la empresa INCARPALM. 593 digital Publisher CEIT, 5(6-1), 459-472. https://dialnet.unirioja.es/servlet/articulo?codigo=7897683

Sánchez Sánchez, L. R. (2015). *COSO ERM y la gestión de riesgos*. Quipukamayoc, 23 (44), 43–50. Universidad Nacional Mayor de San Marcos. https://d1wqtxts1xzle7.cloudfront.net/74741021/COSO_ERM_y_la_gestion_de_riesgos-libre.pdf

SEC. (2025, mayo 20). *Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure – Final Rule*. U.S. Securities and Exchange Commission. https://www.sec.gov/rules-regulations/2023/07/s7-09-22

Stulz, R. M. (2006). Risk management failures during the financial crisis. Journal of Financial Economics, 104(3), 392–412. https://www.sfu.ca/~poitras/419_Stulz_ERM_06.pdf

Superintendencia de Industria y Comercio. (2018a). *Circular Externa 002 de 2018: Lista de países con nivel adecuado de protección y deberes de responsabilidad demostrada*. Superintendencia de Industria y Comercio. https://www.sic.gov.co/circular-externa-002-de-2018

Superintendencia de Industria y Comercio. (2018b). *Circular Externa 003 de 2018: Reporte de incidentes de seguridad de la información*. Superintendencia de Industria y Comercio. https://www.sic.gov.co/circular-externa-003-de-2018

Superintendencia de Industria y Comercio. (2019). *Recomendaciones para el tratamiento de datos en inteligencia artificial*. Superintendencia de Industria y Comercio. https://www.sic.gov.co/recomendaciones-ia

Tarafdar, M., Tu, Q., Ragu-Nathan, B. S., & Ragu-Nathan, T. S. (2014). The impact of technostress on role stress and productivity. *Journal of Management Information Systems, 24*(1), 301–328. https://doi.org/10.2753/MIS0742-1222240109

The White House. (2025). *Removing barriers to responsible American AI innovation*. The White House. https://www.whitehouse.gov/

U.S. Department of Justice & SEC. (2020). *A resource guide to the U.S. Foreign Corrupt Practices Act* (2nd ed.). U.S. Department of Justice. https://www.justice.gov/criminal-fraud/fcpa-resource-guide

US Legal Forms. (2025, 5 de Agosto). *Public company: A comprehensive guide to its legal definition*. https://legal-resources.uslegalforms.com/p/public-company

U.S. Securities and Exchange Commission. (2025). *Public companies*. https://www.sec.gov/resources-small-businesses/capital-raising-building-blocks/public-companies

U.S. Securities and Exchange Commission. (2025). *Types of registered offerings*. https://www.sec.gov/resources-small-businesses/capital-raising-building-blocks/types-registered-offerings

Van der Aalst, W., Bichler, M., & Heinzl, A. (2018). Robotic process automation. *Business & Information Systems Engineering, 60*(4), 269–272. https://www.researchgate.net/publication/325129640_Robotic_Process_Automation

Willcocks, L., Lacity, M., & Craig, A. (2017). Robotic Process Automation: Strategic transformation lever for global business services? *Journal of Information Technology Teaching Cases, 7*(1), 17–28. https://eprints.lse.ac.uk/71146/1/Willcocks_Robotic%20process%20automation_author_2017%20LSERO.pdf