FACULTAD DE POSTGRADO TRABAJO FINAL DE GRADUACIÓN

DISEÑO DE UN SISTEMA DIGITAL DE GESTIÓN DOCUMENTAL EN MIPYMES DE SERVICIOS PROFESIONALES, ESTRUCTURADO CON NORMAS ISO Y MARCO NIST DE CIBERSEGURIDAD: CASO DE ESTUDIO SEGURO TOTAL CORREDURÍA DE SEGUROS

SUSTENTADO POR:

CHRISTIAN VICENTE PADILLA LIMA
JASON OMAR RODRÍGUEZ QUIÑONEZ

PREVIA INVESTIDURA AL
TÍTULO DE MÁSTER EN
GESTIÓN DE LAS TECNOLOGÍAS DE LA INFORMACIÓN

TEGUCIGALPA, FM, HONDURAS, C.A.

03 DE FEBRERO, 2026

UNIVERSIDAD TECNOLÓGICA CENTROAMERICANA

UNITEC

FACULTAD DE POSTGRADO

AUTORIDADES UNIVERSITARIAS

RECTORA

ROSALPINA RODRÍGUEZ GUEVARA

VICERRECTOR ACADÉMICO

NACIONAL JAVIER ABRAHAM

SALGADO LEZAMA

SECRETARIO GENERAL

ROGER MARTÍNEZ

MIRALDA

DECANA DE POSTGRADO

ANA DEL CARMEN RETALLY VARGAS

Diseño de un Sistema Digital de Gestión Documental en MiPymes de Servicios Profesionales, estructurado con Normas ISO y Marco NIST de Ciberseguridad: Caso de Estudio Seguro Total Correduría de Seguros

TRABAJO PRESENTADO EN CUMPLIMIENTO DE LOS REQUISITOS EXIGIDOS PARA OPTAR AL TÍTULO DE MÁSTER EN GESTIÓN DE TECNOLOGÍAS DE LA INFORMACIÓN

ASESOR METODOLÓGICO

JORGE RAÚL MARADIAGA CHIRINOS

ASESOR TEMÁTICO

JUAN CARLOS ALMENDÁREZ FLORES

MIEMBROS DE LA TERNA:

ELVIN BOBABILLA

JOSUÉ MEJÍA

JULISSA CORTÉS

FACULTAD DE POSTGRADO TRABAJO FINAL DE GRADUACIÓN

Diseño de un Sistema Digital de Gestión Documental en MiPymes de Servicios Profesionales, estructurado con Normas ISO y Marco NIST de Ciberseguridad: Caso de Estudio Seguro Total Correduría de Seguros

Christian Vicente Padilla Lima
Jason Omar Rodríguez Quiñonez

Resumen

La presente investigación se centra en explorar y describir las necesidades de las micro, pequeñas y medianas empresas (MiPymes) del rubro de servicios profesionales en Honduras, enfocándose en el caso de estudio de la correduría Seguro Total. El problema principal radica en la falta de digitalización y centralización de documentos, lo cual ha limitado la competitividad, pérdida de información, accesos no autorizados y tiempos altos de búsqueda. Es por esto por lo que se plantea realizar el diseño y las directrices de un Sistema de Gestión Documental, fundamentado en las normas ISO 15489, ISO 30301 e ISO 27001 y tomando en cuenta el Marco de NIST de Ciberseguridad. La investigación cuenta con un enfoque mixto con predominancia de lo cualitativo con un alcance descriptivo y explicativo. La muestra se ha definido probabilística por medio de juicio para los colaboradores, compañías aseguradoras y seguros mediante criterios de inclusión y exclusión. Por otro lado, instrumentos como los cuestionarios, entrevistas, listas de verificación, entre otros permitieron identificar puntos de dolor y oportunidades de mejora para un sistema de gestión documental. Tras analizar los resultados obtenidos, se identificando puntos de mejora como ser el almacenamiento, definición de roles y responsabilidades, definición de políticas de seguridad y colaboración interna y la accesibilidad de la información. Esto ha permitido enlazar las oportunidades identificadas frente a los lineamientos de las Normas ISO y el Marco NIST mediante una propuesta de aplicabilidad.

Palabras clave: Cumplimiento Normativo, Marco NIST Ciberseguridad, Normas ISO, Sistema de Gestión Documental, Transformación Digital.

GRADUATE SCHOOL

Design of a Digital Document Management System in SMEs of Professional Services, Structured with ISO Standards and the NIST Cybersecurity Framework: A Case Study of Seguro Total Insurance Brokers

Christian Vicente Padilla Lima
Jason Omar Rodríguez Quiñonez

Abstract

The present research focuses on exploring and describing the needs of micro, small, and medium-sized enterprises in the professional services sector in Honduras, using the case study of the brokerage firm Seguro Total. The main problem lies in the lack of digitization and centralization of documents, which has limited competitiveness and led to loss of information, unauthorized access, and long search times. For this reason, the study proposes the design and guidelines of a Document Management System, grounded in ISO 15489, ISO 30301, and ISO 27001 standards, and aligned with the NIST Cybersecurity Framework. The research adopts a mixed-method approach with a predominance of qualitative analysis and a descriptive and explanatory scope. The sample was defined probabilistically through judgment sampling for collaborators, insurance companies, and insurers based on inclusion and exclusion criteria. Additionally, instruments such as questionnaires, interviews, and checklists helped identify pain points and improvement opportunities for a potential document management system. After analyzing the results, several areas for improvement were identified, including storage, definition of roles and responsibilities, establishment of security policies, internal collaboration, and information accessibility. This made it possible to connect the identified opportunities with the guidelines of the ISO standards and the NIST Framework through an applicability proposal.

Keywords: Digital Transformation, Document Management System, ISO Standards, NIST Cybersecurity Framework, Regulatory Compliance.

DEDICATORIA

A **mis padres**, los cuales siempre me han apoyo y dado lo mejor para que pueda sobresalir personal y profesionalmente. Por cada uno de sus sacrificios, amor incondicional y por creer en mí en cada paso de mi vida para seguir cumplimiento metas. Sin ellos no fuera la persona que soy hoy.

A las **grandes maestras** dentro de mi familia que me han acompañado y enseñando el valor del aprendizaje Thelma Avelar, Thelma Flores Q.E.P.D, Vilma Ferrufino Q.E.P.D.

-Christian Vicente Padilla Lima

A **mi padre y madre, q**uienes con su increíble esfuerzo me han guiado por un camino lleno de amor, valores y apoyo constante. Gracias por darme dirección y mostrarme que todo esfuerzo tiene su recompensa.

A **mis hermanos,** la luz de mi vida, cuyo amor y apoyo incondicional me brindan la fuerza para seguir creciendo día a día. Sin ustedes, no sería la persona en la que me he convertido.

-Jason Omar Rodríguez Quiñonez

AGRADECIMIENTO

A Dios, por ser quien ha puesto estas oportunidades en mi vida para aprovecharlas y seguir creciendo lleno de fe y esperanza que se vienen nuevas metas por cumplir.

A **mi hermano, novia y tíos** los cuales han estado conmigo en cada paso que he dado tanto en mi vida personal como profesional creyendo en mí e impulsándome a lograr mucho más de lo que soñé.

Al **Lic. Jorge Chirinos y Lic. Juan Almendarez,** por su apoyo incondicional en que esta investigación sea de gran calidad y de impacto para nuestro caso de estudio.

A **mí persona,** por todo el sacrificio, esfuerzo y dedicación invertida en cada una de las clases de la maestría para expandir mi conocimiento y lograr el hito de mi segunda maestría.

-Christian Vicente Padilla Lima

A **Dios** primordialmente, que ha sido el motor de mi vida y el constante apoyo en cada lucha que he tenido.

A **mi padre**, porque ha sido el ejemplo por seguir en cada faceta de la vida, brindándome en todo momento el apoyo y amor que he necesitado.

A **mi madre**, porque ha sido mi guía, la mejor amiga y madre que puedo pedir. Desde muy pequeño, su amor y su confianza en mis capacidades han contribuido a formar al hombre que soy hoy.

A **mis hermanos y pareja**, quienes han sido mi guía y mi luz en cada momento. Su apoyo y esa forma de hacerme ver que puedo lograr lo que me proponga ha sido indispensables para mí.

A **mí mismo**, por cada noche, cada esfuerzo y cada sacrificio que he tenido para estar aquí; por no rendirme nunca y por mantener viva la creencia en alcanzar mis sueños más anhelados.

-Jason Omar Rodríguez Quiñonez

ÍNDICE DE CONTENIDO

ÍNDICE DE TABLAS

ÍNDICE DE FIGURAS

ÍNDICE DE GRÁFICOS

CAPÍTULO I. PLANTEAMIENTO DE LA INVESTIGACIÓN

1.1 INTRODUCCIÓN

La transformación digital ha generado cambios profundos en la forma en que las organizaciones gestionan su información. El almacenamiento, procesamiento y uso estratégico de los datos ya no son exclusivos de las grandes organizaciones, sino también de las MiPymes que se enfrentan a problemas urgentes de actualizar sus procesos informáticos para garantizar su competitividad, eficiencia y asegurar el cumplimiento normativo.

Las MiPymes que operan en áreas como la asesoría legal, contabilidad, seguros o consultoría, solicitan, generan y almacenan grandes volúmenes de documentación relacionada con clientes, contratos, autorizaciones, reportes financieros y obligaciones regulatorias. Sin embargo, en muchos casos esta información es administrada mediante prácticas tradicionales: archivos físicos, almacenamiento disperso o plataformas informales sin control ni trazabilidad. Esta situación genera riesgos como pérdida de información, accesos no autorizados, incumplimiento de requisitos legales y procesos administrativos lentos o ineficientes.

El problema radica en la falta de insumos o herramientas que disponen estas empresas, ya que no cuentan con sistema de gestión digital que estructure su información. Entre las causas más relevantes de este problema encontramos el desconocimiento de herramientas disponibles, la percepción de un alto costo de implementación y falta de capacidades técnicas que apoyen el proceso de implementación como de mantenimiento. Dichas barreras no solo afectan la eficiencia operativa, sino que también comprometen la capacidad de la empresa de resguardar su información y la de sus partes interesadas internas como externas.

Además, factores como el marco legal Nacional refuerzan la necesidad de que las MiPymes aseguradores adopten prácticas documentales alineadas a estándares internacionales como lo es la ISO/EIC 27001 o la Norma ISO 15489 o un marco de Ciberseguridad como lo es la NIST. Estas referencias permiten integrar la gestión documental no sólo como un soporte para la operatividad de la empresa, sino como un pilar estratégico y de gobernanza de datos.

El interés de esta investigación surge tanto del ámbito académico como profesional. Desde la perspectiva académica, se busca aportar a la discusión sobre transformación digital en MiPymes a través de un enfoque realista y aplicable. A su vez, en el ámbito profesional, el objetivo es ofrecer una propuesta concreta para organizaciones que, por falta de recursos o información, continúan operando bajo esquemas tradicionales que ponen en riesgo su

funcionamiento.

También se pretende concientizar sobre las ventajas de la adopción de herramientas de gestión de documentación digital, desafiando que toda solución tecnológica es muy costosa. Se detalla la metodología de la investigación, así mismo, la identificación de las variables, los instrumentos, procedimientos necesarios para la recolección, análisis e interpretación de la información.

Se propone mostrar cómo estas herramientas pueden alinearse a los objetivos estratégicos y a los indicadores de rendimiento (KPIS) de la empresa para una alineación adecuada.El fin de esta investigación es diseñar un sistema de gestión de documentación adaptado a capacidades y necesidades reales de las MiPymes hondureñas orientadas a servicios profesionales basado en un enfoque de seguridad de la información y accesibilidad.

En el capítulo 1 se realiza el planteamiento de la investigación buscando dar respuesta a ¿De qué manera un sistema centralizado de gestión digital de documentación, basado en las Normas ISO y como referencia el Marco NIST de Ciberseguridad, logra contribuir a mejorar la seguridad, accesibilidad y trazabilidad de la información en la MiPymes de servicios profesionales Seguro Total?

En el capítulo II veremos el marco teórico en el cual se desglosa de manera general mediante el macroentorno, microentorno, entorno específico de la organización, teorías de fundamentación, metodologías desarrolladas, instrumentos temáticos y margen legal aplicable a la investigación.

En el capítulo III se explica la metodología a seguir de la investigación teniendo una preponderancia a un enfoque cualitativo acompañado de un alcance exploratorio y descriptivo. De la misma forma se incluye, un desglose de la población y muestra seleccionada para la investigación, así como también las variables y dimensiones a revisar y validar en la investigación para dar respuesta a nuestros objetivos específicos. De manera importante se incluye también un desglose de los instrumentos a aplicar.

En el capítulo IV se hace referencia a los resultados de la aplicación de los instrumentos metodológicos y temáticos que se explican dentro del capítulo II y III, los cuales son validados frente a los objetivos de la investigación.

En el capítulo V con base a los resultados del capítulo IV se incluyen las recomendaciones y conclusiones para dar respuesta a las preguntas investigadas.

En el capítulo VI encontramos un desglose de la aplicabilidad del proyecto basado en una propuesta de diseño y directrices para la empresa Correduría de Seguros Seguro Total.

1.2 ANTECEDENTES DEL PROBLEMA

El diseño e implementación de sistemas de gestión de documentación ha cobrado gran relevancia en el transcurrir de los años, especialmente para las MiPymes que enfrentan un desafío significativo en la administración de información sensible, cumplimientos normativos y eficiencia operativa.

1.2.1 CONTEXTO GLOBAL

En Indonesia, precisamente en la oficina representativa del banco de Indonesia, reportó el uso de la norma ISO 15489:2016, destacando el claro desafío del manejo, clasificación y preservación documental, proponiendo mecanismos como monitoreo regular y registro de archivos (Ardini, 2021).

El objetivo de esta fue evaluar directrices para la creación y gestión de documentos y registro, considerando el fin de la implementación se dieron una serie de inconvenientes entre ellos, procedimientos básicos o deficiencias de clasificación y control de accesos y preservación de documentos. Con ello se realizó la recomendación de un SGD, que facilita la trazabilidad, control de versiones y políticas de retención y manejo de documentación alineado a la norma 15489.

Existen actualmente herramientas como DocuWare, dicha herramienta es un proveedor global que se basa en proveer sistemas DMS, dicha herramienta fue auditada específicamente bajo la ISO 15489, validado por cumplir con los conceptos y principios de seguridad y fiabilidad de la gestión de documentación (Pichur, 2017).

1.2.2 CONTEXTO REGIONAL

En América latina, o quizás principalmente en Centroamérica y el caribe, la adopción es simplemente limitada, la Comisión Económica para América latina y el Caribe señala que más del 65% de las MiPymes aún gestiona su documentación de manera manual o con soluciones no integradas y alineadas al negocio, contribuyendo a generar pérdidas de información y dificultades para el cumplimiento normativo. Si bien en países como Costa Rica o Panamá están mejor posicionados con la adopción de estas herramientas, muchas Pymes regionales incluyendo Honduras, dependen en su totalidad o en manera predominante de procesos manuales o digitales, pero sin alguna estructura formal o uso de marcos o normas internacionales como base.

En Honduras, se estima que las MiPymes representan entre el 30 y 50 % del PIB y alrededor del 60 % de los empleos formales, lo que las convierte en pilares del desarrollo

económico. Sin embargo, enfrentan serias limitaciones tecnológicas, como acceso a infraestructura, conocimientos digitales y recurso humano capacitado.

En Honduras, su gobierno ha desarrollado la agenda digital honduras 2030 con el fin de acelerar la digitalización en sectores clave como administración pública, educación y salud. (IGB&Company, 2023), uno de los principales retos para las MiPymes es el escaso uso de plataformas tecnológicas para gestión de información administrativa y legal. La mayoría de estas empresas no cuenta con protocolos de respaldo, políticas de acceso ni sistemas centralizados de almacenamiento, lo que afecta directamente su capacidad de operación segura y eficiente. A pesar de los esfuerzos institucionales por impulsar la digitalización, como los programas de fortalecimiento empresarial impulsados por SENPRENDE y el CONADI, todavía persiste una brecha importante entre la disponibilidad de herramientas tecnológicas y su adopción efectiva por parte de las MiPymes hondureñas.

Tabla 1: Resumen Comparativo de Factores Claves de un Sistema de Gestión Documental (SGD)

Nivel	Factores clave
Internacional	Mercado DMS Sumamente adecuado para adopción y con un porcentaje alto en beneficios y reducción de costos.
Regional	Baja utilización en MiPymes, así como factores externos que nublan su adopción.
Nacional	MiPymes impactan PIB y empleo; existen Iniciativas digitales nacionales.

Nota: Elaboración Propia

1.2.3 CONTEXTO DE LAS ORGANIZACIONES

Las organizaciones a las que apoyaremos van directamente ligada a servicios legales y seguros, empresas en donde el manejo de información sensible es vital y sumamente importante tanto para el trabajo a realizar como para el sustento propio del negocio, actualmente las empresas manejan información bajo carpetas físicas o sistemas digitales sumamente limitados y que realmente no tienen seguridad adecuada y que pueden estar dispersos en distintas computadoras sin un centro de control específico.

Actualmente también se cuentan con accesos a plataformas de almacenamiento en la nube como ser Google Drive, Sharepoint o OneDrive para gestión de documentos e información personal sensitiva. Sin embargo, no existe un proceso formal, control o adhesión a buenas prácticas que les ayude a monitorear y gestionar de forma eficiente y segura la información.

1.2.4 BRECHAS DE CONOCIMIENTO

Actualmente no existen modelo de gestión de documentación digital adaptado al contexto hondureño para MiPymes de servicios profesionales, esto quiere decir que hay un margen de aplicación sumamente beneficioso, ya que proveerá un punto de partida para empresas que quieran realizar la adopción, así como una ventaja competitiva sobre otros en el mercado.

Actualmente existen softwares que puedan solventar, pero las limitantes como ser de conocimiento, tiempo disponible de investigación y presupuesto para los encargados de las empresas son algunas de las barreras principales de adopción de este tipo de herramientas.

1.2.5 RELEVANCIA DEL PROBLEMA

Atender esta problemática es crucial por su impacto directo en la eficiencia, competitividad y sostenibilidad de las MiPymes de servicios profesionales en Honduras. La implementación de un sistema digital de gestión documental reduce significativamente el tiempo de búsqueda de información, mejora la trazabilidad de los procesos, y garantiza la protección de datos sensibles frente a riesgos de pérdida o acceso no autorizado (Adobe, 2023).A nivel sectorial, esto ayudará a las organizaciones a elevar los estándares de calidad en prestaciones de servicios profesionales, posicionando a las MiPymes como actores competitivos en un mercado totalmente digitalizado. (DIGER)

1.2.6 DEFINICIÓN DEL PROBLEMA

En el entorno actual de transformación digital, la gestión eficiente de la información se ha convertido en una necesidad sumamente estratégica para las empresas. Las MiPymes del sector a estudiar generan, modifican, procesan y almacenan un volumen elevado de datos que tiene un alto valor añadido, desde el factor legal hasta lo operativo. Sin embargo, bajo el contexto del País (Honduras) estas empresas no cuentan con un sistema capaz de gestionar esa cantidad descomunal de información lo que hace que se vean expuestos a múltiples riesgos entre los cuales puede ser operativo o legal.

Las empresas Hondureñas de este sector brindan sus procesos de manera manual n el mayor de los casos, algunos hasta semi digital pero de una manera muy básica y sumamente riesgosa, esto mismo conlleva a problemas que con alto impacto como ser: Fragmentación, duplicidad o simplemente falta de trazabilidad de la información que se tiene, esto sin mencionar las políticas y uso de la misma, ya que no disponen de acceso controlado, políticas, roles y/o un respaldo monitoreado que brinde esa seguridad en el manejo de la data. Cada uno de estos puntos a considerar son una desventaja notable y no solo en su mercado, sino en su propio crecimiento y evolución como organización.

Diversos estudios regionales (DIGER) (CEPAL, 2023) han visualizado que la baja adopción de DMS o meramente, hacer una transformación digital está estrechamente vinculada a los factores como: Falta de conocimiento, percepción del alto costo, Baja cultura organizacional de procesos digitales, poca oferta de soluciones y pocas capacidades económicas.

A pesar de que, si existen herramientas, no existen propuestas realmente llamativas que guíen casi desde cero a estas pequeñas empresas en su desarrollo y que les permitan visualizar una viabilidad absoluta de su implementación adaptada a su realidad.

Considerando estas problemáticas surge una necesidad crucial y es la de Diseñar un sistema de gestión de documentación orientados a las MiPymes de servicios profesionales en Honduras que cumpla con los criterios buscados como seguridad, accesibilidad y, sobre todo, que este desarrollo permite ofrecer una alternativa práctica y viable que contribuya a mejorar la organización interna y protección de la información.

1.3 PREGUNTAS DE INVESTIGACIÓN

1.3.1 PREGUNTA DE INVESTIGACIÓN GENERAL

¿De qué manera un sistema centralizado de gestión digital de documentación, basado en las Normas ISO y como referencia el Marco NIST de Ciberseguridad, logra contribuir a mejorar la seguridad, accesibilidad y trazabilidad de la información en la MiPymes de servicios profesionales Seguro Total?

1.3.2 PREGUNTAS DE INVESTIGACIÓN ESPECÍFICAS

1. ¿Qué brechas existen en los procesos actuales de la MiPymes de Servicios Profesionales Seguro Total en términos de la gestión documental frente a estándares internacionales como ser la ISO 15489-1:2016, ISO 27001 y el Marco NIST de Ciberseguridad?
2. ¿Qué herramientas actuales en el mercado permiten a la MiPyme Seguro Total tener una estructura eficiente, escalable y accesible para implementar un sistema centralizado de gestión documental basado en la ISO 30301:2019 y temas de seguridad de la ISO 27001 y el Marco NIST de Ciberseguridad?
3. ¿Cómo una arquitectura documental basada en los principios de la ISO 154891:2016 y los requisitos de la ISO 30301:2019, e integrada con controles de seguridad de la ISO 27001 y el Marco NIST de Ciberseguridad, permite desarrollar un sistema seguro y escalable para Seguro Total?
4. ¿De qué manera la integración de funciones y categorías del Marco NIST de Ciberseguridad, en conjunto con los controles de la ISO 27001, puede reforzar la

seguridad y la resiliencia de la información en la MiPyme Seguro Total?

5. ¿Qué oportunidades de mejora, alineadas con el Marco NIST de Ciberseguridad y las normas ISO 15489-1:2016, ISO 30301:2019 e ISO 27001, permitirán a la correduría Seguro Total optimizar sus procesos documentales y alinearse con mejores prácticas internacionales?

1.4 OBJETIVOS DEL PROYECTO

1.4.1 OBJETIVO GENERAL

Diseñar un sistema digital de gestión documental centralizado que garantice la seguridad, accesibilidad y correcto manejo de información privada sensible, con las Normas ISO y como referencia base el Marco NIST de Ciberseguridad que apoye a las MiPymes del rubro servicios profesionales aplicado a la Correduría de Seguro Total**.**

1.4.2 OBJETIVOS ESPECÍFICOS

1. Analizar los procesos actuales de gestión documental en la MiPyme Seguro Total para identificar riesgos y debilidades en el manejo de PII, contrastándolos con los principios de la ISO 15489-1:2016 y ISO 27001 y el Marco NIST de Ciberseguridad.
2. Evaluar herramientas o sistemas existentes que cumplan con los requisitos de las ISO 30301:2019, IS0 27001 y el Marco NIST de Ciberseguridad que permitan a Seguro Total tener un sistema estandarizado, seguro y escalable.
3. Evaluar una arquitectura de gestión documental alineada a los estándares de las ISO 15489-1:2016, ISO 30301:2019 y ISO 27001 y bajo el Marco NIST de Ciberseguridad que sea resiliente, accesible y se integre con la gobernanza empresarial de Seguro Total.
4. Evaluar y recomendar las funciones y categorías del Marco NIST de Ciberseguridad permiten a la MiPyme Seguro Total mejorar sus procesos actuales de gestión documental.
5. Identificar y proponer oportunidades de mejora en los procesos de gestión documental, tomando como referencia los requisitos de la ISO 30301:2019, las guías funcionales de la ISO 15489 y los controles de seguridad de la ISO/IEC 27001.

1.5 JUSTIFICACIÓN

El presente documento contiene una investigación sobre la recopilación, gestión, almacenamiento y seguridad de los documentos y datos relacionados en ellos de los usuarios internos y externos para las MiPymes de servicios profesionales. En este contexto la investigación se realiza un caso de estudio utilizando a la empresa hondureña Seguro Total Correduría de Seguros.

La relevancia de esta investigación dentro de la MiPymes de servicios profesional Seguro Total es por el alto volumen de documentos personales que almacena, utilizan y administran en su día a día de sus operaciones. Por lo tanto, tener un sistema de gestión documental centralizado apoyado de normas internacionales de calidad como ser las ISO y apoyado del Marco NIST de Ciberseguridad, asegura poder ser más eficientes a nivel de consultas, procesos, seguridad y calidad.

Seguro Total no posee en la actualidad una arquitectura robusta de TI y controles de proceso y seguridad para el tratamiento de documentos personales como ser identidades, licencias, formularios, reclamos y cotizaciones. La empresa opera con métodos manuales o semi digitales para almacenar y procesar sus documentos. Igualmente, almacenar copias físicas de la documentación como respaldo. Los métodos digitales utilizados por Seguro Total son Google Drive y la carga de documentos físicos escaneados a los diferentes portales de las aseguradoras. Al no tener un sistema centralizado, su capacidad de respuesta actual se encuentra limitada ante auditorías, clientes y entes reguladores.

La implementación de un Sistema Digital de Gestión Documental (DMS) adaptado a las capacidades y necesidades de esta organización dentro del rubro de servicios profesionales específicamente para las corredurías representa una oportunidad estratégica para optimizar procesos, reducir tiempos administrativos, garantizar la integridad de la información y en futuro cumplir con las leyes que el gobierno hondureño implemente. Además, este tipo de solución documental facilita la adopción de buenas prácticas internacionales como las establecidas en la ISO 154891:2016, ISO 30301:2019 y ISO27001 y el Marco NIST de Ciberseguridad, adaptadas al contexto hondureño.

Desde la perspectiva gubernamental la importancia de esta investigación es ver como marcos y normas internacionales pueden utilizarse como referencia directa frente a la elaboración de una ley de protección de datos y como este diseño de sistema permite establecer guías y estándares para las MiPymes dentro de este rubro que manejan este tipo de información personal sensible. Esto es importante, ya que internacionalmente existen países como ser

Estados Unidos, Alemania, Inglaterra en los cuales el del almacenamiento de documentos con información personal sensible tiene altos niveles de regulación, estándares de seguridad, control de accesos y sanciones en el caso de no cumplir con los puntos mencionados anteriormente.

Desde el punto de vista académico, este estudio contribuye al conocimiento sobre cómo integrar marcos de gestión documental y tecnologías accesibles en MiPymes de servicios profesionales con recursos limitados, generando un modelo replicable para empresas de características similares. En el ámbito profesional, permitirá ofrecer una herramienta práctica que fortalezca la gestión empresarial, centralice la información y disminuya riesgos legales y operativos.

A nivel de la investigación permite a la MiPyme de servicios profesionales Seguro Total estar a la vanguardia dentro del mercado hondureño logrando poder evaluar y posteriormente implementar un sistema digital centralizado de gestión documental que utilice las mejores prácticas disponibles en el mercado y pueda aprovecharlo como una ventaja competitiva para formar alianzas con corredurías regionales, por ejemplo, en Costa Rica y Panamá donde ya existe un base sobre la protección de datos.

En síntesis, la elaboración de esta investigación busca crear un diseño, modelo y guía práctica para que la empresa Seguro Total y las MiPymes del rubro de servicios profesionales en Honduras evolucionen de manera escalable y eficiente hacia un sistema digital de gestión documental moderno y seguro que se alinee a normas ISO y el Marco NIST de Ciberseguridad como estándar. Como un impulsador para la transformación digital la adopción de un sistema digital centralizado para la documentación permite ser más eficientes a nivel operativo, información sea más accesible y facilita que normas o marcos referenciales para tomar como base para una ley de protección de datos. Ante esta situación, surge la siguiente pregunta del problema:

¿Cómo afecta la ausencia de un sistema digital centralizado de gestión documental, alineado a normas ISO 27001, 15489, 30301 y al marco NIST de Ciberseguridad, a la seguridad, accesibilidad y trazabilidad de la información en la MiPyme de servicios profesionales Seguro Total?

CAPÍTULO II MARCO TEÓRICO

2.1 MACROENTORNO (INTERNACIONAL)

2.1.1 EVOLUCIÓN DE LA GESTIÓN DOCUMENTAL.

Desde los inicios de la historia humana la documentación ha sido una pieza vital para almacenar y transferir conocimiento entre las personas. En un inicio la información se transmitía solamente de boca en boca, posteriormente las antiguas civilizaciones utilizaban los jeroglíficos para registrar información de forma permanente como ser en sus templos, estatuas u objetos cotidianos. Aunque esto no es directamente considerado como un documento o más aún como un documento archivístico, estos son los predecesores de la documentación archivística.

Según Maso (2023), hacia el 3200 a.C., en la antigua Mesopotamia surge la escritura como la primera base para la documentación y la archivística actual. Al principio la escritura consistía en dibujos de objetos y figuras, pero con el tiempo evolucionó a un sistema de escritura más técnico de signos conocidos como cuneiformes, el cual es un término que proviene del latín cuneus y hace referencia las incisiones del cálamo en tablillas de arcilla. Mediante este proceso los escribas fueron las piezas claves, al ser los encargados en registrar y transmitir el conocimiento de la escritura en la antigua Mesopotamia.

Encontramos también durante el reinado de Shulgui la tarea de los escribas de transcribir los textos sagrados y conservarlos en tablillas dentro de la Casa de la Sabiduría dedicada a la diosa Nisaba, con el propósito de que nunca se perdieran, lograron ver la primera base del almacenamiento de la documentación. Más adelante, los descubrimientos arqueológicos del siglo XIX evidencian que estas tablillas se agrupaban por temas o por personas, mostrando prácticas tempranas de organización documental asemejando a lo que hoy en día conocemos como una biblioteca, utilizando etiquetas, numeración e incluso el nombre del escriba para facilitar su identificación.

En la Edad Media los monasterios y catedrales fueron los centros principales para la preservación documental los cuales eran utilizados en temas religiosos. Hacia el umbral de la Edad Moderna encontramos la invención de la imprenta por medio de Gutenberg en 1440 el cual fue el apoyo vital para la reproducción y distribución masiva de documentación, reemplazando las copias manuscritas de la información que se venían realizando. Se considera que el primer libro impreso por parte de él fue la Biblia de Gutenberg en 1455(Luzón, 2025).

Según Rendon Rojas (2017), a partir de este momento la archivística comenzó a profesionalizarse, especialmente en las naciones posrevolucionarias en Europa, donde

surgieron las primeras escuelas y servicios enfocados en la preservación documental. Un ejemplo fundamental fue la Escuela de Chartes en París, donde se formaban profesionales y consolidaron técnicas de archivística, destacando figuras como ser Jules Michelet. Encontramos también durante esta etapa tensiones entre los historiadores y archivistas, en donde autores como Langlois y Seignobos defendían que la "la historia se hace mediante documentos", lo que vino a reforzar el papel de archivo o documentación dentro de la investigación.

Dentro de este contexto aparece el Manual Holandés de Müller, Feith y Fruin (1898), considerado como un pilar en el estatus científico de la archivística al delimitar sus métodos y objetivos. En el siglo XX, surgen aportes claves que logran consolidar la disciplina como ser Jekinson que destacó la figura del archivo como el "guardián de la evidencia" y Casanova definió la archivística como una ciencia autónoma.

Finalmente, Rendón Rojas (2017) expone que desde los años ochenta la normalización descriptiva y la preservación de documentos electrónicos impulsaron el crecimiento de la archivística. En este nuevo paradigma que se presenta, la información contenida en los documentos se convierte en el foco central, transformando la figura del archivero en un gestor de información orientada a la transparencia, el acceso y la conservación dentro de contextos organizacionales.

2.1.2 EVOLUCIÓN DE LA GESTIÓN DE LA INFORMACIÓN

La archivística ha experimentado una transformación significativa a lo largo del tiempo, impulsada principalmente por la digitalización y el desarrollo de la computación y las tecnologías de la información desde la década de 1970. Los primeros avances incluyeron programas de procesamiento de texto y sistemas especializados que facilitaron la creación y edición de documentos. Posteriormente, en los años 1980, el uso de los lectores de códigos de barras mejoró la precisión en la identificación y rastreo de registros, mientras que la aparición del CD/CDROM permitió almacenar y distribuir grandes volúmenes de información, optimizando los espacios físicos y facilitando la organización documental.

Con el cambio de siglo, los avances tecnológicos asociados a la cuarta revolución industrial introdujeron herramientas como el correo electrónico y, más tarde, los servicios de almacenamiento en la nube, que consolidaron la gestión documental en entornos digitales. Estas innovaciones habilitaron el intercambio ágil de documentos, la colaboración remota, el control de versiones y la preservación segura de archivos en línea. En conjunto, estos hitos muestran cómo la archivística se ha adaptado a un mundo cada vez más digital, en el que la seguridad y

protección de la información son aspectos esenciales tanto para personas como para organizaciones.

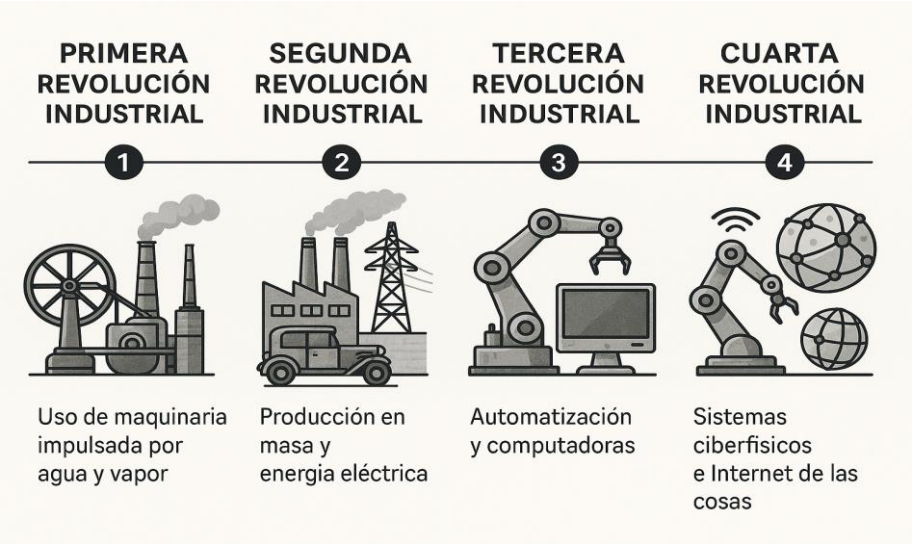
Figura 1: Evolución de la Archivística

Nota: Elaborada por los autores

2.1.3 TRANSFORMACIÓN DIGITAL EN LATINOAMÉRICA

Hablar de una transformación digital no puede ser posible sin mencionar la cuarta revolución industrial, la cual precisa el autor (Schwab, 2020) que la cuarta revolución industrial es aquella donde se conecta el mundo físico, digital y biológico impulsado por tecnologías emergentes que precisan ayudar en las actividades. Por ende, la transformación digital no puede ser entendible sin la cuarta revolución industrial y su impacto en la sociedad.

Figura 2: Cronología de la Transformación Digital



Nota: European Commission (2020)

2.1.3.1 IMPLICACIÓN DE LA TRANSFORMACIÓN DIGITAL

La transformación digital implica la integración de tecnologías digitales en todos los aspectos de la organización y de la vida cotidiana. De acuerdo Páez (2022) se trata de la incorporación de herramientas digitales en los procesos de funcionamiento y en la manera de relacionarse con el entorno humano.

En términos prácticos, esta transformación supone la digitalización de actividades y procesos que antes se realizaban en formatos analógicos. Gómez y Caro (2022) lo definen de forma precisa:

> "La digitalización es la conversión de datos y procesos analógicos en un formato legible por máquina. La digitalización es el uso de tecnologías y datos digitales, así como la interconexión que da lugar a actividades nuevas o a cambios en las existentes."

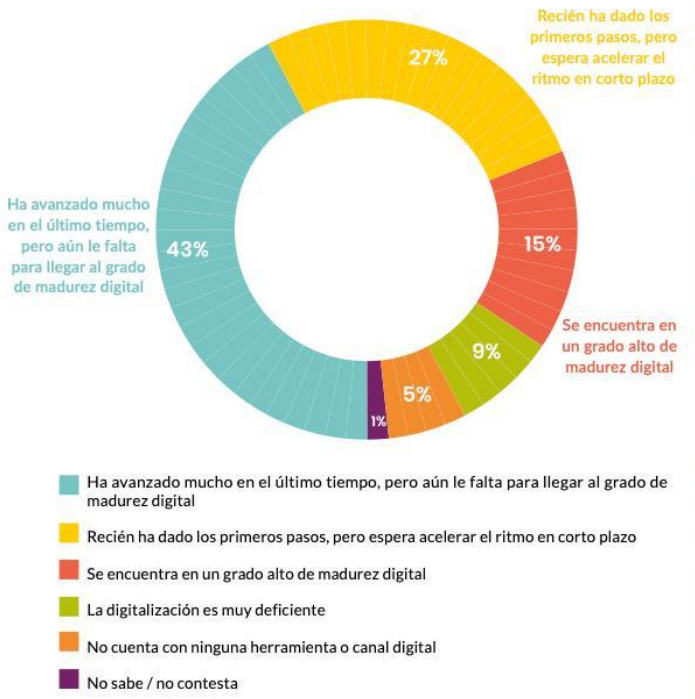
En el contexto latinoamericano estas implicaciones adquieren una dimensión estratégica, solo las MiPymes representan más del 90% del tejido empresarial de la región, enfrentan el doble desafío de mantenerse competitivas y adaptarse a un entorno mucho más digital en constante cambio. Considerando este factor, la transformación digital no solo es un proceso tecnológico, sino cultural y organizacional que exige innovación, formación de capacidades digitales y políticas o cumplimiento capaces de cerrar brechas tecnológicas.

2.1.3.2 BRECHAS Y PANORAMA GENERAL DE TRANSFORMACIÓN DIGITAL EN AMÉRICA LATINA

En América Latina, la transformación digital se perfila como una oportunidad de crecimiento económico y de mejora en la competitividad regional. Su potencial es enorme, aunque aún enfrenta desafíos estructurales que dificultan una adopción plena y homogénea. El sector manufacturero ha marcado el paso, con países como Brasil, Argentina y México incorporando de forma acelerada tecnologías como la robótica y el Internet de las Cosas (IOT) para optimizar la calidad de producción, reducir tiempos de inactividad y mejorar la eficiencia operativa. Este dinamismo ha impulsado el valor del mercado de transformación digital, que pasó de 88.26 mil millones de dólares a 107.23 mil millones en 2025 y que proyecta alcanzar los 242 mil millones para 2030 (Mordor intelligence, 2023). La federación internacional de robótica destaca que Brasil concentra un 47% de robots en la industria automotriz y un 22% en instalaciones recientes, cifras que reflejan la expansión de estas tecnologías en la región, donde actualmente la adopción representa alrededor del 10% del total mundial.

Por otra parte, las micro, pequeñas y medianas empresas (MiPymes), que generan cerca del 60% del empleo formal y representan una base crucial del tejido productivo, avanzan de manera desigual de su digitalización. De acuerdo con la Secretaría General Iberoamericana (SEGIB, 2023), un 86% se encuentra en alguna fase de este proceso, aunque con grandes brechas en términos de madurez digital, la capacitación de empleados y aprovechamiento estratégico de herramientas. La pandemia de COVID19 aceleró la transformación, con un 86% de MiPymes adoptando tecnologías digitales básicas, desde la facturación electrónica hasta el comercio en línea, y un 39% reconociendo que la digitalización fue decisiva para su supervivencia. Sin embargo, persisten importantes desigualdades: Según CEPAL (2023), muchas empresas todavía utilizan internet de manera pasiva y muestra resistencia a invertir en tecnologías emergentes lo que agrava la brecha digital, especialmente entre hogares urbanos, con un 77% de conectividad, y rurales, con apenas un 38%. Esta realidad confirma que la digitalización no es solo un factor de modernización, sino una condición necesaria para la sostenibilidad y competitividad de las economías latinoamericanas.

Gráfico 1: Nivel de digitalización de MiPymes en Latinoamérica



Nota: Información obtenida de (SEGIB, 2023)

Tabla 2: Nivel de Digitalización en Latinoamérica

País	Nivel de digitalización de PYMES	Políticas de apoyo	Observaciones clave
Colombia	Medio Alto	Sí	Programas como "Colombia a un Clic" y "Vende en Línea" impulsan la digitalización.
México	Medio	Parcial	Iniciativas en marcha, pero con desafíos en infraestructura y capacitación.
Perú	Medio	Parcial	Progresos en sectores específicos, pero falta de políticas integradas.
Argentina	Medio Bajo	Parcial	Avances limitados y falta de estrategias nacionales coherentes.
Brasil	Medio Bajo	Parcial	Desigualdades regionales y necesidad de políticas más coordinadas.
Ecuador	Bajo	Parcial	Brechas significativas en acceso y uso de tecnologías digitales.
Bolivia	Bajo	Limitado	Infraestructura deficiente y escaso apoyo gubernamental.
Venezuela	Muy Bajo	Limitado	Conectividad limitada y falta de políticas de apoyo efectivas.
Chile	Alto	Sí	Lidera en transformación digital, con estrategias nacionales integradas.
Uruguay	Alto	Sí	Avances significativos en conectividad y habilidades digitales.
Paraguay	Medio Alto	Sí	Implementación de políticas efectivas para apoyar la digitalización.

Nota: Información obtenida de (Pozo Benites, 2025).

2.1.3.3 IMPACTO DE LA DIGITALIZACIÓN EN LAS MIPYMES

El proceso de transformación digital en las pequeñas y medianas empresas ha demostrado tener un impacto directo y significativo en el fortalecimiento de su desempeño económico.

Según Pozo Benites (2025) la adopción de tecnologías digitales mejora sustancialmente la eficiencia operativa, incrementa la productividad, potencia las ventas y facilita el acceso a nuevos mercados. Estas mejoras no solo elevan la competitividad de las empresas, sino que también les permiten adaptarse con mayor resiliencia a contextos de crisis e incertidumbre económica.

Según la OCDE (2023), las MiPymes han incorporado herramientas como:

- Aumento promedio del 20% en sus ingresos gracias a la expansión de canales de venta en línea.
- Reducción del 15% en costos administrativos mediante uso de sistema de gestión de documentos.

- Mejora del 25% de velocidad en respuesta de los clientes.

CEPAL (2023) menciona que la digitalización no solo ayuda con la productividad, sino que contribuye a la formalización de la empresa integrando herramientas como la facturación digital, sistema de pagos electrónicos y PO's así, como una gran trazabilidad digital documental.

El Banco interamericano de desarrollo (BID, 2023) realizó un estudio donde las MiPymes digitales destacan en la región ya que adoptaron en base a sus necesidades soluciones tecnológicas capaces de fomentar y mejorar automatizaciones operativas, de igual manera, esto resalta ya que tienden a generar mayor inclusión financiera y a si proveer al cliente una serie de ventajas como créditos, seguros o financiamiento externo.

Según el World Bank (2021) para las MiPymes orientadas a servicios profesionales, la digitalización destaca en áreas clave como:

- Gestión documental: reducción de pérdidas de información sensible y mayor cumplimiento regulatorio.
- Acceso a una cartera de clientes mayor: logran acceder a mayor clientela llegando a lo internacional gracias a sus plataformas virtuales y su asesoría digital.
- Reducción de costos y riesgo operativo: Con la automatización de procesos se minimiza errores humanos y mejora gradualmente la trazabilidad.

Tabla 3: Beneficios de la Digitalización

Beneficio de la Digitalización	Impacto en MiPymes
Mayor eficiencia operativa	Automatización de procesos, reducción de costos administrativos (OECD, 2023)
Incremento de productividad e ingresos	Expansión de canales digitales que aumentan ventas (OECD, 2023).
Mejora en atención y fidelización	Atención al cliente más rápida vía plataformas digitales (OECD, 2023).
Formalización y control documental	Integración de herramientas tributarias/digitales que mejoran cumplimiento y trazabilidad (CEPAL, 2023).
Resiliencia frente a crisis	Mayor capacidad de mantener operaciones y ventas durante crisis (BID, 2024).
Inclusión financiera	Acceso a crédito, seguros y servicios financieros vía plataformas digitales (World Bank, 2021).

Nota: Elaborado por los autores

2.1.4 COMPETENCIAS Y MERCADO REGIONAL

Actualmente el mercado está siendo feroz e impulsado en los países con mayor adopción por la digitalización y todo lo que engloba la cuarta revolución industrial. En América latina la industria de seguros ha comenzado a digitalizarse de una manera avanzada impulsándose por el crecimiento de la Insurtech.

2.1.4.1¿QUÉ ES INSURTECH?

Según Investopedia, "Insurtech se refiere al uso de innovaciones tecnológicas diseñadas para generar ahorros y eficiencia en el modelo actual de la industria aseguradora. "Entre sus características más importantes tiene el uso de análisis de datos, IA, IoT, BlockChain y aprendizaje automático para modernizar funciones.

Insurtech tiene como misión mejorar la experiencia del cliente al aprovechar el máximo de la tecnología, el cliente podrá tener mayor impacto en su uso del seguro ampliando cobertura y selección del más conveniente acorde a sus necesidades, con eso se promueve la eficiencia operativa brindando una solución práctica y accesible al cliente y usuario en cualquier momento. Insurtech gestiona mayormente áreas como: Reclamaciones, suscripciones, ejecución del contrato y mitigación de riesgos. Con esto busca reducir problemas operativos o malas experiencias de los clientes.

Según MAPFRE Economics (2024), América latina cuenta con más de 500 Insurtech, de las cuales 206 se encuentran localizadas en Brasil, con esto se posiciona como el principal hub regional de innovación en seguros. Para América latina se prevé según MAPFRE Economics (2024), que el crecimiento sea de un 1.6%, sin embargo, depende grandemente de factores económicos con Estados Unidos y su aumento podría llegar hasta un 8.6% en 2025.

2.1.5 PAÍSES LÍDERES EN INNOVACIÓN

2.1.5.1CHILE

Tiene un total de 29 Insurtech y 3 startups, orientadas a la distribución digital, servicios para aseguradoras e intermediarios, así como, nuevos modelos de negocio. (Cardona Giraldo et al.,2023). Alguna empresa emergente de chile se orienta más específicamente a temáticas como ser:

- Prospección de clientes
- Suscripción
- Comercialización
- Emisión
- Cobros

- Servicio al cliente
- Fidelización

2.1.5.2 BRASIL

Forma gran parte de las Insurtech de la región, alcanzando un 37% de participación en la región incluyendo propuestas de valor innovadoras y dirigidas al desarrollo comercial de bróker de seguros o nichos específicos de mercado como ser: seguros por telefonía móvil, canales de distribución y venta digital (Cardona Giraldo et al.,2023).

De acuerdo con ThreePoints Informe Insurtech: "El principal problema de las startups brasileñas es que no tienen trascendencia más allá de sus fronteras. Analizando el ecosistema Insurtech de Brasil, nos encontramos con que el 6% de sus empresas buscan desafiar los modelos de negocio tradicionales, con innovaciones como el modelo "pay when you drive" o modelos "peer to peer Insurance".

2.1.5.3 COLOMBIA

La federación de aseguradores colombianos (FASECOLDA) organizó el seminario Insurtech Colombia 2021, donde se enfatizó la necesidad de que las aseguradoras e Insurtech converjan en modelos de colaboración para mejorar la sostenibilidad y competitividad del sector. Así mismo la compañía Sura proyecta convertirse en la principal Insurtech latinoamericana para 2025, con un portafolio de productos en sectores emergentes como energías renovables, agro y nuevas soluciones de movilidad, alcanzando 2.6 millones de clientes (Calderón et al., 2021).

Tabla 4: Ejemplos de Insurtech en Colombia

Insurtech	Propuesta de valor	Tipo de Innovación
Wesura	Servicios personalizados 100% online	Seguros digitales a demanda
Sekure	Integración de seguros y asistencia digital	Plataformas integradas B2B y B2C
Seguro canguro	Permite adquirir seguros de vehículo acorde al uso y necesidad	Modelo flexible de seguros
QueSeguro	Protección de planes EPS de forma digital	Salud digital
Finesa	Especializada en créditos y pólizas de vehículos	Insutech Híbrida
Soft Seguros	Gestión digital de pólizas, siniestros y renovaciones	Automatización de procesos

Nota: (Calderón et al., 2021) (*suramericana Lanza Insurtech Para Que Filiales Seguros SURA Avancen En Mercado Digital Grupo SURA*, 2022).

2.1.5.4 MÉXICO

En la actualidad se están creando nuevos modelos de negocio, acompañados de Aseguradoras y reaseguradores, tomando una parte del riesgo desde la creación de nuevos productos asumiendo parte de los riesgos. Por su parte los reaseguros se llevan a cabo por medio de ciclos y capacidad catastrófica de los riesgos a nivel general, las Insurtech buscan desarrollar estrategias a largo plazo y no influenciada por los ciclos de riesgo, de la mano de la transformación digital por medio de inversión estratégica. (Cardona Giraldo, Fajardo Sánchez, Yepes Molina, & Viasus, 2023)

Actualmente gracias a las múltiples habilidades de innovación que han adquirido las Fintech, se han podido expandir la aplicación de las nuevas tecnologías digitales en un gran aumento de los nuevos modelos de negocio que han surgido en México, generando un cambio en el sistema financiero tradicional.

2.1.6 RIESGOS DE REZAGO DE FINTECH FRENTE ASEGURADAS DIGITALIZADAS

El rotundo crecimiento de las Fintech y Insurtech en América latina ha transformado de manera profunda el mercado financiero y asegurador. Dichas compañías tienen múltiples ventajas como modelos digitales ya nativos, productos más ágiles, personalizados y económicos lo que realmente es una amenaza para las MiPymes que están incursionando en ese mercado.

De acuerdo con CEPAL (2023) más del 40% de consumidores digitales de la región prefieren servicios de seguros mediante Fintech o Insurtech. Esto es una clara desventaja hacia las corredurías tradicionales ya que su mercado se ve disminuido drásticamente por los nuevos startups.

Las pequeñas corredurías deben adoptar herramientas digitales, ya que según Deloitte (2023) podrían perder hasta un 30% de la participación en el mercado en los próximos años, siendo desplazado por aseguradoras que presentan digitalización madura como un sistema de gestión documental, firma electrónica o analítica avanzada. Como se muestra en la tabla 14 los riesgos que puedan asumir.

Tabla 5: Riesgos de Aseguradoras Tradicionales frente a las Fintech

País	Innovación	Ventaja competitiva	Riesgo para MiPymes
Nubank (Brasil)	Banca 100% digital con servicios de seguros de vida, tarjetas hasta accidentes vehiculares.	Más de 80 millones de usuarios, experiencia sencilla y precios de sus productos accesibles.	Las corredurías pierden una gran parte del mercado porque el seguro se ofrece desde la aplicación

País	Innovación	Ventaja competitiva	Riesgo para MiPymes
			bancaria.
Mercado Pago (México, Argentina)	Micro seguros de vida, robo o salud.	Base de usuarios de comercio electrónico muy amplia y facilidades de pago mediante móvil.	Los seguros son servicios complementarios.
Sura (Colombia)	Nueva estrategia para 2025, ampliar mercado de seguros a turismo, jugadores de videojuegos competitivos o energías renovables.	Proyección e innovación continua, alcance de más de 2.6 millones de usuarios.	Elevar el estándar de innovación, dificultando a las MiPymes que no se digitalizan.
Betterfly (Chile)	Seguros de vida orientados a la salud.	Modelo que conecta con la salud generando una fuerte atracción a personas de una edad avanzada.	Riesgo en empresas que no igualen dichos beneficios.
Insurtech Locales (Colombia, Chile, Brasil, México)	Seguros flexibles y a demanda del usuario.	Adaptación rápida a cualquier necesidad que tenga un usuario.	Innovación flexible en contra de procesos rígidos de las corredurías tradicionales.
Aseguradoras internacionales Digitalizadas	Uso de SDG, firma electrónica, big data y análisis de datos preventivos.	Procesos rápidos y seguros.	MiPymes quedan en desventaja por operar bajo formatos manuales.

Nota: Información obtenida de (CEPAL, 2023) (Cardona Giraldo, Fajardo Sánchez, Yepes Molina, & Viasus, 2023) (MAPFRE Economics, 2024.

2.1.7 SISTEMAS DE GESTIÓN DOCUMENTAL (SGD)

2.1.7.1 DEFINICIÓN Y COMPONENTES BÁSICOS DE UN SGD.

Un DMS (Document Management System) por sus siglas en inglés o SGD (Sistema de Gestión Documental) se define como el uso de un sistema de computación y software para almacenar, administrar y acceder a documentos e imágenes que provienen de documentos físicos que han sido capturados mediante diferentes tecnologías como ser escáneres, teléfonos u otros dispositivos (Aiim, 2025.).

La base de todo SGD es un documento que se define en la publicación web de la AIIM (International Organization for Standarization) referenciando a la norma ISO 12651 se define como “información u objeto registrado que puede tratarse como una unidad” (Aiim, s.f.).

2.1.7.2 FUNCIONES CLAVES, BENEFICIOS Y DESAFÍOS DE LA IMPLEMENTACIÓN DE UN SDG

Las funciones claves de este tipo de sistema son las siguientes:

Tabla 6: Funciones Clave de un Sistema de Gestión Documental

Funciones Clave de un Sistema de Gestión Documental	
Función	**Explicación**
Almacenamiento y organización	Ofrece una solución de almacenamiento centralizada y organizada para los documentos. Facilita de la misma forma conceder permisos de visualización y de edición a los usuarios correspondientes.
Accesibilidad y Recuperación	Asegura acceder de forma rápida y sencilla a los documentos. Permitiendo recuperar versiones anteriores de documentos para consultas o seguimientos.
Seguridad y Permisos	Ofrece opciones de cifrado y protección de los documentos mediante diferentes técnicas de seguridad.
Control y seguimiento	Permite gestionar y rastrear fácilmente cambios que se realicen en los documentos.
Colaboración y gestión de flujos de trabajo	Facilita la gestión y colaboración de documentos entre diferentes miembros de la organización.
Automatización de Procesos y aprobación de documentos	Facilita establecer procesos de verificación y aprobación automática de documentos, reducción errores y cuellos de botella en los procesos de la organización.
Uso de Metadatos	La utilización de metadatos de indexación facilita la categorización y la búsqueda de documentos.
Integración con otros sistemas	Permite integrarse con otros sistemas que utilice una organización para asegurar un flujo fluido de la información y mantener la información actualizada en todos los sistemas que interactúan en la arquitectura empresarial de la organización.

Nota: Información obtenida de (Papertrail, 2024)

Tabla 7: Beneficios de un Sistema de Gestión Documental

Beneficios de un Sistema de Gestión Documental	
Beneficio	**Explicación**
Protección de los datos	Almacenamiento mediante controles de seguridad alrededor del ciclo de vida del documento.
Organización de contenido	Centralización de documentos mediante un SGD.
Accesibilidad simplificada	Facilita el acceso a la información y toma de decisiones más rápida e informada con base en documentos actualizados.
Mayor usabilidad	Facilitar el día a día de los usuarios o clientes mediante el uso de SGD.
Colaboración mejorada	Facilita el traslado de conocimiento entre equipos y el acceso a la versión más actualizada de un documento.
Cumplimiento Normativo	Los SGD permiten llevar control de todo el versionamiento de un documento lo que permite a las organizaciones mantener actualizada su información para temas normativos y auditorías.
Mayor Productividad	Mediante la centralización de los documentos los usuarios son más eficientes buscando información.

Nota: Información obtenida de (*Software De Gestión De Contenido Empresarial | Hyland* (2025) y (Udoagwu, 2025)

Tabla 8: Desafíos de la utilización de un Sistema de Gestión Documental

Desafíos de la utilización de un Sistema de Gestión Documental	
Desafíos	**Explicación**
Errores de Identificación	Se debe mantener presente en la configuración del sistema la existencia de políticas y normativas para asegurar la correcta identificación y protección de documentos confidenciales y con información sensible de la organización como de los clientes.
Tipos de documentos dinámicos	Mediante la evolución de los medios digitales al configurar un SGD se debe tener presente que el sistema es compatible para almacenar los diferentes tipos de documentos que gestiona la organización.
Seguridad	Ante el rápido crecimiento de los

Desafíos de la utilización de un Sistema de Gestión Documental	
Desafíos	**Explicación**
	ciberataques hoy en día la implementación de un SGD se debe adherir a las mejores prácticas y controles de seguridad para asegurar la protección de los datos.
Gestión del cambio	La introducción de un SGD a una organización está sujeta a la capacitación del personal humano de la organización para asegurar una adopción eficiente de la herramienta y reducir o evitar la resistencia al cambio.
Costos	Muchas veces las organizaciones no disponen del capital suficiente para adquirir un SGD que tenga todas las medidas de seguridad y se adapte realmente a las necesidades de la organización.
Cumplimiento Normativo	En algunos países el uso de SGD es fundamental para cumplir con normativas legales y así evitar sanciones y asegurar la protección de la información.
Integración con otros Sistemas	Se debe buscar asegurar que el SGD seleccionado sea compatible con otras herramientas que utiliza la organización como ser ERPs, CRMs entre otros para mantener una arquitectura empresarial de TI sostenible y eficiente.
Escalabilidad	El SGD debe ser capaz de crecer de la mano con el crecimiento de la organización con base al espacio de almacenamiento y consulta de un mayor volumen de documentos.
Dependencia de archivos físicos	Muchas organizaciones hoy en día sin importar su tamaño dependen aún de la gestión manual y física de documentos, lo que dificulta el control y acceso a la información.
Digitalización de documentos	La tarea de digitalizar los documentos existentes en la organización para cargar en el SGD es una tarea compleja y larga que puede llegar a desmotivar a los equipos.

Nota: Información de (Udoagwu, 2025).

2.1.7.3 TIPOS DE SGD: EN LA NUBE, ON-PREMISE, HÍBRIDOS.

Actualmente se distingue los diferentes tipos de SGD:

Tabla 9: Tipos de Sistemas de Gestión Documental

Tipo	Definición	Ventajas	Desventajas	Ejemplos
On premises (local)	Instalado en servidores propios.	Control total; datos en modo local; alta personalización.	CAPEX alto; requiere TI interna; actualizaciones más lentas; seguridad es responsabilidad de la organización.	OpenText Content Suite; Hyland OnBase (on-prem); Alfresco (on-prem)
Cloud / SaaS	Servicio en la nube del proveedor.	Despliegue rápido; OPEX; escalable; actualizaciones automáticas.	Menos control; dependencia del proveedor; límites de personalización.	DocuWare Cloud; Laserfiche Cloud; Box; M-Files Cloud
Híbrido	Combinación de local y nube.	Flexibilidad; datos sensibles locales y colaboración en nube.	Arquitectura y gobierno más complejos; integración adicional.	SharePoint Server + SharePoint/OneDrive; OnBase híbrido

Nota: Elaborado por los autores

2.1.7.4 TIPOS DE SGD POR TIPO Y ALCANCE

De la misma forma se distinguen a nivel de alcance funcional los diferentes tipos de SGD:

Tabla 10: Desglose de Sistemas de Gestión por Tipo y Alcance

Tipo	¿Cómo aporta valor a la organización?	Casos típicos	Ejemplos típicos
SGD básico	Repositorio, control de versiones, búsquedas y permisos.	Oficina general, Pyme, backoffice.	DocuWare; eFileCabinet; LogicalDOC
ECM (Gestión de Contenido Empresarial) / CSP (Plataforma de Contenidos)	DMS y flujos de trabajo, taxonomías, APIs e inteligencia y analítica.	Corporativo, múltiples áreas, integraciones ERP/CRM.	OpenText; Hyland OnBase; Nuxeo; M-Files
EDRMS (Sistema Electrónico e Gestión de Documentos y Registros)	Gestión de retención, disposición y auditoría de registros.	Sector público; industrias reguladas (finanzas, salud).	Micro Focus Content Manager; OpenText Records; Alfresco Governance Services

Tipo	¿Cómo aporta valor a la organización?	Casos típicos	Ejemplos típicos
Gestión de casos/expedientes	DMS orientado a trámites/casos.	Gobierno, legal, seguros, atención ciudadana.	Laserfiche; OnBase Case Management; Pega (con DMS)
CLM (Gestión de Ciclo de Vida de Contratos)	Ciclo de vida de contratos, plantillas, cláusulas y firma.	Legal, compras, ventas B2B.	Icertis; DocuSign CLM; Agiloft
Control documental (Calidad/ISO)	Aprobaciones, vigencias y distribución controlada (solo lectura).	Manufactura, farmacéutica, HSE, ISO 9001/GMP.	MasterControl; Veeva QMS Docs; OpenText QMS
Colaborativo/ofimático	Edición simultánea, compartición y comentarios en línea.	Trabajo del conocimiento, remoto e híbrido.	Microsoft 365 (SharePoint/OneDrive); Google Workspace (Drive)
DAM (Gestión de Activos Digitales)	Gestión de imágenes, video y activos de marca.	Marketing, ecommerce, branding.	Bynder; Adobe AEM Assets; Widen

Nota: Elaboración por los autores

Tabla 11: Desglose de Sistemas de Gestión por Categoría y Proveedor

Categoría	Subcategoría	Proveedores/Productos representativos	Despliegue
ECM / CSP	Contenidos	OpenText Content Suite, IBM FileNet, Hyland OnBase	Cloud / On-prem / Híbrido
EDRMS	Registros	OpenText RM, Microsoft Purview, Google Vault	Cloud / On-prem
Colaborativo	Suite ofimática	Microsoft 365, Google Workspace	Cloud / Híbrido
Colaborativo	Contenido empresarial	Box, Dropbox, Egnyte	Cloud
Casos/Expedientes	Case management	OnBase CM, Pega + DMS	Cloud / On-prem
CLM	Contratos	Icertis, DocuSign,	Cloud / On-prem

Categoría	Subcategoría	Proveedores/Productos representativos	Despliegue
		Agiloft	
Calidad/Regulados	Control documental	MasterControl, Veeva Vault, OT QMS	Cloud / On-prem
DAM	Activos digitales	Bynder, Adobe AEM Assets, Canto	Cloud / On-prem
Legal	DMS jurídico	iManage, NetDocuments, OT eDOCS	Cloud / On-prem
Open Source	Repositorio documental	Alfresco, OpenKM, LogicalDOC	Cloud / On-prem

Nota: Elaboración por los autores

2.1.7.5 IMPORTANCIA EN EMPRESAS DE SERVICIOS PROFESIONALES (SEGUROS, CONTABLES, LEGALES).

En las MiPymes de servicios profesionales, el problema no es solamente almacenar y gestionar documentos, encontramos que las MiPymes de este rubro buscan acceder de manera rápida y sencilla a los documentos, controlar versiones, llevar control de aprobaciones y proteger información sensible de la organización como de los clientes debido al alto volumen de documentación que utilizan.

Un SGD permite a las MiPymes de este rubro almacenar documentos en un repositorio único con metadatos útiles (cliente, servicio, estado, responsable, vigencias) y reglas claras de consulta y de acceso. Los efectos principales que resultan del uso de un SGD son menos reprocesos, más trazabilidad y olvidarnos de solo mantener copias físicas de los documentos, eliminar silos de información y mejorar la colaboración. (Docunecta, 2019).

Aplicado directamente al rubro de corredurías de seguros encontramos que un el SGD se vuelve el sistema principal de almacenamiento y consulta de documentos como ser cotizaciones, identificaciones, registros tributarios, pólizas, endosos, carnés, recibos, evidencias mediante imágenes, seguimiento de siniestros, entre otros. El uso de SGD facilita organizar y centralizar la información por aseguradora, tipo de seguro y por tipo de cliente.

En la economía actual del conocimiento y de la información, los documentos dejan de ser solo archivos y se convierten en activos estratégicos en donde se concentran los procesos,

decisiones, contratos, evidencias de la organización, habilitando la toma de decisiones oportuna mediante información actualizada, apoyando al cumplimiento regulatorio y reduciendo riesgos operativos.

La correcta gestión mediante el uso de un SGD, por ejemplo, utilizando, el control de versiones, gobierno del ciclo de vida, seguridad y trazabilidad los documentos aceleran el trabajo y generan una ventaja competitiva al aportar a la obtención de los objetivos estratégicos de la organización, facilitando aprender de cada caso, reutilizar lo ya resuelto, Responder más rápido a clientes y auditorías, y transformar información en valor tangible lo que puede llegar a traducirse en mayores ventas y fidelización de los clientes.

Para las MiPymes de servicios profesionales y en particular una correduría esto se logra traducir en expedientes completos y más confiables, renovaciones a tiempo, siniestros mejor documentados y decisiones basadas en evidencias concretas, olvidándonos de tomar decisiones basadas en suposiciones o la intuición.

En síntesis, para MiPymes de servicios profesionales y particularmente para una correduría un SGD profesionaliza la gestión de la información mediante el orden, consultas rápidas, protección y versionamiento. Logrando evolucionar de sol archivar por si acaso a gestionar el documento como un activo que promueve el crecimiento del negocio. Con ello, se reduce el retrabajo, mejora la experiencia del cliente y se da un salto importante en cumplimiento y ciberseguridad, que hoy es condición básica para competir y crecer.

2.1.8 SEGURIDAD Y ACCESIBILIDAD EN LOS SGD

2.1.8.1 PRINCIPIOS DE LA SEGURIDAD DE LA INFORMACIÓN (CONFIDENCIALIDAD, INTEGRIDAD, DISPONIBILIDAD – CIA TRIAD).

Como base de toda implementación de un sistema tecnológico hoy en día, la ciberseguridad ha cobrado mayor importancia por la protección de la información. Según la definición de la empresa IBM se define como todas aquellas tecnologías, prácticas y políticas que previenen los ciberataques o mitigan el impacto en las organizaciones o en las personas.

"La ciberseguridad tiene como objetivo proteger los sistemas informáticos, las aplicaciones, los dispositivos, los datos, los activos financieros y las personas contra él ransomware y otros malware, las estafas de phishing, el robo de datos y otras ciberamenazas(Ibm, 2024)."

Según el informe Global sobre Amenazas 2025 de Crowdstrike (Crodwstrike, 2025) menciona los siguientes puntos principales sobre los ataques cibernéticos o amenazas que existen hoy en día:

- El tiempo de propagación promedio de la ciberdelincuencia desde encontrar un host vulnerable hasta realizar todo el proceso del ciberataque se redujo a 48 minutos en el 2024, encontrando el más rápido de 51 segundos.
- Los métodos de ataque están evolucionando y mostrando que existen aún muchas vulnerabilidades y los usuarios están fallando en seguir medidas de protección.
- Se observó un aumento del 35% de las campañas de intrusiones interactivas.
- Los atacantes recurren ahora al uso de tecnologías emergentes como ser la IA generativa para refinar la ingeniería social, ser más rápidos en términos de campañas de desinformación y respaldar actividad maliciosa en la red.
- Ataques directamente ligados a china van en aumento, estos aumentaron en un 150% afectando sectores como ser los financieros, medios de comunicación, producción industrial e ingeniería.
- Los entornos en la nube se encuentran ante un mayor asedio debido al alto volumen de datos que almacenan y errores de configuración que los usuarios realizan al momento de su implementación o mantenimiento, por lo cual el reporte menciona un aumento del 26 % de las intrusiones de la nube

Es por esto por lo que los términos base de la CID o CIA según define Fortinet que son confidencialidad, integridad y disponibilidad de los sistemas cobra importancia.

Cada uno de estos se define de la siguiente manera:

Tabla 12: Desglose de Componente de la CID/CIA

Componente	Definición
Confidencialidad	Implica todos aquellos esfuerzos de una organización por mantener sus datos resguardados y privados.
Integridad	Garantizar en todo momento que los datos sean únicos, fiables, precisos y no tengan manipulaciones por parte de los usuarios.
Disponibilidad	Significa mantener todos los sistemas, redes y aplicaciones de la arquitectura empresarial accesible y disponibles en el momento que los usuarios desean acceder a ellos, sin altos tiempos de espera.

Nota: Información obtenida de (*¿What Is the CIA Triad and Why Is It Important? | Fortinet*,2025.)

2.1.9 TRANSFORMACIÓN DIGITAL EN LAS MIPYMES

2.1.9.1 RELEVANCIA DE LA TRANSFORMACIÓN DIGITAL PARA LA COMPETITIVIDAD

La transformación digital según IBM se define como “es una iniciativa estratégica que incorpora la tecnología digital en todas las áreas de una organización. Evalúa y moderniza los procesos, productos, operaciones y pila tecnológica de una organización para permitir una innovación continua, rápida y orientada al cliente.” (O’Brien, Downie, & Scapicchio, 2024).

Se distinguen a nivel general las siguientes tecnologías que aportan a la transformación digital de las organizaciones:

Tabla 13: Tecnologías Promotoras de la Transformación Digital

Tecnología	**Definición**	**¿Para qué sirve en la transformación digital?**
Computación en la nube (Cloud / Híbrida)	Uso de recursos de TI bajo demanda mediante el uso de IaaS, PaaS o SaaS (pública, privada o híbrida).	Escalar rápido, pagar por uso, acceder a servicios avanzados y modernizar aplicaciones.
Tecnología móvil	Apps y servicios en smartphones/tabletas.	Nuevos modelos (tickets/carteras móviles), experiencia cliente 24/7 y fuerza de campo conectada.
Internet de las cosas (IoT)	Dispositivos con sensores que envían datos en tiempo real.	Conectar operación física con analítica/IA para automatizar y decidir mejor.
Inteligencia artificial (IA) y ML	Sistemas que aprenden de datos y automatizan tareas cognitivas. Esta tecnología se encuentra en constante crecimiento y aprendizaje para ofrecer mejores respuestas a los usuarios.	Personalización, asistencia (chatbots), análisis avanzado y eficiencia.
Automatización (RPA)	Bots que ejecutan pasos repetitivos definidos por un usuario.	Reducir reprocesos, acelerar backoffice y liberar al equipo para tareas de mayor valor.

Tecnología	Definición	¿Para qué sirve en la transformación digital?
DevOps / DevSecOps	Prácticas para integrar desarrollo, operaciones y seguridad de forma continua asegurando softwares y desarrollos de mayor calidad y orientados a los usuarios.	Entrega rápida de software seguro; base para innovar con agilidad.
Digitalización	Convertir documentos físicos a datos/archivos digitales.	Fundamento para procesos electrónicos, acceso y trazabilidad.
Blockchain	Registro distribuido e inmutable de transacciones.	Trazabilidad y confianza en cadenas de suministro/finanzas.
Ecosistemas (APIs / Integraciones)	Conexión entre aplicaciones y sistemas para ofrecer más valor teniendo una arquitectura interconectada.	Extender servicios, single sign-on, Marketplace y co-innovación.
Gemelos digitales	Réplicas virtuales de procesos/productos/entornos para realizar pruebas para la mejora de la eficiencia o eficacia.	Probar y optimizar sin parar la operación; decidir con simulación.

Nota: Información obtenida de (Ibm, 2024)

2.1.9.2 FACTORES DE ÉXITO Y FRACASO EN LA ADOPCIÓN TECNOLÓGICA

Tabla 14: Factores que afectan la Adopción Tecnológica

Factor	Qué implica	Cómo se ve en la práctica
Propósito y caso de uso claro	Beneficio tangible (tiempo, costo, riesgo, ingresos).	Implementamos SGD para renovaciones sin retrasos y expedientes completos.

Factor	Qué implica	Cómo se ve en la práctica
Patrocinio visible de dirección	Liderazgo que prioriza, quita bloqueos y asigna recursos.	Directivos revisan avances quincenales y resuelven dependencias.
Gestión del cambio (personas)	Capacitación, comunicación, incentivos y "campeones".	Comunicar el por qué, formar en cómo, medir adopción.
Diseño centrado en el usuario	Utilidad percibida y facilidad de uso determinan adopción.	Búsquedas por cliente/pólizas en dos (2) clics; plantillas simples.
Despliegue incremental	Utilización de metodologías ágiles	1) Repositorio+metadatos; 2) Flujos+firma; 3) Retención+integraciones.
Arquitectura y datos	Integraciones estables y metadatos mínimos para valor.	Email a expediente, CRM/ERP, control de versiones y trazabilidad.
Gobierno y métricas	Dueños de proceso, políticas (seguridad/retención) y KPIs.	Tablero: tiempo de búsqueda, renovaciones a tiempo, SLA siniestros.
Gestión de riesgos	Seguridad, cumplimiento, continuidad.	MFA, cifrado, perfiles por rol, respaldo y plan BCP.

Nota: Información obtenida de (*Unlocking Success in Digital Transformations*, 2018)

2.2 MICROENTORNO NACIONAL

2.2.1 TRANSFORMACIÓN DIGITAL EN HONDURAS

El crecimiento de la transformación en Honduras va tomando forma, pero de manera lenta y a pasos cortos. En honduras se depende mucho de factores externos a la propia necesidad o solicitud de más avances digitales ya que posee factores desventajosos que no permiten la correcta evolución de esta entre ellos la falta de conectividad, iniciativas propias del gobierno, falta de leyes y programas que apoyen directamente a las empresas para la formación de nuevos procesos que conlleva la digitalización como el eje central de cada proyecto.

2.2.1.1 PROBLEMÁTICAS PARA EVOLUCIÓN DE LA TRANSFORMACIÓN DIGITAL

Según Datareportal (2025), Honduras registró 7.19 millones de usuarios de internet lo que representaba un 65.8%, 7.51 millones de conexiones móviles lo cual equivale a un 68.8% de la población y una mejora considerable del 35.56 Mbps y 57.40 Mbps como medianas de descarga. Además, un 95.4% de las conexiones móviles califican como banda ancha (3G/4G/5G), esto confirma que la infraestructura tecnológica progresa, pero aún se tiene un alto porcentaje fuera de línea (34.2%).

Estas métricas, gran parte de ellas pertenecen a zonas más urbanizadas y donde existe mayor concentración de personas, tales como Tegucigalpa y San Pedro Sula. Desdé 2020, el país opera Chequeo Digital, herramienta oficial para medir el nivel de adopción de tecnologías en MiPymes y orientar a planes de mejora. Dicha herramienta creada por SENPRENDEBID evalúa seis dimensiones:

1. Tecnología y Habilidades digitales
2. Comunicación y canales de venta
3. Organización y personas
4. Estrategia y transformación digital
5. Datos y analítica
6. Procesos

A nivel de gobierno digital, Honduras ya cuenta con un Plan de gobierno digital 20232026 con el fin de impulsar la interoperabilidad, seguridad y servicios en línea. Actualmente se muestran rezagos y problemáticas en la ejecución de un gobierno electrónico como la necesidad de fortalecer gobernanza tecnológica y estandarización de datos.

2.2.2 PROGRAMAS NACIONALES E INTERNACIONALES DE APOYO A MIPYMES

La digitalización en MiPymes no depende únicamente del sector público, sino también de un contexto amplio entre gobierno digital, políticas públicas, estrategias nacionales e intervenciones como programas internacionales que buscan subsanar esa brecha digital tan amplia que existe actualmente. Dichos programas tienen como objetivo poner una base sólida para las MiPymes que buscan una transformación digital sostenible.

2.2.2.1 AGENDA 2030 DE HONDURAS

La agenda 2030 incluye 17 objetivos de desarrollo sostenible como marco de referencia para alcanzar un desarrollo sostenible en el país. Según el Programa Nacional de las Naciones Unidas para el Desarrollo (PNUD) La Agenda 2030 aborda necesidades sociales, económicas y ambientales que forman un plan maestro para conseguir un futuro sostenible para las naciones. La disposición de cada país a cumplir la Agenda 2030 muestra el compromiso que existe por reducir las desigualdades y crear comunidades más justas e inclusivas para todos y todas.

Con el programa se han establecido 68 metas y 99 indicadores consensuados con actores como el gobierno, sociedad civil y la academia con el fin de adaptarse al país. Dicho esto, de acuerdo con el segundo informe Nacional Voluntario (2020) se reportaron varios objetivos de desarrollo clave:

- Reducción de pobreza y pobreza extrema.
- Mejora en la seguridad alimentaria.
- Buenas prácticas en educación básica.
- Avance en infraestructura y transparencia pública.

Aun con la idea de la aplicación de esta agenda y lo que conlleva en base a sus objetivos se han encontrado algunos desafíos:

- Falta de mecanismos robustos de seguimiento y evaluación correcta de los avances.
- Necesidad de fortalecer estructuras de gobernanza, coordinación y transparencia en implementación. (PNUD, 2020)

Con ello podemos mostrar en la tabla 15 algunos objetivos de desarrollo sostenible en base a su relación con el sistema de gestión documental.

Tabla 15: Dimensiones de la Agenda Digital 2030 Honduras

Dimensión de la agenda 2030	Contexto Hondureño	Relación con sistema de gestión documental.
Objetivo de desarrollo sostenible 9	Prioriza infraestructura e innovación tecnológica.	Digitalización del sistema de gestión documental, automatización de procesos y conectividad empresarial conjunta.
Objetivo de desarrollo sostenible 8	Promueve empleo digno y crecimiento económico.	Nuevos canales de servicio y eficiencia operativa.
Objetivo de desarrollo sostenible 16	Mejora la transparencia de la información.	Trazabilidad de la documentación y seguridad del manejo de esta.
Objetivo de desarrollo sostenible 17	Impulsa alianzas estratégicas.	Programas de SENPRENDEBID

Nota: Información obtenida (PNUD, 2020), Elaborado por autores

2.2.2.2 PROGRAMA DEL BANCO INTERAMERICANO DE DESARROLLO

Considerando las dimensiones BID y entidades nacionales lanzaron cooperaciones para acelerar la transformación digital de MiPymes:

- HOT1375: Este proyecto tiene por objetivo acelerar el proceso de transformación digital de las MiPymes en Honduras desde una intervención con el sector privado (en coordinación con el sector público). El fin es mejorar las capacidades para incrementar la resiliencia, asegurar la continuidad de la actividad emprendedora adaptando sus modelos de negocio al contexto de crisis sanitaria y nueva normalidad, y favorecer de forma general el aumento del empleo decente en el país y la formalización. (BID, 2020)
- HOG1256: Este proyecto tiene por objetivo acelerar el proceso de transformación digital de las MiPymes en Honduras desde una intervención con el sector privado (en coordinación con el sector público). El fin es mejorar las capacidades para incrementar la resiliencia, asegurar la continuidad de la actividad emprendedora adaptando sus modelos de negocio al contexto de crisis sanitaria y nueva normalidad, y favorecer de forma general el aumento del empleo decente en el país y la formalización. (BID, 2020)
- HOT1456: El objetivo general de esta Cooperación Técnica (CT) es fortalecer las capacidades de instituciones estratégicas para el despliegue de servicios de asistencia técnica y extensionismo tecnológico para las MIPYME en Honduras, con enfoque territorial, de género y transición climática; lo que además ayudará a la preparación del programa de apoyo a la modernización tecnológica y digitalización de MIPYME (HOL1249) en el país. Esto se alcanzará a través de tres objetivos específicos:
    - Ampliar el conocimiento sobre las demandas y necesidades de apoyo a la modernización tecnológica de las MIPYME hondureñas, incluyendo tecnologías climáticas.
    - Diseñar un portafolio de instrumentos de apoyo a la modernización tecnológica de las MIPYME adaptadas al contexto local y con enfoque de género.
    - Apoyar el intercambio de experiencias regionales y buenas prácticas en la implementación de instrumentos de mejora de gestión y modernización tecnológica de MIPYME. (BID, 2020)
- HOL1202: Este programa promoverá la transformación digital que el gobierno brinda a los ciudadanos y fortalecerá la capacidad de las Pymes y startups para participar en la economía digital. Para lograrlo, el programa:

- Mejorará los servicios gubernamentales mediante la implementación de soluciones de gobierno electrónico para servicios a los ciudadanos.
- Implementará un programa de identidad digital.
- Brindará infraestructura de conectividad de banda ancha.
- Promoverá un ecosistema digital para el empleo e inversiones en la economía digital, fortaleciendo la capacidad de las Pymes y startups, promoviendo mayores niveles de capital humano especializado en industrias creativas y digitales. (BID, 2020)

2.2.3 BARRERAS ESTRUCTURALES Y SOCIALES EN HONDURAS

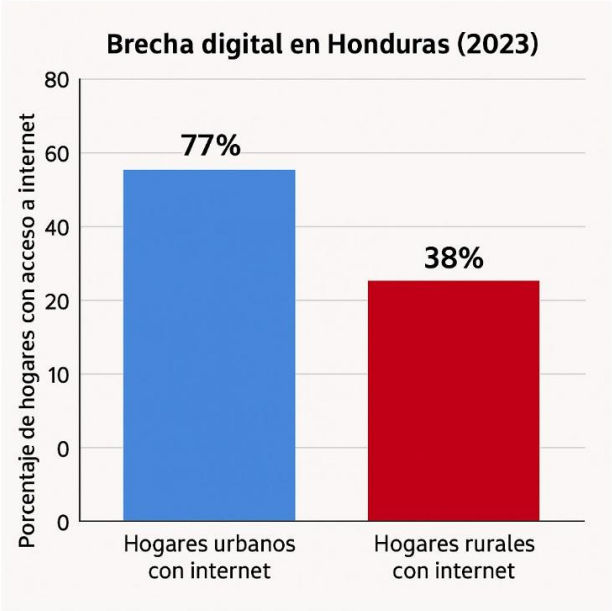
Considerando los avances recientes en conectividad y programas existentes que promueven la digitalización en Honduras, se sigue enfrentando contra importantes barreras estructurales y sociales que limitan la adopción plena de tecnología digital para aplicarlas en procesos y automatizaciones dentro de las MiPymes, particularmente en las que ofrecen servicios profesionales.

2.2.3.1 BRECHA DIGITAL

El internet en el país alcanzó un 65.8% de la población según Datareportal (2025), con esto podemos identificar que ya hay un avance significativo en el país, pero encontramos marcado la diferencia entre zonas rurales y urbanas, donde vemos que casi un 77% del casco urbano cuenta con internet mientras que sólo un 38% de zonas rurales cuenta con ello en sus localidades.

La falta de conexión limita mucho la adopción de digitalizar muchas medidas y procesos que son favorables para realizarlo ya que no se cuenta con la infraestructura necesaria para aplicar dichas mejoras. Igualmente, la falta de conectividad afecta directamente a las MiPymes, ya que muchas de ellas se encuentran fuera del casco urbano.

Gráfico 2: Brecha Digital en Honduras



Nota: Información obtenida de (DIGER,2023)

2.2.3.2 COSTOS Y FRAGMENTACIÓN TECNOLÓGICA

Según CEPAL (2023) hay un gran déficit de talento humano capacitado lo que se considera uno de los mayores obstáculos para las MiPymes, ya que su mano de obra se percibe como costosa. En gran parte de las empresas carecen de personas con habilidades aptas para aplicar herramientas de gestión de documentación digital, ciberseguridad o analítica de datos limitando drásticamente a la empresa a buscar talento humano costoso.

Aparte del costo de mano de obra humana, existe una gran brecha para poder implementar una inversión tecnológica amplia. Según BID (2023) apenas un 15% de los MiPymes Hondureños tienen acceso a financiamiento formal, un porcentaje sumamente corto para la necesidad que muchas MiPymes poseen.

Considerando el inconveniente que es la financiación adecuada y disponible debemos añadir la percepción de costes sumamente altos para la implementación, se percibe de esa manera y eso causa mucha confusión y la adopción de medidas en contra de estos gastos muy grandes ya que muchas MiPymes no consideran contar con el colchón económico necesario. Con ello, muchas empresas usan las herramientas a coste 0 pero de manera sumamente limitada, algunas como Facebook, WhatsApp o Instagram que pueden solventar muchas cosas, son utilizados de manera simple y básica para comunicación o marketing pero con escasa adopción de manera empresarial o alineada con la estrategia del negocio creando así un entorno pasivo de uso de internet proponiendo presencia sin capacidad para generar transacciones o aprovechar análisis de datos como una ventaja competitiva.

2.2.3.3 CULTURA ORGANIZACIONAL Y BRECHAS SOCIALES

Uno de los factores principales de la falta de implementación de digitalización es la cultura empresarial.

- Muchas MiPymes siguen operando bajo procesos manuales y documentación física en archiveros o bandejas, esto genera una amplia resistencia al cambio y desconfianza de un cambio que suele ser necesario.
- Según IFC (2021) la adopción de herramientas digitales se suele reducir a herramientas básicas como redes sociales y hojas de cálculo sin verificar las necesidades de la MiPymes o alinearlas con los objetivos del negocio.
- En Honduras se asocia mucho a la falta de marcos legales y protección de datos personas, también que se tiene la falsa creencia que los entornos digitales no son seguros y que puede causar daños o costosas repercusiones.

Con estos factores podemos notar claramente una problemática difícil de evadir y que causa una ralentización de la adopción de tecnologías innovadoras.

Otro factor que influye en la adopción de nuevas tecnologías son las brechas sociales, Según BID (2023) las mujeres emprendedoras tienen menor acceso a financiamiento, capacitación digital y redes de apoyo lo que limita claramente la participación en el ámbito digital, así mismo los jóvenes pasa algo similar, aunque están sumamente adaptados a las innovaciones tecnologías presentan problemas con la inserción al mundo laboral y a crédito para emprender.

2.2.4 COMPETENCIA LOCAL EN CORREDURÍAS DE SEGUROS

El mercado de seguros está compuesto por aseguradoras y corredurías locales, cuya competencia va más basada entre modelos de negocio donde se encuentran procesos manuales y algunos pioneros que ya comienzan a realizar la digitalización en múltiples procesos, este factor impacta en el mercado y la competitividad de este, confianza y atención al cliente y la capacidad de afrontar las necesidades y ofrecer soluciones que se requieran.

2.2.4.1 EMPRESAS CON OPERACIONES MANUALES

La mayor parte de las corredurías locales se siguen manteniendo en modelos de negocio donde lo tradicional manda, factores como expedientes físicos, contratos en papel y atención presencial son normales y comunes lo cual genera retrasos en trámites, duplicidad de documentos y errores en información sensible.

Pese a los avances actuales en la digitalización en otros sectores, el ámbito asegurador en Honduras evidencia un rezago significativo en la adopción de herramientas tecnológicas, lo

que se traduce en una limitación directa para su eficiencia y competitividad en el mercado.

2.2.4.2 EMPRESAS PIONERAS EN DIGITALIZACIÓN DE PROCESOS

Empresas MAPFRE, seguros Atlántida o FICOHSA han comenzado con la implementación de procesos para digitalizar factores que brinden una mejor experiencia al usuario.

- Pólizas electrónicas
- Cotizaciones
- Apps móviles
- Propuestas de seguros a demanda
- Facturación electrónica
- Sistemas de control de expedientes

Estas empresas aprovechan la infraestructura digital para ofrecer servicios más ágiles, eficientes y con soluciones necesarias para clientes exponenciales entre ellas trazabilidad y una gestión óptima de documentación. Generando así una gran ventaja sobre las corredurías tradicionales. Considerando los factores que tienen las corredurías más grandes con respecto a las tradicionales, es sumamente simple entender sus barreras y limitaciones.

Tabla 16: Barreras de Corredurías Tradicionales frente a Pioneros en el Mercado

Factor	Descripción de barrera
Regulaciones ambiguas	Existe muy poca información acerca de implementaciones de digitalización (p. ejemplo la firma electrónica).
Costes percibidos altos	Para las corredurías tradicionales los costes de implementación de nuevas tecnologías suelen ser percibidos de manera muy alta o incosteable.
Cultura organizacional	Resistencia a dejar formatos físicos o tradicionales, muy arraigados al uso de procesos manuales por zona de confort.
Falta de apoyo institucional	Muy poca confianza y resultados conocidos para digitalizar MiPymes.

Nota: Elaborado por autores

2.2.5 OPORTUNIDAD DE IMPLEMENTACIÓN Y ADOPCIÓN DE UN SISTEMA DE GESTIÓN DOCUMENTAL

Con la implementación de un sistema de gestión documental alineado a las normas ISO 15489 y 27001 con reforzamiento en la NIST brindará una gran ventaja en la gestión documental, así como una transformación para ser pioneros en el sector.

Tabla 17: Oportunidades de Diferenciación mediante la Adopción de SGD

Dimensión estratégica	Situación actual de correduría hondureñas	Ventajas de adopción	Impacto en la empresa
Gestión documental	Archivos físicos, duplicidad de información, dispersión de información.	Organización y trazabilidad bajo la ISO 15489.	Reducción de pérdidas de información y mejora en el manejo de información sensible.
Cumplimiento normativo	Procesos manuales que dificultan auditorías y cumplimiento de leyes relacionadas.	Documentación trazable y registros de movimiento de información, facilidad de auditar.	Facilidad en realización de auditorías y cumplimientos regulatorios.
Eficiencia operativa	Procesos actuales lentos y sumamente manuales, altos gastos en papelería y archivos físicos.	Procesos automatizados, firma electrónica y experiencia rápida del usuario.	Aumento en el ahorro de costos, tiempos de espera y ejecución reducidos.
Experiencia del usuario	Atención presencial limitada, baja transparencia de tiempos de trámites, sobrecarga de papel.	Mejora en la experiencia del cliente, procesos y asesorías virtuales.	Confianza del cliente y percepción de digitalización por parte del usuario completa.
Innovación y mejora competitiva	Rezago frente a empresas emergentes o aseguradoras locales con procesos digitales.	Adopción de estándares internacionales de renombre proporcionando confianza y profesionalismo.	Posicionamiento entre pioneras de innovación, brindando digitalización y una base para ejemplificación de procesos realizados adecuadamente.
Seguridad de la información	Vulnerabilidad a pérdida de documentación, problemas externos por factores como incendios o robos.	Controles de seguridad en tiempo real, manejo de la información bajo cifrado y respaldo.	Mayor confianza del cliente, cumplimiento de estándares de calidad y transparencia.

Nota: Elaborado por autores

2.3 ENTORNO ESPECÍFICO EMPRESARIAL (CASO SEGURO TOTAL)

Seguro Total Correduría de Seguros S de R.L. se origina por iniciativa de su socio fundador Agustín Humberto Avelar Sandoval, quien dio sus primeros pasos como profesional independiente en la venta de seguros en el año 1975, hasta llegar a constituirse como una Sociedad de Responsabilidad Limitada que 28 años después se denominada como “Seguro

Total Correduría de Seguros S. de R.L.”

Actualmente se encuentra constituida mediante escritura Pública No. 89 ante los oficios del Abogado y Notario Arturo H. Medrano, debidamente inscrita en el “Registro de Agentes Dependientes, Agentes independientes o Corredores de Seguros” mediante el registro No. REGSFCS222021 autorizados para operar en todos los ramos de seguros y fianzas a nivel nacional. Se encuentran también inscritos en la Cámara de Comercio e Industria de Tegucigalpa (CCIT), en la Asociación Nacional Industriales (ANDI), en la Cámara Hondureña de Corredores de Honduras (CAHDECOSE) y AHPROINSE (Asociación Hondureña de Profesionales Intermediarios de Seguros). A nivel general mantiene aproximadamente 8,000 clientes entre pólizas individuales y colectivas.

La correduría posee oficinas en las ciudades de Tegucigalpa y San Pedro Sula y se distingue por la venta de seguros a persona naturales como a jurídicas ofreciendo los siguientes productos autorizados por la CNBS que se agrupan en tres ramas principales que son las siguientes:

Tabla 18: Agrupaciones de Tipos de Seguros

Rama	Seguros
Personas	Vida, Gastos Médicos, Accidentes, Saldo de Deuda, Fondo de Pensiones, Asistencia de Viajes
Patrimoniales	Incendio, Equipo Electrónico, Maquinaria, Construcción
Fianzas	Fianzas

Nota: Elaborado por los autores

Posee contratos comerciales de venta de seguros de las siguientes compañías aseguradoras:

- Ficohsa Seguros (Interamericana de Seguros)
- MAPFRE Seguros Honduras
- Seguros Atlántida
- Seguros Crefisa
- PAN American Life
- Seguros del País
- ASSA Seguros de Honduras
- Davivienda (Seguros Bolívar de Honduras)

2.3.1 MISIÓN

Somos una Correduría de seguros que nace para brindar tranquilidad a nuestros clientes con asesoría en servicios y productos de Seguros que promueven el crecimiento y resguardo de su patrimonio ante posibles riesgos, con el personal comprometido altamente calificado y motivado.

2.3.2 VISIÓN

Ser una correduría diferenciada por su calidad humana, ofreciendo respuestas rápidas y efectivas con un servicio tecnológico de alta calidad, equipo humano encaminado a la satisfacción del cliente por medio de respuestas rápidas confiables y seguras.

2.3.3 VALORES

- Compromiso
- Lealtad
- Transparencia
- Honestidad
- Confidencialidad
- Respeto

2.3.4 ESTRUCTURA ORGANIZATIVA

Figura 3: Estructura Organizativa Correduría Seguro Total

Nota: Elaborada por autores

Como se muestra en la imagen de desglosa la estructura organizativa de la correduría en donde a nivel de su oficina central en Tegucigalpa, Honduras posee 12 colaboradores y en la oficina de San Pedro Sula, Hondura mantiene solamente un colaborador.

2.3.5 HERRAMIENTAS UTILIZADAS

La correduría a nivel general utiliza como soporte tecnológico para la gestión documental las herramientas que proporciona Google Workspace, principalmente utilizando Gmail y Google Drive. Asimismo, cuenta con un sistema de control y seguimiento de solicitudes elaborado por Soluciones Dinámicas, no obstante, dicho sistema no almacena o referencia documentos asociados a las distintas pólizas.

De forma paralela, la correduría mantiene expedientes físicos con copias de todas sus pólizas y sus documentos asociados a los clientes, tales como cotizaciones, identidades, RTN, escrituras, licencias, inclusiones y exclusiones, reclamos (incluidas copias de las facturas presentadas). precertificaciones, siniestros de daños, imágenes de las inspecciones de propiedades y automóviles, entre otros. Para optimizar el espacio físico de la oficina, estos archivos físicos se administran a través de la empresa RANSA, en donde se envían documentos de mayor antigüedad o de pólizas ya no vigentes, cuando se requiere la consulta y estos no se encuentran disponibles en el archivo físico de la oficina, se solicita su retornó para su revisión.

Esto demuestra que no todos los documentos de la correduría se encuentran almacenados de manera digital lo que facilita su seguimiento y control.

Adicionalmente, la correduría se apoya de los portales digitales de las diferentes compañías de seguros para elaboración de cotizaciones, seguimiento de solicitudes, generación de carnés, carga de reclamos y seguimiento de pagos, conforme a los procedimientos establecidos por cada compañía aseguradora.

2.3.6 PROCESO ACTUAL

El proceso actual que genera el uso y solicitud de documentos son todos aquellos en donde se realiza la cotización y venta de un seguro. De manera general se distingue el siguiente proceso:

1.Posible cliente contacta por medio de teléfono, correo electrónico o directamente en la oficina de cotización sobre un seguro.
2.Asesor de ventas solicita información básica como ser nombre completo, edad, número de identidad, correo electrónico y tipo de seguro para generar las cotizaciones.

3.Asesor de ventas genera 3 cotizaciones con el cliente y las comparte por medio de correo electrónico y al número de teléfono del cliente.
4.Cliente recibe solicitudes y cualquier duda consulta con el asesor de ventas.
5.Cliente acepta y forma la cotización y confirma con el asesor de ventas.
6. Asesor de ventas comparte el formulario de inscripción y el cliente lo llena.
7.Asesor de ventas solicita documentación adicional según el tipo de seguro y de manera general se solicita imagen de la identidad y RTN.
8.Asesor de ventas recibe formulario y documentación adicional y envía la información a la compañía aseguradora correspondiente por medio de correo electrónico.
9.Asesor de ventas recibe confirmación de recepción de la información.
10. La compañía aseguradora emite la póliza y la comparte con la correduría.
11. Se comparte la información con el cliente e inicia la vigencia de la póliza.

2.3.7 BRECHAS Y RIESGOS DETECTADOS

Actualmente, los controles de seguridad digital son mínimos, ya que únicamente se cuenta con una contraseña de acceso al correo electrónico, la cual no exige requisitos básicos para garantizar que sea segura. En cuanto a los archivos físicos, estos se encuentran a la vista de cualquier persona, lo que permite que puedan ser abiertos y consultados sin restricción, comprometiendo la confidencialidad de la información.

Asimismo, no existe un sistema de versionamiento digital que facilite la trazabilidad de los documentos ni un control estructurado sobre los archivos físicos, más allá de una organización básica por ramo y orden alfabético, lo cual limita la capacidad de mantener actualizada la información.

A nivel normativo, dado que en Honduras aún no existe una ley específica de protección de datos, la empresa no incurre en incumplimientos legales, aunque esta ausencia de regulación no mitiga los riesgos asociados al manejo inadecuado de la documentación.

Se han detectado también brechas de seguridad en términos del almacenamiento de los documentos físicos y eliminación de las copias físicas en la oficina principal de Tegucigalpa de la correduría donde encontramos los siguientes hallazgos.

- Archivos físicos a la vista de todo el personal, sin la utilización de llaves para asegurar su integridad.
- Archivos sin eliminar a vista de todo el personal.
- Archivero abierto sin un índice de identificación.

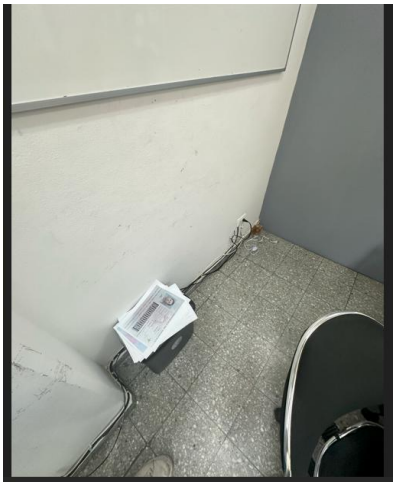
Figura 4: Archivo Principal

Nota: Tomada por los autores en la oficina principal de Tegucigalpa, Honduras.

Figura 5: Archivos físicos de reclamos sin seguridad

Nota: Tomada por los autores en la oficina principal de Tegucigalpa, Honduras.

Figura 6: Archivos destinados a Eliminación sin Procesar:



Nota: Tomada por los autores en la oficina principal de Tegucigalpa, Honduras.

2.3.8 NECESIDADES Y OPORTUNIDADES

El sistema de gestión documental debe contemplar funcionalidades que garanticen la seguridad, trazabilidad y disponibilidad de la información conforme a los lineamientos de la ISO 15439, ISO 30301, ISO/IEC 27001 y el NIST Marco de Ciberseguridad.

Entre los requerimientos funcionales destacan: el control de accesos basado en roles, versionamiento automático de documentos, auditoría de cambios, respaldo seguro de la información, y capacidad de clasificación y búsqueda eficiente de archivos.

En el plano técnico, se requiere infraestructura con mecanismos de cifrado, autenticación multifactor, almacenamiento en servidores seguros o en la nube con certificaciones internacionales, integración con sistemas ya existentes como ser Google Drive y Gmail etc.; asegurando tener un cumplimiento con protocolos de seguridad para mitigar riesgos de fuga o alteración de datos.

2.3.9 CAPACITACIÓN Y CAMBIO CULTURAL PARA ADOPCIÓN DEL SISTEMA

La implementación de un sistema de gestión documental no solo demanda infraestructura tecnológica, sino también un proceso de cambio cultural dentro de la organización. Para lograr esto se deben seguir las siguientes acciones:

1.Capacitacitación a los colaboradores en el uso de la plataforma, considerando las mejores prácticas en el manejo de la información y en la importancia de la seguridad con base al cumplimiento normativo.

2.Establecer un procedimiento para garantizar la actualización constante de la documentación

logrando reducir duplicados y así evitar información obsoleta.

3.Fomentar una cultura de responsabilidad compartida en la cual cada usuario o colaborador de la empresa entienda sus roles y responsabilidades en la clasificación, actualización y protección de la información.

2.4 TEORÍAS DE SUSTENTO

2.4.1 NORMAS ISO

La investigación se sustenta de manera principal en las normas internacionales ISO, específicamente en la ISO 154891:2016 sobre la gestión documental y la ISO 27001:2022 sobre la gestión de seguridad de la información. Estas normas no deben entenderse como guías de referencias, sino como estándares reconocidos mundialmente que definen la excelencia, establecen parámetros de calidad y promueven la confiabilidad de los procesos organizacionales. Tal como lo establece la propia organización "Las normas definen lo que es excelente, estableciendo puntos de referencia coherentes tanto para las empresas como para los consumidores, garantizando así la fiabilidad, generando confianza y simplificando las opciones" (ISO, 2025).

La Organización Internacional de Normalización (ISO, por sus siglas en inglés) es una entidad independiente y no gubernamental, dicha organización reúne a expertos en el mundo con el propósito de consensuar las mejores prácticas en múltiples ámbitos del quehacer humano. Sus aportes abarcan desde la inteligencia artificial y la gestión de la calidad, hasta el cambio climático, energía renovable, seguridad de la información y los sistemas de gestión documental. En este sentido su misión es clara: "hacer la vida más fácil, más segura y mejor, para todos y en todas partes" (ISO, 2025).

Las Normas ISO proporcionan especialidades o normas esenciales que se encargan principalmente de factores como: Calidad, Seguridad de la información, gestión antisoborno, gestión ambiental, seguridad y salud laboral y hasta información tecnológica o gestión de sistemas. Considerando este factor la ISO promueve un sinfín de posibilidades de mejora en la ejecución de las actividades laborales brindando así un seguro y sobre todo una mejor perspectiva de ejecución de acciones útiles para el desarrollo de la propia organización.

Hasta la fecha hay un total de 25953 Normas Internacionales y otros documentos que abarcan prácticamente todos los aspectos de la tecnología, la gestión y la producción. Miembros que representan a ISO en su país y 828 Comités técnicos y subcomités encargados de la elaboración de normas. En el marco de esta investigación, el enfoque se orienta al uso de las normas ISO 15489-1:2016 e ISO/IEC 27001:2022, que constituyen la base técnica para el

diseño de un Sistema Digital de Gestión Documental (DMS) en MiPymes de servicios profesionales, garantizando seguridad, accesibilidad y trazabilidad de la información crítica.

2.4.1.1 ISO 15489-1:2016 GESTIÓN DOCUMENTAL

La ISO 15489 regula los principios y requisitos para la gestión de documentos en las organizaciones, tanto en formato digital como físico, asegurando su autenticidad, integridad, confiabilidad y usabilidad a lo largo de todo su ciclo de vida. Según Ya rasca Chávez (2024), este estándar considera los documentos no sólo como soportes para las operaciones comerciales, sino como recursos informativos estratégicos que fortalecen la memoria institucional y respaldan la toma de decisiones.

El estándar se organiza en 2 partes

1. ISO 15489-1:2016: Define los conceptos fundamentales, principios y requisitos generales de la gestión documental
2. ISO/TR 15489-2:2016: Desarrolla estrategias y metodologías para implementar un sistema de gestión documental, incluyendo herramientas como;
    a. Cuadro de clasificación
    b. Calendario de retención documental
    c. Tabla de acceso y seguridad
    d. Procedimiento para disposición de documentos

De esta manera, la norma vela porque los documentos conserven valor probatorio, histórico y operativo a lo largo de todo su ciclo de gestión.

2.4.1.2 ISO/IEC 27001:2022 – SEGURIDAD DE LA INFORMACIÓN

La ISO/IEC 27001:2022 es un estándar internacional más reconocido para el establecimiento de un sistema de gestión de seguridad de la información (SGSI). Aplicable a organizaciones de cualquier tamaño o sector. Su objetivo principal es proteger la información sensible y valiosa que pueda incluir datos de empleados, clientes, proveedores o propiedad intelectual.

Según Yungán Cazar (2022), la ISO 27001 proporciona una lista estructurada de controles de seguridad que sirven como lista de verificación para evaluar la madurez de la organización en aspectos como:

- Análisis y gestión de riesgos de seguridad de la información.
- Políticas de acceso y control de usuarios.
- Continuidad de negocio y recuperación ante incidentes.
- Auditorías internas y mejora continua del SGSI

La norma no solo establece una metodología de gestión de riesgos, sino que también garantiza un marco internacionalmente aceptado para la protección de datos, cumplimiento normativo y la generación de confianza entre partes interesadas.

La integración de las ISO 154891:2016 y la ISO/IEC 27001:2022 es un pilar para construir sistemas documentales modernos y seguros. Mientras la primera norma asegura la correcta organización, trazabilidad y disponibilidad de documentos, la segunda refuerza su seguridad y resiliencia frente a todo tipo de riesgos.

2.4.2 CUARTA Y QUINTA REVOLUCIÓN INDUSTRIAL

La cuarta revolución industrial, concepto iniciado por Klaus Schwab en 2016, ha evolucionado en los últimos años con el énfasis en digitalización masiva, la integración de tecnologías emergentes como la IA, internet de las cosas (IoT), la analítica avanzada, etc. De acuerdo con Xu, David y Kim (2021) la cuarta revolución industrial se distingue por la convergencia de sistemas físicos, digitales y biológicos, lo que ha transformado la producción y los servicios en una serie de toma de decisiones organizacionales de alto impacto.

Una de las características principales de la cuarta revolución industrial es la gestión estratégica de datos. En un contexto donde la información es tan relevante y se genera una cantidad exorbitante de datos las organizaciones deben disponer de herramientas para recopilar, almacenar, proteger y analizar datos en tiempo real.

Tabla 19: Períodos de la Cuarta Revolución Industrial

Período	Período de Transición	Recurso Energético	Logro Principal	Avance Técnico	Industrias Principales	Medios de Transporte
I: 1760–1900	1860–1900	Carbón	Máquina de vapor	Máquina de vapor	Textil, Acero	Tren
II: 1900–1960	1940–1960	Electricidad a base de petróleo	Motor de combustión interna	Motor de combustión interna	Metalurgia, Automotriz, Construcción de maquinaria	Tren, Automóvil
III: 1960–2000	1980–2000	Energía nuclear, Gas natural	Computadoras, Robots	Computadoras, Robots	Automotriz, Química	Automóvil, Avión
IV: 2000–	2000–2010	Energías renovables	Internet, Impresora 3D, Ingeniería genética	Internet, Impresora 3D, Ingeniería genética	Industrias tecnológicas avanzadas	Automóvil eléctrico, Tren de alta velocidad

Nota: Información obtenida de Xu, M., David, J. M., & Kim, S. H. (2020).

La quinta revolución industrial en cambio se basa más en la sostenibilidad del humano con la interacción de la tecnología y la sociedad, Según la Comisión Europea (2024) esta etapa no solo busca mayor automatización, sino una colaboración hombre–máquina orientada a la personalización, la resiliencia y la responsabilidad ética en el uso de datos. (European Commission, 2024).

La quinta revolución industrial recibe la noción como una transformación digital equilibrada entre tecnología y humanidad, abordando retos sociales que previamente no se tomaban tan en consideración. Ahora, identificamos componentes como la automatización, IA con propósito humano o ligado a la ayuda humana y participación de múltiples factores orientados a la facilidad y relación favorable entre humano máquina (ResearchGate, 2023).

La integración de las Normas ISO (154891:2016 y 27001:2022) con los principios de la Cuarta y Quinta Revolución Industrial constituye el sustento teórico de esta investigación. Mientras las ISO proporcionan un marco normativo y técnico para garantizar la seguridad, trazabilidad y confiabilidad de los documentos, las revoluciones industriales ofrecen la visión estratégica que alinea la digitalización documental con la innovación tecnológica, la sostenibilidad y el enfoque humano.

2.5 METODOLOGÍAS DESARROLLADAS

2.5.1 METODOLOGÍAS APLICADAS A NIVEL INTERNACIONAL

Las metodologías utilizadas para la implementación de un SGD varían a nivel mundial, dentro de esta sección encontrará un resumen de algunas investigaciones y artículos que referencian diferentes metodologías. Resaltando de la investigación que aplicación o las metodologías utilizadas utilizan como base las normas ISO como ser la 15489 y la 30301.

Según lo investigado por Naula López (2023), en el ámbito de la gestión documental se identifican diversas metodologías que pueden aplicarse en las organizaciones en este caso aplicadas a PYMES en Ecuador. Entre las más relevantes mencionadas en la investigación se encuentran DIRKS, BPMN, RTA y PMBOK.

La metodología DIRKS (Designing and Implementing Recordkeeping Systems), basada en la Norma ISO 15489, plantea ocho etapas secuenciales: investigación preliminar, análisis de acciones de la empresa, identificación de requerimientos, evaluación de sistemas existentes, definición de tácticas, diseño del programa, implementación y revisión posterior. Esta metodología permite garantizar la trazabilidad y conservación de los documentos, así como la

identificación y mitigación de riesgos relacionados con la información (Naula López, 2023, pp. 2425).

Según Naula López (2023), diferentes metodologías ofrecen aportes relevantes a la gestión documental. Por ejemplo, encontramos la BPMN (Business Process Model and Notation) que permite representar gráficamente los procedimientos internos en fases de diseño, modelado, ejecución, monitoreo y optimización, favoreciendo la automatización y la eficiencia del flujo documental. De la misma forma, encontramos otros modelos como ser el RTA (Red de Transparencia y Acceso a la Información) la cual incorpora cuestionarios, guía y directrices que estandarizan a los procesos documentales bajo buenas prácticas internacionales de archivística.

Igualmente encontramos que Naula López menciona el uso de la metodología del PMBOK (Project Management Body of Knowledge), estructurada en cinco fases (iniciación, planificación, ejecución, seguimiento/control y cierre), aporta un enfoque de gestión de proyectos aplicable también a iniciativas de gestión documental. aunque se analizaron estas metodologías, la investigación se basó en DIRKS por considerarse más clara y sencilla de aplicar en pequeñas y medianas empresas, al estar directamente orientada a procesos documentales y apoyada en estándares internacionales

De la misma forma encontramos la siguiente investigación según, Díaz Suárez, Junco Vázquez y Ruíz González (2021), la metodología MOPIG (Modelo para la Implementación de la Gestión de Documentos) ofrece una guía especializada para organizar, controlar y gestionar documentos, asegurando la transparencia administrativa, la trazabilidad de las decisiones y el apoyo a la toma de decisiones empresariales. Aunque inicialmente fue diseñada para entornos empresariales, ha demostrado ser adaptable al ámbito académico, aplicándose exitosamente en la Universidad de La Habana para la Maestría en Gestión de Información (pp. 3435).

Según Balboa y Medina (2021), los sistemas de gestión documental deben evaluarse considerando estándares internacionales como la ISO 15489, la ISO 16175 y la ISO 23081, que garantizan la fiabilidad, autenticidad, integridad y disponibilidad de los documentos en todo su ciclo de vida. Estas normas constituyen un soporte teórico y técnico esencial en los procesos de transformación digital del Estado, ya que permiten definir requisitos funcionales y archivísticos que aseguran la correcta gestión de documentos electrónicos (pp. 34).

El Modelo de Gestión Documental (MGD), definido por la Secretaría de Gobierno Digital del Perú, constituye un marco que busca ordenar y mejorar la manera en que se administran los documentos institucionales en el Estado. Este modelo plantea lineamientos que garantizan que los documentos sean auténticos, completos y accesibles a lo largo de su ciclo de vida,

promoviendo la trazabilidad de la información y reduciendo trámites innecesarios. Además, fomenta la transparencia administrativa y se encuentra fundamentado en la norma internacional UNEISO 30301, que establece los requisitos para la correcta gestión de la información documentaria (Del Pino & Pinedo, 2025, p. 18).

En el ámbito hospitalario, Del Pino y Pinedo (2025) desarrollaron un modelo de gestión documental digital orientado a hospitales de nivel III en el Perú. El modelo transforma el flujo documental tradicional en un proceso totalmente digital, apoyado en arquitecturas empresariales (TOGAF), arquitecturas de software C4 y procesos definidos en BPMN. Los módulos centrales incluyen registro, envío, recepción, seguimiento, firma digital y notificaciones automáticas, lo que garantiza la trazabilidad de los documentos administrativos. En sus conclusiones, los autores señalan que la implementación del sistema permitió optimizar los tiempos de respuesta, reducir la pérdida de información y fortalecer la eficiencia institucional, alcanzando una aceptación general del 89.2% entre los usuarios. Asimismo, destacan beneficios tangibles como la reducción del 21.5% en gastos de impresión y el incremento del 30.4% en la eficiencia de la gestión de insumos hospitalarios, evidenciando el impacto positivo de la digitalización en la gestión documental (pp. 18, 6768).

2.5.2 METODOLOGÍA APLICADA AL PROYECTO

Luego de la investigación hemos definido la utilización de las siguientes metodologías como bases o directrices para el diseño de una Sistema de Gestión Documental de manera integral buscando cumplir con las bases de las Normas ISO y como apoyo el Marco NIST de Ciberseguridad.

2.5.2.1 METODOLOGÍA DIRKS

La metodología DIRKS (Designing and Implementing Recordkeeping Systems) fue desarrollada a finales de la década de 1990 e inicios de la década de 2000, impulsada por el Archivo Nacional de Australia y la Autoridad de Registros del Estado de Nueva Gales del Sur.

Según el National Archives of Australia (2001), la metodología DIRKS se fundamenta en el estándar australiano AS ISO 15489:2002 sobre gestión de documentos o Records Management por sus siglas en inglés.

La metodología comprende 8 pasos que son los siguientes:

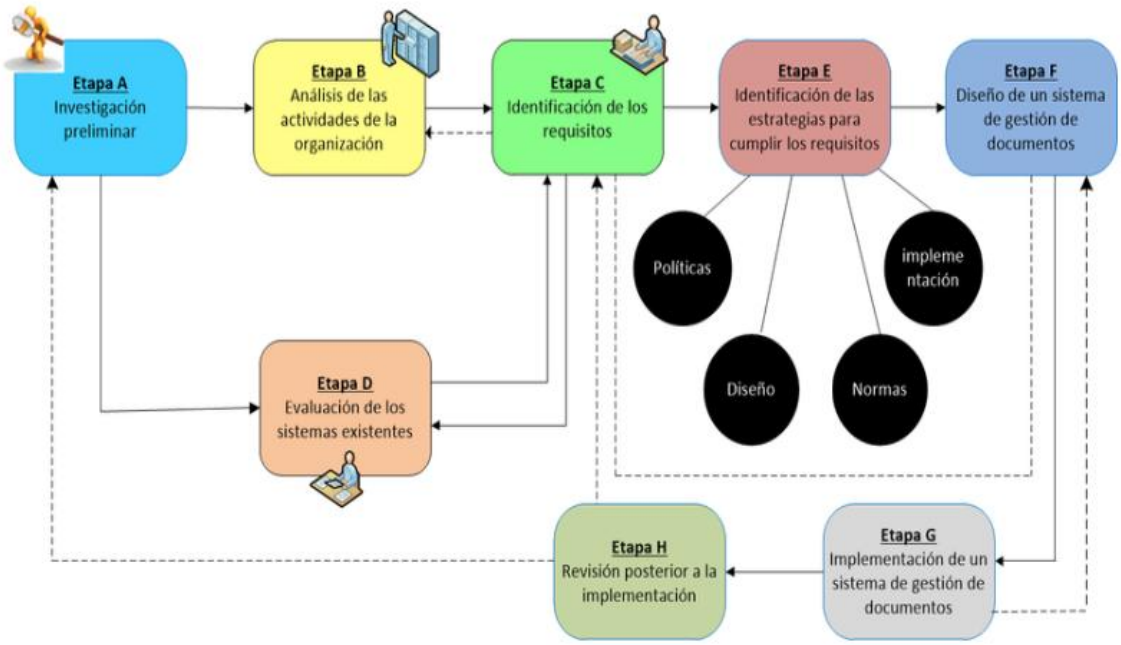
1. Investigación Preliminar:
    a. Recolectar información para identificar estructuras organizativas y legales de la organización.

   b. Obtener entendimiento de los factores que influyen en la organización para crear y mantener registros.
   c. Entender las actividades del negocio, infraestructuras tecnológicas, riesgos de manejo de activos y accionistas.
2. Análisis de la actividad del Negocio:
   a. Identificar de la organización sus funciones de negocio, actividades y transacciones para identificar cuando, como y donde se realizan dichas actividades.
3. Identificación de necesidades de Record Keeping (Mantenimiento de Registros):
   a. Identificar normativas legales, negocio y otras fuentes de información para identificar los requisitos de evidencia y de información que aplican a la organización.
4. Evaluación de los sistemas existentes:
   a. Evaluar los sistemas actualmente utilizados para llevar a cabo las operaciones de la organización.
   b. Identificar dichos sistemas para identificar brechas en términos de cumplimiento con los requisitos de gestión documental.
5. Identificación de estrategias para la gestión documental:
   a. Definición de estrategias que permiten a los sistemas cumplir con los requisitos de gestión documental
   b. Selección de estrategias que se ajusten a la cultura y entorno de la organización.
6. Diseño de un Sistema de Gestión Documental
   a. Diseñar un sistema de gestión documental que incorpore las estrategias seleccionadas.
7. Implementar un sistema de gestión documental:
   a. Asegurar que todos los componentes del nuevo sistema (o del rediseñado) funcionen de acuerdo con los requisitos establecidos.
   b. Capacitar al personal en el uso de los nuevos sistemas.
   c. Desplegar la tecnología necesaria.
   d. Convertir datos heredados.
   e. Gestionar el cambio organizacional.
8. Revisión posterior a la implementación:
   a. Recopilar información sobre la efectividad del sistema de gestión documental.
   b. Realizar encuestas o entrevistas al personal acerca del sistema.

c. Corregir los problemas identificados.

Como se estipula en este proyecto, los puntos 7 y 8 no serán elaborados en esta investigación; sin embargo, se mantendrán presentes para que el equipo de la Correduría Seguro Total pueda considerarlos en el cumplimiento, desarrollo y monitoreo de la implementación del Sistema de Gestión Documental (SGD).

Figura 7: Proceso Metodología DIRKS



Nota: Información obtenida de Cárdenas Giler, Wilches Medina, Peñate Santana & Lozada Núñez, 2018).

2.5.2.2 METODOLOGÍA NIST MARCO DE CIBERSEGURIDAD

El diseño del Sistema Digital de Gestión Documental se apoya en el marco NIST de Ciberseguridad, el cual de manera general aporta las referencias o guías de Identificar, Proteger, Detectar, Responder y Recuperar como ejes principales para que el sistema de gestión documental contemple la gestión de riesgos y la protección de la información en entornos digitales y físicos.

Como base para este proyecto y considerando que la empresa objetivo del caso Seguro Total Correduría de Seguros es catalogada como una MiPyme del rubro de servicios profesionales, la investigación se apoya de la Guía de inicio rápido para pequeñas empresas del Marco de Seguridad Cibernética 2.0 del NIST. Ver Anexo 2

El Marco de Ciberseguridad del NIST (National Institute of Standards and Technology),

fue desarrollado por el Departamento de Comercio de los Estados Unidos, el cual es reconocido internacionalmente como una guía para la gestión de riesgos cibernéticos, siendo un pilar fundamental para apoyar a las organizaciones a poder identificar, analizar y reducir riesgos asociados a la seguridad digital de la información (National Institute of Standards and Technology, 2024).

Aunque este marco, como se indica anteriormente es reconocido a nivel internacional, su implementación es de carácter voluntario y en el caso de Honduras aún no se ha considerado como base normativa en términos de la gestión de la seguridad. Esto es de gran importancia debido a que como menciona la empresa Crodwstrike en su reporte de amenazas estas se están modernizando, lo que causa que la actualización e identificación de brechas digitales sea fundamental.

Por esta razón, la utilización de este marco como apoyo para el desarrollo de la investigación potencia el diseño del sistema de gestión documenta, al adherirse a estándares ya establecidos y a mejores prácticas

Según el National Institute of Standards and Technology (2024) las acciones generales de Gobernar que se deben considerar son las siguientes:

1. Entender:
    a. Comprender cómo los riesgos cibernéticos afectan el cumplimiento de su misión como organización.
    b. Comprender la existencia de requisitos legales, normativos y contractuales en materia de seguridad cibernética.
    c. Comprender y establecer quién es el responsable de elaborar y ejecutar la estrategia de seguridad cibernética.
2. Evaluar:
    a. Evaluar el impacto potencial de una pérdida total o parcial de los activos y operaciones críticas del negocio.
    b. Evaluar si la adquisición de un seguro cibernético es adecuada para su empresa.
    c. Evaluar riesgos de seguridad cibernética que plantean los proveedores y otros terceros antes de entablar relaciones formales.
3. Establecimiento de Prioridades:
    a. Darle prioridad a la gestión de riesgos de seguridad cibernética junto con otros riesgos empresariales.
4. Comunicación:
    a. Comunicar el apoyo de la dirección de la empresa a una cultura consciente de

riesgos, ética y mejora continua.

b. Comunicar, aplicar y mantener políticas para gestionar riesgos de seguridad cibernética.
c. Establecer el contexto organizativo.

De la misma forma el National Institute of Standards and Technology (2024) establece en sus ejes principales las siguientes acciones que se deben tener en consideración:

1. Identificar:
    a. Comprender qué activos confía o mantiene su empresa creando un inventario de hardware, software, sistemas y servicios.
    b. Evaluar activos informáticos y físicos en busca de posibles vulnerabilidades.
    c. Evaluar la eficacia de un programa de seguridad cibernética de la empresa para identificar qué áreas necesitan mejoras.
    d. Priorizar el inventario y la clasificación de sus datos empresariales.
    e. Priorizar la documentación de las amenazas internas y externas a la seguridad cibernética y las respuestas asociadas mediante un registro de riesgos.
    f. Comunique los planes, las políticas y las mejores prácticas de seguridad cibernética a todo el personal y a los terceros pertinentes.
    g. Comunique al personal la importancia de identificar las mejoras necesarias en los procesos, procedimientos y actividades de gestión de riesgos de seguridad cibernética.
2. Proteger:
    a. Comprenda a qué información deben tener o tienen acceso los empleados. Restrinja el acceso a la información sensible sólo a aquellos empleados que la necesiten para realizar su trabajo.
    b. Evalúe la puntualidad, la calidad y la frecuencia de la capacitación en materia de seguridad cibernética que imparte su empresa a los empleados
    c. Dar prioridad al requisito de autenticación de múltiples factores en todas las cuentas que lo ofrezcan y considerar el uso de gestores de contraseñas para ayudarle a usted y a su personal a generar y proteger contraseñas seguras.
    d. Dar prioridad al cambio de las contraseñas predeterminadas del fabricante.
    e. Priorice la actualización periódica y la aplicación de parches en el software y los sistemas operativos. Active las actualizaciones automáticas para recordarlas.
    f. Dé prioridad a la realización periódica de copias de seguridad de sus datos y a la comprobación de estas.

g. Priorizar la configuración de sus tabletas y portátiles para activar el cifrado de disco completo para proteger los datos.
h. Comunique a su personal cómo reconocer ataques comunes, informar sobre ataques o actividades sospechosas y realizar tareas básicas de higiene cibernética

3. Detectar:
    a. Comprenda cómo identificar indicadores comunes de un incidente de seguridad cibernética
    b. Evalúe sus tecnologías informáticas y servicios externos en busca de desviaciones del comportamiento esperado o típico.
    c. Evalúe su entorno físico en busca de signos de manipulación o actividad sospechosa.
    d. Dé prioridad a la instalación y el mantenimiento de software antivirus y antimalware en todos los dispositivos de la empresa, incluidos los servidores, las computadoras de escritorio y las portátiles.
    e. Contrate a un proveedor de servicios para monitorear computadoras y redes en busca de actividad sospechosa si no cuenta con los recursos para hacerlo internamente.
    f. Comunicarse con su encargado de incidentes autorizado, sobre los detalles pertinentes del incidente para ayudarlos a analizarlo y mitigarlo.
4. Recuperar:
    a. Comprenda cuál es su plan de respuesta a incidentes y quién tiene autoridad y responsabilidad para implementar los diversos aspectos del plan
    b. Evalúe su capacidad para Responder a un incidente de seguridad cibernética.
    c. Evalúe el incidente para determinar su gravedad, lo sucedido y su causa raíz.
    d. Dé prioridad a la adopción de medidas para contener y erradicar el incidente a fin de evitar daños mayores.
    e. Comunique un incidente de seguridad cibernética confirmado a todas las partes interesadas internas y externas, como ser los clientes, socios comerciales, organismos encargados de hacer cumplir la ley, organismos reguladores, según lo exijan las leyes, las regulaciones, los contratos o las políticas.

2.6 INSTRUMENTOS UTILIZADOS

2.6.1 INSTRUMENTOS DIRKS

Como se mencionó anteriormente, la metodología DIRKS expone una serie de pasos fundamentales para la implementación de un sistema de gestión documental, los cuales pueden adaptarse a cualquier tipo o tamaño de organización. Por esta razón, se consideran los instrumentos que la metodología aporta como apoyo para la investigación orientada a la implementación del sistema.

El documento *National Archives of Australia* (2001) proporciona tablas, directrices y mostrando su aplicación mediante el uso de ejemplos ilustrativos que sirven como base metodológica y como instrumentos de referencia. Estos ejemplos nos permiten orientar la elaboración de cuadros de clasificación, tablas de requisitos, matrices de evaluación de sistemas y análisis de riesgos, entre otros insumos necesarios para el desarrollo de la presente investigación. De la misma manera, este documento proporciona preguntas base para la elaboración de entrevistas estructuradas y semiestructuradas y realizar un levantamiento de requerimientos en conjunto con el equipo de la Correduría de Seguro Total. Ver Anexo 3.Detallamos en la siguiente tabla lo que debemos incluir:

Tabla 20: Instrumentos Metodología DIRKS

Instrumento	Finalidad general	Elementos principales
Tabla de requisitos de gestión documental (Recordkeeping requirements)	Registrar de manera estructurada los requisitos legales, normativos o de negocio vinculados a la gestión documental.	Organización, fuente normativa, tipo de fuente, referencia, función/actividad, cita, requisitos derivados (creación, captura, retención, acceso), evaluación de riesgo.
Matriz de evaluación de sistemas existentes	Diagnosticar si los sistemas actuales cumplen con los requisitos de gestión documental e identificar brechas.	Requisito, respuesta (sí/no), brecha detectada.
Tabla de análisis de riesgos	Identificar riesgos documentales y establecer medidas de control.	Acción, consecuencia, decisión, nivel de riesgo.
Estrategias y plan de acción	Definir lineamientos y actividades para implementar o mejorar un sistema de gestión documental.	Estrategia, actividades, responsables, tiempos, indicadores de seguimiento.

Nota: Información obtenida de Nota: Información obtenida de *National Archives of Australia* (2001)

2.6.2 INSTRUMENTOS NIST MARCO DE CIBERSEGURIDAD

El Marco de Ciberseguridad del NIST ofrece como apoyo una serie de matrices y listas de verificación contenidas en la Guía de inicio rápido para pequeñas empresas del Marco de Seguridad Cibernética 2.0. Estas matrices no sólo orientan la aplicación de las cinco funciones del marco (Gobernar, Identificar, Proteger, Detectar, Responder y Recuperar), sino que también sirven como instrumentos metodológicos para la investigación.

> Resulta relevante destacar que dichas herramientas pueden utilizarse como base para diseñar entrevistas estructuradas o semiestructuradas, así como para registrar observaciones directas de los investigadores, complementando la recolección de información necesaria para la construcción del Sistema Digital de Gestión Documental. Ver Anexo 4, Ver Anexo 5.

Encontramos las siguiente matrices y material como instrumentos de apoyo para aplicar esta metodología:

Tabla 21: Instrumentos Metodología NIST

Instrumento NIST	Función CSF	¿Qué es?	¿Cómo se aplica en un SDG?
Lista de contexto organizativo y requisitos legales	Gobernar	Plantilla para documentar misión, riesgos, requisitos legales/normativos.	Sirve para alinear el sistema documental con la misión de la empresa y la normativa que aplica.
Inventario de activos de información	Identificar	Tabla para registrar software, hardware, datos sensibles, responsables y riesgos.	Permite reconocer los documentos digitales, sus custodios y los riesgos asociados (ej. pérdida de acceso).
Lista de autenticación multifactor (MFA)	Proteger	Lista de verificación para saber en qué cuentas críticas está habilitado MFA.	Garantiza protección de cuentas donde se almacenan o acceden documentos sensibles.
Guía de detección de incidentes	Detectar	Indicadores de ataques: accesos fallidos, lentitud, alertas antivirus, correos sospechosos.	Ayuda a definir alertas básicas para Detectar accesos indebidos al sistema documental.
Plan básico de respuesta a incidentes	Responder	Formato para asignar responsables, contactos clave y protocolos de comunicación.	Asegura que la organización sepa cómo reaccionar si hay un incidente en su sistema documental.
Manual de recuperación	Recuperar	Conjunto de procesos para restaurar operaciones y priorizar activos críticos.	Permite restablecer acceso a documentos tras un incidente y aprender de la experiencia.

Nota: Información obtenida de *National Archives of Australia* (2001),

2.7 CONCEPTUALIZACIÓN

1. **Sistema de Gestión documental (SGD):** Conjunto de procesos y herramientas digitales que permiten la captura, almacenamiento, clasificación, consulta y verificación de calidad de documentos (ISO, 2016).

2. **NIST SP 80053 Controles de seguridad y privacidad para sistemas de información:** Catálogo de controles de seguridad y privacidad para sistemas de información y organización. Tiene como fin proteger la confidencialidad, integridad y disponibilidad de la información (National Institute of Standards and Technology, 2020).
3. **Norma ISO 154891:2016**: Norma internacional sobre conceptos y principios para la gestión de documentos. (ISO,2016)
4. **Seguridad de la información:** Protección de la confidencialidad, integridad y disponibilidad de documentos digitales. (ISACA, 2021)
5. **Gobierno de TI:** Marco que permite alinear a TI con objetivos organizacionales, validando la disminución de riesgos y generando valor al servicio. (ISACA, 2022)
6. **Metodología:** Conjunto de principios. Procedimientos, técnicas que guían de manera sistemática la planificación, desarrollo y verificación de un proyecto o una investigación.
7. **Políticas de retención documental**: Reglas sobre cuánto tiempo se debe conservar documentos antes de su eliminación segura y adecuada.
8. **Cumplimiento normativo:** Aplicación de la ley de protección de datos personales y regulación sobre la seguridad en el entorno
9. **Transformación digital en MiPymes**: Adopción digitales para modernizar procesos, mejorar eficiencia operativa y reducir costos operativos en la MiPymes.
10. **Interoperabilidad:** habilidad de los sistemas para comunicarse, intercambio íntegro de datos y trabajar de manera integrada con otras plataformas digitales.
11. **Usuarios finales:** Personas que interactúan directamente con el sistema, siendo responsables de la consulta y gestión de documentos. (Kotler, 2016)
12. **Competencia tecnológica**: empresas o soluciones que ofrecen servicios similares de gestión documental representando alternativas que obligan a la diferenciación (Porter, 2008)
13. **Gestión de servicios de TI**: Conjunto de buenas prácticas que orientan a la entrega operación de servicios de TI con enfoque en valor, agilidad y mejora continua deseada. (ITIL Foundation, 2019)
14. **Confidencialidad:** Propiedad de la información por la que es solo accesible mediante autorizaciones. (ISO/EIC, 2013)
15. **Disponibilidad de la información:** Características que asegura que la información que se solicite sea accesible y utilizable cuando sea requerido. (ISO/IEC 27001, 2013)

16. **Trazabilidad documental:** Capacidad de seguir el rastro de un documento a lo largo de su ciclo desde su creación hasta donde se requiera su disponibilidad (ISO, 2016)
17. **Continuidad del negocio:** Capacidad de una organización para mantener operaciones críticas incluso durante incidentes que afecten la operativa del negocio. (ISO, 2016)

2.8 MARCO LEGAL

2.8.1 MARCO LEGAL (INTERNACIONAL)

En América latina la transformación digital ha avanzado bajo marcos legales que regulan firmemente la protección de datos y el comercio digital, actualmente en países de la región hay muchas regulaciones y normativas que brindan esa seguridad.

2.8.1.1 Reglamento general de protección de datos (RGDP)

El Reglamento General de Protección de Datos (RGPD), también conocido por sus siglas en inglés como General Data Protection Regulation (GPDR) es la normativa que fue creada por la Unión Europea en el año 2016 y que entró en vigor el 25 de mayo de 2018. El RGPD se encarga de regular cómo las organizaciones recopilan, almacenan, procesan datos personales de ciudadanos en la Unión Europea (UE). La RGPD cuenta con principios fundamentales como la licitud, limitación de la finalidad, minimización de datos, exactitud y otros como la integridad y confidencialidad. (Unión Europea, 2016)

El RGPD ha tenido un impacto significativo en América Latina, funcionando como un referente normativo de creación y reforma de las reinstalaciones de cada país basadas en la protección de datos. Dicho esto, este fenómeno ha tenido un impacto gigantesco en los países de la región los cuales lo utilizaron como guía para crear principios como transparencia, minimización de datos, responsabilidad y mejorar esas brechas de seguridad.

Países como LGDP en Brasil (2020), la ley 81 de Panamá (2019) y la data Protection Act de Belice (2021) así como en Chile y Argentina. En las normas las objetivo de garantizar la protección de la información y priorizar las exigencias normativas y para poder gestionar la transformación digital como pilar.

Actualmente a nivel regional existen regulaciones que permiten la ejecución de un sistema digital de gestión documental, dichas regulaciones permiten a los países mantener una línea de calidad del tratamiento de la información y su consumo autorizado.

- Costa Rica

  Ley No 8968(2011): “ley de protección de la persona frente al tratamiento de sus datos personales”.

  Ley que aplica a datos personales en bases automatizadas o manual públicas o privadas, ley que garantiza que la documentación digital de datos personales sea tratada y protegida bajo principios de confidencialidad, minimización y finalidad. (Tribunal Supremo de Elecciones Normativas, 2011)

- Guatemala

  Decreto No 472008: “Ley de reconocimiento de comunicaciones y firmas electrónicas”. Brinda validez legal a documentos firmados electrónicamente reconociendo así, transacciones digitales.

- El Salvador

  Decreto 144,2014: “Ley de protección de datos personales”

  Regula tratamiento de datos personales del sector público y privado, donde se incluye datos sensibles, biométricos y transferencia internacional. Dicho decreto establece un marco claro de cumplimiento, lo que fortalece la seguridad de una digitalización y que va complementado con una reforma de ley especial contra delitos informáticos que endurece y mejora la seguridad del tratamiento de la información.

- Nicaragua

  Ley No 729: “Firma electrónica”.

  Reconoce y brinda valor a la firma electrónica y regula la certificación digital. En los países CA, Nicaragua es el país donde sí existe marco legal pero no se ha implementado en práctica ya que carecen de proveedores acreditados de esta certificación.

- Panamá

  Ley No 81: “protección de datos personas”.

  Regula el tratamiento de datos por entidades públicas aun de manera internacional, esto reforzado con la ley 51 de comercio electrónico donde se le reconoce el valor jurídico de documentos electrónicos de manera digital.

De igual manera algunos países latinoamericanos brindan leyes que ayudan a la comprensión y el manejo adecuado de la información.

Tabla 22: Resumen Marco Legal Internacional

País	Marco legal	Alcance
Brasil	Ley 11.419 Ley 11.063	Reconoce documentos electrónicos con evidencia

País	Marco legal	Alcance
		adecuada. Brasil cuenta con un modelo llamado ICP Brasil que regula la infraestructura de certificación digital. (Tecalis, 2025)
Argentina	Ley 25.506 Decreto 743/2024	Distingue entre firma digital y electrónica sumado al decreto 743 que permite una certificación remota reforzando la autenticidad de la información. (Edicom, 2024)
Chile	Ley 19.799/2003	Brinda validez jurídica de la firma electrónica avanzada. (DanaConnect, 2024)
Colombia	Ley 527/1999 Decreto 2364 Decreto 333/2014	Reconoce la autenticidad de documentos electrónicos y escritos físicos y se cuentan con entidades certificadas. (DanaConnect, 2024)
Perú	Ley 27629/2000	Cuenta con un diferenciador de firmas según seguridad y cuenta con regulaciones para documentos de alto valor legal. (DanaConnect, 2024)

Nota: Información obtenida de (DanaConnect, 2024)

2.8.2 MARCO LEGAL (NACIONAL)

En Honduras existen regulaciones indirectas que pueden servir como mecanismo de iniciación para aplicar nuevas leyes donde se regule legalmente la utilización y el manejo adecuado de información.

2.8.2.1 LEY DE FIRMAS ELECTRÓNICAS

Reconoce la validez jurídica de las firmas electrónicas en Honduras donde crea la figura de prestadores de servicios de certificación que velan por garantizar la autenticidad, integridad y el no repudio al uso de documentos electrónicos y su validez.

Actualmente agentes como el Registro Nacional de las Persona (RNP) y la Secretaría de Gobernación y Justicia (SGJ) han sido actores en la reglamentación y certificación del aplicativo. (La Gaceta, 2013)

2.8.2.2 LEY DE TRANSPARENCIA Y ACCESO A LA INFORMACIÓN PÚBLICA Y SU REGLAMENTO

Establece como derecho a toda persona a solicitar y recibir información pública, esto conlleva a instituciones públicas a proveer proactivamente información básica y establecer oficiales de información y cualquier mecanismo de respuesta que ayude a entregar de manera íntegra y adecuada cualquier información solicitada. (Tribunal Superior de Cuentas, 2014)

2.8.2.3 COMISIÓN NACIONAL DE BANCA Y SEGUROS

La Comisión Nacional de Banca y Seguros presenta facultades regulatorias sobre el sistema financiero y asegurador, sus normas son de carácter regulatorio y obligatorio para aquellas agencias como Bancos, Cooperativas y Aseguradoras.

Actualmente existen normas como:

- Normas para la gestión integral de riesgos tecnológicos y de seguridad de la información: Dicha norma obliga a agencias bancarias como aseguradoras a tener controles de seguridad en la gestión de documentos electrónicos, así como la continuidad del negocio. Esta norma promete preservar la confidencialidad, integridad y disponibilidad de la información. (CNBS, 2022)
- Normas de gobierno corporativo: Dicha norma establece que toda institución debe presentar la información de manera clara y accesible para las políticas internas, auditorías y cualquier solicitud para visualizar información electrónica. (CNBS, 2019)

CAPÍTULO III METODOLOGÍA

3.1 ENFOQUE

Según (Hernández Sampieri, Lucio, & Fernández Collado, 2018) el enfoque de investigación constituye la orientación general que guía al investigador en la manera de recolectar, analizar e interpretar la información con el fin de Responder a las preguntas planteadas. Con base a esto se presenta la siguiente tabla en donde se desglosa por cada objetivo específico de la investigación el tipo de enfoque que aplica para su validación y aplicación.

Tabla 23: Resumen de Enfoques para la aplicación de los Objetivos Específicos

Objetivo Específico	Enfoque	Alcance	Diseño
Analizar los procesos actuales de gestión documental en la MiPyme Seguro Total para identificar riesgos y debilidades en el manejo de PII, contrastándolos con los principios de la ISO 154891:2016 y ISO27001 y el Marco NIST de Ciberseguridad.	Cualitativo	Exploratorio Descriptiva	Estudio de caso
Evaluar herramientas o sistemas existentes que cumplan con los requisitos de las ISO 30301:2019, IS027001 y el Marco NIST de Ciberseguridad que permitan a Seguro Total tener un sistema estandarizado, seguro y escalable.	Mixto	Descriptivo	Estudio de caso/ No experimental transeccional
Diseñar una arquitectura de gestión documental alineada a los estándares de las ISO 154891:2016, ISO 30301:2019 y ISO27001 y bajo el Marco NIST de Ciberseguridad que sea resiliente, accesible y se integre con la gobernanza empresarial de Seguro Total.	Cualitativo	Descriptivo	Estudio de caso
Evaluar y recomendar las funciones y categorías del Marco NIST de Ciberseguridad permiten a la MiPyme Seguro Total mejorar sus procesos actuales de gestión documental.	Mixto	Exploratorio Descriptiva	Estudio de caso/ No experimental transeccional
Identificar y proponer oportunidades de mejora en los procesos de gestión documental, tomando como referencia los requisitos de la ISO 30301:2019, las guías funcionales de la ISO 15489y los controles de seguridad de la ISO/IEC 27001.	Cualitativo	Descriptivo	Estudio de caso

Nota: Elaborada por los autores.

Se define según (Hernández Sampieri, Lucio, & Fernández Collado, 2018) El enfoque cualitativo se basa en métodos de recolección de datos no estandarizados ni número como entrevistas abiertas, observaciones no estructuradas y análisis de documentos, con el propósito de explorar a profundidad fenómenos y comprender significados.

De la misma forma define que los enfoques mixtos "Los enfoques mixtos representan un conjunto de procesos sistemáticos, empíricos y críticos de
investigación e implican la recolección y el análisis de datos cuantitativos y cualitativos, así como su integración y discusión conjunta, para realizar inferencias producto de toda la información recabada (meta inferencias) y lograr un mayor entendimiento del fenómeno bajo estudio.

Considerando los objetivos de la investigación podemos verificar que se tiene un enfoque mixto, ya que poseemos en mayor grado el enfoque cualitativo para determinar observaciones, características y percepciones, así como también, se necesita un enfoque cuantitativo para la obtención de datos en escenarios puntuales.

3.2 ALCANCE

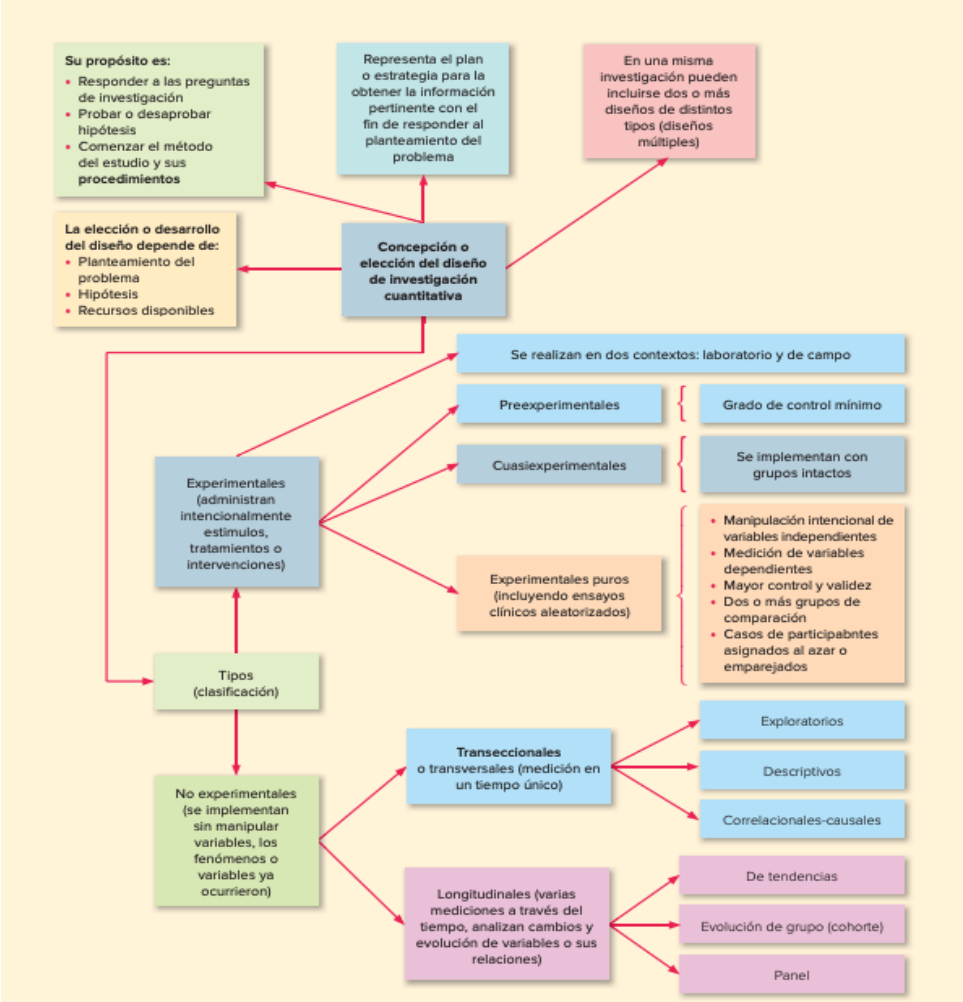
El alcance de una investigación define el nivel de profundidad con que se aborda un problema, pudiendo clasificarse en exploratorio, descriptivo, correlacional o explicativo (Hernández Sampieri & Fernández Collado, 2018). En este estudio se adopta un enfoque exploratorio-descriptivo, ya que combina el análisis inicial de un fenómeno poco abordado en el contexto nacional con la caracterización sistemática de sus procesos.

El carácter exploratorio responde a que la gestión documental en MiPymes del sector asegurador hondureño ha sido escasamente investigada, por lo que se recurre a marcos internacionales como la norma ISO 15489, ISO 27001, y el marco de ciberseguridad del NIST para su abordaje. A su vez, es descriptivo porque busca detallar el estado actual de los procesos mediante herramientas como el FODA, con base en estándares normativos y buenas prácticas en seguridad y manejo de la información.

3.3 DISEÑO

Según Hernández Sampieri & Fernández Collado (2018, p.151) se entiende por diseño como el plan o estrategia concebida para obtener información que se desea y consiste en el esquema o programa que señala lo que se ha de hacer para alcanzar los objetivos y Responder a las preguntas planteadas.

Figura 8: Tipos de diseño y enfoques



Fuente: Hernández Sampieri & Fernández Collado (2018, p.153)

Considerando el concepto y utilidad del diseño, al tener un enfoque mixto se verifica que dentro de los cuantitativos encontramos una serie de tipo como los no experimentales y que según Hernández Sampieri & Fernández Collado (2018, p.152) "se caracterizan porque no se manipulan deliberadamente variables, sino que se observan los fenómenos tal como se dan en su contexto natural para después analizarlos".

De igual manera encontramos los diseños transeccionales donde "se recolectan datos en un solo momento, en un tiempo único. Su propósito es describir variables y analizar su

incidencia en un punto específico del tiempo" (Hernández Sampieri & Fernández Collado, 2018, p.154).

Por otro lado, en los diseños cualitativos se destaca el estudio de caso, el cual se define como "una forma de investigación cualitativa que consiste en analizar a profundidad una unidad de estudio, a fin de comprender sus particularidades y su funcionamiento en un contexto determinado" (Hernández Sampieri & Fernández Collado, 2018, p.493).

En función de lo anterior, el presente trabajo se adopta de mayor manera. un diseño cualitativo basado en el estudio de caso, ya que la investigación promueve un análisis profundo de dos organizaciones aseguradoras, lo cual permite comprender particularidad y funcionamiento con relación a la gestión documental.

Por otro lado, la investigación adopta un diseño cuantitativo no experimental, de tipo transeccional exploratorio-descriptivo, ya que el estudio se centra en observar los procesos de la gestión documental en su contexto natural, sin manipulación de variables y en su único momento temporal. Esto permite describir y analizar de manera óptima riesgos, debilidad y oportunidades de mejora.

3.4 POBLACIÓN

Una población se define como aquel conjunto de individuos y objetos que comparten ciertas características. De la misma forma, esta definición incluye a todo aquel grupo bien definido sobre el que cualquier investigación quiera extraer conclusiones. (Narváez, 2023)

La población de esta investigación se define en función de los actores y elementos que intervienen directamente en los procesos de la correduría de seguros. Se ha considerado a los colaboradores, las compañías aseguradoras con las que mantiene relación y los diferentes tipos de seguros que se comercializan, ya que representan los componentes más críticos del negocio. Esta selección permite que el estudio abarque tanto la perspectiva interna de la organización como la interacción con las aseguradoras y la diversidad de productos ofrecidos, garantizando así un análisis integral y pertinente de la gestión documental.

Tabla 24: Población a realizar investigación y análisis

Dimensión	Población	Desglose Población
Colaboradores	13	4(Directivos) + 9(colaboradores)+ 1(personal de limpieza) + 1 (conductor)

Dimensión	Población	Desglose Población
Compañía Aseguradora	8	Ficohsa Seguros (Interamericana de Seguros), MAPFRE Seguros Honduras, Seguros Atlántida, Seguros Crefisa, PAN American Life, Seguros del País, ASSA Seguros de Honduras Davivienda (Seguros Bolívar de Honduras)
Tipos de Seguros	12	Vida, Gastos Médicos, Accidentes, Saldo de Deuda, Fondo de Pensiones, Asistencia de Viajes Incendio, Equipo Electrónico, Maquinaria, Construcción Fianzas

Fuente: Elaborada por autores

3.5 MUESTRA

La definición de una muestra no probabilística es donde "La elección de las unidades no depende de la probabilidad, sino de razones relacionadas con las características y contexto de la investigación. Aquí el procedimiento no es mecánico o electrónico, ni con base en fórmulas de probabilidad, sino que depende del proceso de toma de decisiones de un investigador o de un grupo de investigadores" (Hernández Sampieri & Fernández Collado, 2018, p.200).

Un muestreo no probabilístico se define como aquel en donde las muestras serán seleccionadas basadas en el conocimiento y la credibilidad del investigador. En donde se debe los investigadores seleccionan aquellos que creen son los adecuados para participar en el estudio de investigación. (Ortega, 2023)

El propósito de la investigación no es alcanzar una representatividad estadística, sino realizar un análisis profundo y pertinente de los procesos de gestión documental y de seguridad de la información. Por ello, se aplicará un muestreo no probabilístico de tipo intencional o por juicio, lo que facilita seleccionar de manera directa a los actores y procesos más vinculados con la problemática, priorizando aquellos que resultan críticos para la operación del negocio.

Dado que la población de estudio se encuentra conformada por un número reducido de colaboradores (directivos y usuarios), así como por un grupo específico de compañías

aseguradoras y tipos de seguros, este enfoque metodológico asegura el acceso a información relevante y especializada. De esta manera, los hallazgos obtenidos se orientan a generar propuestas sólidas y aplicables, alineadas con los estándares internacionales ISO 15489, ISO 30301, ISO 27001 y el Marco NIST de Ciberseguridad, apoyándose también en la Metodología DIRKS, lo que fortalece la pertinencia y utilidad de la investigación para la organización.

Tabla 25: Muestra a realizar estudio de investigación

Dimensión	Población	Muestra	Desglose Muestra
Colaboradores	13	11	4(Directivos) +7(colaboradores)
Compañía Aseguradora	8	2	Ficohsa Seguros y Mapfre Seguros
Tipos de Seguros	12	3	Vida, Gastos Médicos, Automóviles

Fuente: Elaborada por autores

3.6 CRITERIOS DE INCLUSIÓN Y EXCLUSIÓN

Según la publicación (Nikolopoulou, 2023) en la página web de Scribbr los criterios de inclusión y exclusión se definen como aquellos que determinarán que miembros (personas, objetos o procesos) de la población objetivo podrán o no participar en el estudio de investigación.

Para el desarrollo de esta investigación considerando la población general previamente descrita, se han definido criterios de inclusión y exclusión relacionado con los colaboradores, compañías aseguradoras y tipos de seguros. De manera que la investigación se concentre en los elementos más críticos para la aplicación de los instrumentos de recolección de datos. Los cuales se detallan en las siguientes tablas:

Tabla 26: Criterios de inclusión y exclusión

Colaboradores	
Criterios de Inclusión	**Criterios de Exclusión**
El colaborador tiene más de 2 años de experiencia en el rubro de servicios profesionales.	Colaborador no tiene más de 2 años de experiencia en el rubro de servicios profesionales.
El colaborador está graduado como	El Colaborador no cumple con el

Colaboradores	
Criterios de Inclusión	**Criterios de Exclusión**
bachiller a nivel de estudios como requisito de la CNBS.	requisito de estudio como bachiller impuesto por la CNBS
El colaborador está certificado por la CNBS o está en proceso de iniciación de la certificación en el próximo año 2026.	El Colaborador no está certificado por la CNBS o no contempla realizar la certificación para el año 2026.
El colaborador tiene acceso a información sensible o privada de los clientes.	El colaborador no posee la autorización de acceder a información sensible o privada de los clientes.
Colaborar tiene experiencia con herramientas digitales (manejo de herramientas básicas digitales).	El colaborador no posee conocimientos o no utiliza herramientas digitales.
Dominio de la herramienta de almacenamiento de información en la nube Google Drive.	El colaborador no utiliza directamente la herramienta de Google Drive.

Fuente: Elaborada por autores

Tabla 27: Criterios por Compañías Aseguradoras

Compañías Aseguradoras	
Criterios de Inclusión	**Criterios de Exclusión**
La compañía está certificada y autorizada para vender seguros por la CNBS.	La compañía no está autorizada por la CNBS para la venta de seguros.
La compañía desarrolla e implementa la transformación digital al digitalizar procesos que ayudan a las corredurías o agentes individuales.	La compañía no cuenta con herramientas o procesos digitales como apoyo a las corredurías o agentes individuales.
La compañía posee certificaciones internacionales.	La compañía no posee certificaciones internacionales.
La correduría cuenta con alianza y autorización para la venta de seguros de la compañía aseguradora.	La correduría no tiene alianza o autorización de la venta de los productos de la compañía aseguradora.
La compañía representa más del 15% de su cartera activa de la correduría.	La compañía representa un porcentaje menor al 15% de su cartera activa.

Compañías Aseguradoras	
Criterios de Inclusión	**Criterios de Exclusión**
El porcentaje de participación de mercado de la compañía de seguros se sitúa dentro de los primeros 5 lugares en el 2024, aplicado al mercado hondureño.	La compañía no se sitúa en los primeros 5 lugares del ranking de compañías aseguradoras del 2024.

Fuente: Elaborada por autores

Tabla 28: Criterios por Tipo de Seguro

Tipo de Seguro	
Criterios de Inclusión	**Criterios de Exclusión**
El seguro representa más del 20% de la cartera activa.	El tipo de seguro no es del 20% de la cartera activa.
El seguro se presenta como los primeros 3 lugares dentro del reporte del CAHDA con mayor crecimiento en ventas y siniestros.	El seguro no está en las primeras tres posiciones del reporte del CAHDA en crecimiento de ventas y siniestros.
Cantidad de documentos adicionales excluyendo los básicos que son la ID, RTN que genera el documento en caso de siniestros(reclamos)	El seguro no presenta una cantidad alta de documentación extra en cuanto al proceso de venta o de siniestros.

Fuente: Elaborada por autores

3.7 OPERACIONALIZACIÓN DE VARIABLES

Tabla 29: Variables y dimensiones a utilizar

Variable	Definición Teórica	Definición Operacional	Dimensiones	Indicador General	Indicadores Desglosados	Instrumentos
Diseño del sistema digital de gestión documental bajo normas ISO y marco NIST de ciberseguridad.	Conjunto de principios, procesos y técnicas que permiten gestionar documentos de manera eficiente, conforme a la ISO 15489 e ISO 30301 (ISO, 2016).	Adaptación de normas ISO 15489,30301:2019,27001 sobre los procesos actuales de la correduría.	Procesos Actuales de gestión documental Cumplimiento Normativo (ISO 15489, ISO 30301, ISO 27001) Seguridad con base al Marco NIST	Nivel de organización y acceso a documentos (existencia de políticas, trazabilidad y accesibilidad)	Existencia de políticas documentales Existencia de niveles de acceso a la información Existencia de Políticas de Riesgos Existencia de políticas de recuperación Existencia de Procesos Documentados Tiempo de búsqueda de la información Porcentaje de actualización de información Procesos alineados con NIST o ISO.	Guía de entrevista semiestructurada Lista de verificación Observación Matriz de análisis de datos Matriz NIST
Herramientas de Gestión Documental	Plataformas y tecnologías que facilitan el almacenamiento, acceso y control de documentos digitales (ISO, 2016).	Evaluar cómo estas herramientas digitales cumplen y contribuyen a crear un sistema de gestión documental aplicando las ISO 15489,30301:2019,27001 y el Marco	Seguridad Accesibilidad Disponibilidad Funcionalidad Cumplimiento Normativo	Grado de usabilidad y alineación de las herramientas con ISO 30301/16175	Seguridad de la Herramienta Facilidad de Uso Soporte de la Herramienta Adaptabilidad al Negocio Costo Operativos de Implementación	Entrevista semiestructurada Cuestionario abierto Matriz FODA

		NIST de Ciberseguridad.				
Arquitectura de Gestión Documental	La arquitectura de TI es el plan que muestra cómo se construyen, conectan y gestionan los sistemas tecnológicos de una empresa. Incluye reglas y estructuras para que el hardware, el software, los datos y las redes funcionen juntos de forma clara y organizada. (Roivainen, s.f.)	Diseño de una arquitectura de un sistema de gestión documental que se acople a la arquitectura empresarial actual de la correduría.	Integración con arquitectura empresarial Estandarización Seguridad		Nivel de formalización e integración de la arquitectura documental con procesos corporativos	Encuesta tipo Likert
Funciones Guía NIST para Pequeñas Empresas	Desarrollado por el Departamento de Comercio de los Estados Unidos, el cual es reconocido internacionalmente	Adaptar el Marco NIST de Ciberseguridad con base a la Guía para Pequeñas empresas para mejorar la seguridad y	Gobernar Identificar Detectar Responder Recuperar Proteger	Grado de adopción de funciones del NISTCSF en la gestión documental	Cantidad de brechas de seguridad digitales y físicas Existencia de controles de seguridad Identificación de activos	Guía rápida NIST

	como una guía para la gestión de riesgos cibernéticos, siendo un pilar fundamental para apoyar a las organizaciones a poder identificar, analizar y reducir riesgos asociados a la seguridad digital de la información (National Institute of Standards and Technology, 2024).	gestión documental.			críticos(documentos) Conocimiento de seguridad digital de los colaboradores Existencia de un plan de incidentes	
Oportunidades de Mejora Proceso de Gestión Documental	La mejora de procesos son metodologías mediante las cuales un equipo evalúa sus procesos en uso y los adapta con la intención de aumentar la productividad, reducir los costes, simplificar los flujos de trabajo, adaptarse a	Evaluar y recomendar mejores prácticas relacionadas con las ISO 15489,30301:2019,27001 y el Marco NIST de Ciberseguridad.	Procesos Administrativos Procesos Tecnológicos Eficiencia Operativa Accesibilidad Cumplimiento Normativo	Número y relevancia de brechas de mejora identificadas respecto a normas ISO/NIST	Número de requisitos de ISO 30301, ISO y ISO 27001 que no se cumplen actualmente Sugerencias de mejoras Categorización de brechas Optimización de flujos de trabajo Nivel de digitalización Satisfacció	Entrevista semiestructurada Diagrama de procesos Matriz de análisis de datos

	las cambiantes necesidades de negocios o mejorar la rentabilidad (Laoyan, 2025).				n de usuarios internos	

Fuente: Elaborada por autores

3.8 HIPÓTESIS

Variable: Oportunidades de Mejora Proceso de Gestión Documental

La gestión documental es una parte esencial para el buen funcionamiento de una organización, ya que garantiza la disponibilidad, integridad, confidencialidad y disponibilidad de la información durante todo su ciclo de vida. En el caso de las MiPymes del sector de servicios profesionales, la falta de procesos documentales estructurados y adaptados a los estándares internacionales puede generar ineficiencias operativas, riesgos de seguridad de la información y dificultades para cumplir con los requisitos regulatorios y organizativos.

Se entiende por posibilidades de mejora del proceso de gestión documental las brechas, puntos débiles o áreas sujetas a fortalecimiento, que surgen de la evaluación de los procesos administrativos y tecnológicos utilizados con el fin de optimizar la eficiencia operativa, mejorar la disponibilidad de la información, fortalecer el control de seguridad y asegurar el cumplimiento de la legislación. Estas oportunidades se identifican mediante un análisis sistemático de los procesos existentes frente a las buenas prácticas definidas en ISO 15489, ISO 30301, ISO 27001 y el Marco NIST.

En este estudio la variable se procesa desde un enfoque integrado que toma en cuenta tanto los procesos administrativos relacionados con la formalización, estandarización y documentación de los procesos de trabajo, como los procesos tecnológicos relacionados con el uso de herramientas digitales, mecanismos de control, seguridad de la información y niveles de digitalización. También se incluyen factores relacionados con la eficiencia operativa, la disponibilidad de la información y el cumplimiento legal, que son elementos clave para evaluar el desempeño actual del proceso de gestión documental. El análisis de esta variable permite no sólo identificar diferencias existentes entre la práctica actual y los estándares internacionales, sino también obtener insumos objetivos para la formulación de recomendaciones encaminadas

a la mejora continua. De esta manera, las oportunidades para mejorar el proceso de gestión documental se convierten en un eje central en la toma de decisiones y el desarrollo de una estrategia de fortalecimiento alineada con las necesidades organizacionales y los marcos regulatorios.

3.8.1 PLANTEAMIENTO

En el contexto de la gestión documental de la correduría Seguros total, la ausencia de procesos estructurados y estandarizados, el uso limitado de herramientas tecnológicas alineadas con normas internacionales y la falta de controles formales de seguridad de la información generas problemas operativos, dificultados con acceso a la información y riesgos asociados al incumplimiento normativo.

Considerando que al mejora continua de los procesos documentales es un elemento clave para garantizar la eficiencia, seguridad y la sostenibilidad organizacional, resulta necesario analizar las oportunidades de mejora existentes en los procesos documentales, administrativos y tecnológicos de la correduría. Dicho análisis debe realizarse en coherencia con los principios y requisitos establecidos por las normas ISO 15489, 27001 y la 30301 así como el marco NIST de ciberseguridad. En este sentido, la situación actual de la mediación muestra un importante margen de mejora, apoyado en claras oportunidades para fortalecer la gestión documental, reducir las brechas identificadas y reducir los riesgos asociados a la misma, lo que sienta las bases para la implantación de un modelo de gestión documental adaptado a los estándares internacionales.

3.8.2 RESULTADOS OBTENIDOS

En base a la aplicación de instrumentos se logra evidenciar que el proceso de gestión documental presenta una serie de oportunidades de mejora sumamente relevantes que impactan directamente en su eficiencia, confiabilidad y sostenibilidad de la correduría. Estas oportunidades se muestran de manera transversal en la coordinación de las actividades documentales con las operaciones diarias, control y trazabilidad de los documentos, seguridad de la información y la continuidad del negocio.

Se lograr identificar que la gestión documental no se encuentra plenamente integrada con actividades operativas, lo que limita la coordinación interdepartamental y la trasferencia efectiva del conocimiento. Esta situación evidencia una oportunidad de mejora orientada a estructurar la gestión documental como un proceso organizacional alineado a la estrategia interna, en concordancia con los principios establecidos por las normas ISO 15489 e ISO 30301, los cuales promueven una gestión documental estructurada.

En base a los resultados asociados al control, autenticidad, veracidad y trazabilidad de los documentos confirman la existencia de debilidades en la forma en que la documentación es organizada, descrita y clasificada. La ausencia de criterios formales para la gestión de metadatos y la estandarización documental afecta la confiabilidad de la información, reforzando la necesidad de fortalecer estos elementos conforme a los lineamientos que promueve la norma ISO 15489.

Conforma a la seguridad de información, los resultados evidencian oportunidades de mejora en los controles de acceso y protección de los documentos, tanto física como digital. Estas condiciones reflejan un nivel incipiente de madurez en materia de seguridad documental, lo que confirma la pertinencia de adoptar controles alineados a la norma ISO 27001 y a la función Gobernar del marco NIST de ciberseguridad.

Finalmente, los resultados relacionados con la disponibilidad y continuidad de la gestión documental indican la necesidad de fortalecer los mecanismos que garanticen la disponibilidad, recuperación y preservación de la información en caso de incidentes. Esta oportunidad de mejora cumple con los principios de disponibilidad de la norma ISO 15489 y los requisitos de continuidad del negocio de la norma ISO 27001, lo que confirma la importancia de la solidez del proceso documental.

3.9 TÉCNICAS, INSTRUMENTOS Y PROCEDIMIENTOS

3.9.1 TÉCNICAS

Según Hernández Sampieri (2018, p. 217) las técnicas son los procedimientos prácticos utilizados para recolectar datos y obtener información relevante aplicados de acuerdo con el enfoque y el diseño de la investigación. Por otro lado, en la se menciona la investigación cualitativa, donde las técnicas de recolección de datos son flexibles e interactivas, orientadas a captar significados, percepciones y experiencias de los participantes en su contexto natural. (Hernández Sampieri, Fernández Collado & Baptista,2018, p. 385). Entre las técnicas a utilizar, podemos observar:

Entrevista semiestructurada: es una de las prácticas más utilizadas en el proceso de investigación con enfoque cualitativo donde se mide múltiples aspectos de manera más práctica y simplificada. También se define como la combinación de respuestas previamente definidas con flexibilidad para profundizar en los temas según las respuestas del entrevistado (kvale, S. & Brinkmann, 2015).

- Encuesta: es una práctica formal y válida para sustraer información en base a distintos tipos de preguntas adecuadas. También la definen como:
- "La encuesta es un instrumento de investigación que recoge información mediante un cuestionario estandarizado" (Arias, F., 2012, p.75)
- Observación: la observación es una técnica que consiste en el registro sistemático, válido, confiable de comportamiento o hechos manifiestos (Hernández Sampieri, 2018, p. 221).
- Matriz de valoración o checklist: Los instrumentos de tipo lista de verificación o matriz permiten sistematizar la evaluación de un objeto o proceso en función a criterios definidos, facilitando su comparación (Sierra Bravo, R., 2003, p. 321).

3.9.2 INSTRUMENTOS

Según Hernández Sampieri (2018, p.219) los instrumentos son el recurso material que se utiliza para registrar información proporcionada por las técnicas de recolección de datos, con ello podemos definirlo como el recurso necesario para determinar y recolectar información necesaria para el desarrollo de la investigación. En la investigación podemos distinguir instrumentos metodológicos y temáticos.

3.9.2.1 INSTRUMENTOS METODOLÓGICOS

Según Sierra Bravo, R. (2003) son recursos que facilitan la organización, sistematización y análisis de la información mediante técnicas e instrumentos temáticas, asegurando coherencia entre objetivos, variables e interpretación de resultados. Instrumentos metodológicos utilizados para la investigación:

- Matriz de análisis FODA: es un instrumento estratégico que permite identificar fortalezas, oportunidades, debilidades y amenazas de un objetivo de estudio (Weihrich, 1982, p.60). Ver Anexo 6
- Cuestionario de encuesta de tipo Likert: Permite medir actitudes o percepción de grados de acuerdo y desacuerdo, siendo uno de los instrumentos más utilizados en ciencias sociales (Arias, 2012, p. 75).Ver Anexo 7
- Cuestionario semiestructurado: Una entrevista semiestructurada es un método de investigación cualitativa que se utiliza para comprender a fondo los sentimientos y creencias del encuestado sobre temas específicos. A medida que el entrevistador prepara las preguntas con antelación, puede ajustar el orden, omitir las que sean redundantes o crear nuevas. Además, el entrevistador debe estar preparado para hacer preguntas de seguimiento y obtener más detalles. Ver Anexo 8
- Matriz de análisis de datos: Es la herramienta principal que permite el registro de los valores de las diferentes variables con un ordenamiento de la información fácilmente visible, a partir del cual ejecutar los diferentes análisis. Ver Anexo 9
- Diagramas/Mapas de Procesos: Son una representación gráfica de los procesos hechos en una organización donde se colocan los principales autores y pasos a realizar para completar una tarea. (Ekon, 2025) Ver Anexo 10
- Matriz de Evaluación de Herramientas: Es la herramienta principal que permite a los investigadores evaluar según sus criterios establecidos las herramientas disponibles en el mercado para la implementación de un SGD. Ver Anexo 11
- Listas de Verificación ISO: Son aquellos instrumentos metodológicos diseñados para evaluar el grado de cumplimiento de una organización respecto a los requisitos establecidos por la norma, en este caso para la investigación se utilizaron listas de verificación para las ISO 15489,30301 y 27001.Ver Anexo 12, Ver Anexo 13, Ver Anexo 14.

3.9.3 PROCEDIMIENTOS

Según Hernández Sampieri (2018) El procedimiento es la secuencia de pasos que se siguen de manera organizada para aplicar una técnica y recolectar los datos requeridos por la investigación.

Para el desarrollo de la captura de la información se usarán herramientas como Microsoft workspace o papel, con el fin de capturar la mayor información posible en base a las técnicas e instrumentos que se puedan desarrollar, por otro lado, se usarán herramientas como Google Forms o en su derivado Microsoft Forms para la captura en línea de la información necesaria. En base a ello, se realizará en la tabla 29 una breve descripción del proceso a seguir para capturar de la información:

Tabla 30: Instrumentos y procedimientos a realizar

Instrumento	Procedimiento
Cuestionario de encuesta de tipo Likert	● Preparar cuestionario basado en dimensiones de accesibilidad, usabilidad y seguridad de la información. ● Validar instrumento con prueba piloto a gerente de la empresa. ● Aplicar cuestionario a personal seleccionado de la empresa. ● Verificar datos mediante hojas de cálculo y analizador de datos.
Matriz de análisis FODA	● Preparar cuadro de aplicabilidad donde se enmarcan las fortalezas, oportunidades, debilidades y amenazas. ● Aplicar encuesta y captura de información mediante entrevistas, foros controlados y grupos focales donde mediante observación y apuntes se recolecta información.
Cuestionario semiestructurado	● Diseñar una guía de preguntas abiertas como cerradas en la cual se determine la finalidad de la recolección de datos. ● Aplicar cuestionario a público objetivo. ● Registrar y analizar información recolectada. ● Diseñar gráficas y métricas de información obtenida mediante hojas de cálculo y gestores de análisis de

Instrumento	Procedimiento
	datos.
Matriz de análisis de datos	● Verificar información recolectada de los demás instrumentos. ● Validar acorde a variables, dimensiones e importancia para realizar una categorización adecuada. ● Validar patrones e identificarlos para realizar un plan de estudio adecuado. ● Realizar conclusiones y plan de estudio.
Listas de Verificación ISO	● Verificar información recolectada de los demás instrumentos. ● Colocar SÍ/No en la lista y colocar evidencia o comentario
Matriz de análisis de herramientas	● Seleccionar herramientas para el estudio ● Seleccionar dimensiones a medir y asignar pesos ● Validar herramienta seleccionada
Mapas o Flujos de Proceso	● Hablar con los colaboradores y directivos y diagramar los flujos actuales ● Diagramar flujos como propuestas

Fuente: Elaborada por autores.

El fin de la aplicación de estos instrumentos es medir patrones, variabilidades y posibles oportunidades de mejora para la aseguradora.

3.10 FUENTES DE INFORMACIÓN

Las fuentes de información son según (Equipo editorial Etecé, 2025) Las fuentes son aquellos documentos que se consultan para obtener datos de un tema, en el cual los investigadores desean conocer más sobre él. En el cual, en cualquier tipo de investigación académica, escolar o periodística, son el soporte que se usa para producir un escrito u otro tipo de trabajo.

3.10.1 FUENTES DE INFORMACIÓN PRIMARIAS

En esta investigación, las fuentes primarias se entienden como aquellos datos o información que se obtienen de manera directa en el transcurso del estudio de caso de la Correduría Seguro Total. En el cual estas fuentes se generan o recolectan para dar respuesta a las preguntas de investigación, como también a los objetivos específicos de la investigación, permitiendo un análisis directo al caso de estudio.

3.10.2 FUENTES DE INFORMACIÓN SECUNDARÍA

En el marco de esta investigación, las fuentes secundarias corresponden a información previamente elaborada por otros autores u organizaciones internacionales, las cuales sirven de apoyo y brindan mayor contexto al estudio de caso de la Correduría Seguro Total. Estas fuentes incluyen literatura académica, normativas, artículos, informes institucionales y documentos digitales, que permiten contrastar y enriquecer los hallazgos obtenidos de las fuentes primarias. Su función principal es proporcionar un sustento teórico y comparativo que contribuya a validar y complementar el análisis del caso investigado.

3.11 MATRIZ DE CONGRUENCIA

Tabla 31: Matriz de congruencia

No	Pregunta de Investigación	Objetivo	Metodología	Variables	Dimensiones	Indicadores	Instrumentos
1	¿Qué brechas existen en los procesos actuales de la MiPymes de Servicios Profesionales Seguro Total en términos de la gestión documental frente a estándares internacionales como ser la ISO 154891:2016, ISO 27001 y el Marco NIST de Ciberseguridad?	Analizar los procesos actuales de gestión documental en la MiPyme Seguro Total para identificar riesgos y debilidades en el manejo de PII, contrastándolos con los principios de la ISO 154891:2016 y ISO27001 y el Marco NIST de Ciberseguridad.	Cualitativo	Gestión Documental	Procesos Actuales de gestión documental Cumplimiento Normativo (ISO 15489, ISO 30301, ISO 27001) Seguridad con base al Marco NIST	· Existencia de políticas documentales · Existencia de niveles de acceso a la información · Existencia de Políticas de Riesgos · Existencia de políticas de recuperación · Existencia de Procesos Documentados · Tiempo de búsqueda de la información · Porcentaje de actualización de información · Procesos	Guía de entrevista semiestructurada Lista de cotejo y Observación Matriz de análisis de datos

						alineados con NIST o ISO.	
2	¿Qué brechas existen en los procesos actuales de la MiPymes de Servicios Profesionales Seguro Total en términos de la gestión documental frente a estándares	Identificar y proponer oportunidades de mejora en los procesos de gestión documental, tomando como referencia los requisitos de la ISO 30301:2019, las guías funcionales de la ISO	Cualitativo	Oportunidades de Mejora Proceso de Gestión Documental	Seguridad Accesibilidad Disponibilidad Funcionalidad Cumplimiento Normativo	· Número de requisitos de ISO 30301, ISO/TS 161752 y ISO 27001 que no se cumplen actualmente · Sugerencias de mejoras · Categorización de brechas · Optimización de flujos de trabajo · Nivel de digitalizaci	Entrevista semiestructurada Cuestionario abierto Matriz FODA

	internacionales como ser la ISO 154891:2016, ISO 27001 y el Marco NIST de Ciberseguridad?	15489y los controles de seguridad de la ISO/IEC 27001.				ón · Satisfacción de usuarios internos	
3	¿Qué herramientas actuales en el mercado permiten a la MiPyme Seguro Total tener una estructura eficiente, escalable y accesible para implementar un sistema centralizado de gestión documental basado en la ISO	Evaluar herramientas o sistemas existentes que cumplan con los requisitos de las ISO 30301:2019, IS027001 y el Marco NIST de Ciberseguridad que permitan a Seguro Total tener un sistema estandarizado, seguro y escalable.	Mixto	Herramientas de Gestión Documental	Integración con arquitectura empresarial Estandarización Seguridad	· Seguridad de la Herramienta · Facilidad de Uso · Soporte de la Herramienta · Adaptabilidad al Negocio Costo Operativos de Implementación	Encuesta tipo Likert

	30301:201						
4	¿De qué manera la integración de funciones y categorías del Marco NIST de Ciberseguridad, en conjunto con los controles de la ISO 27001, puede reforzar la seguridad y la resiliencia de la información en la MiPym	Evaluar y recomendar las funciones y categorías del Marco NIST de Ciberseguridad permitena la MiPyme Seguro Total mejorar sus procesos actuales de gestión documental	Mixto	Funciones Guía NIST para Pequeñas Empresas	Gobernar Identificar Detectar Responder Recuperar Proteger	· Cantidad de brechas de seguridad digitales y físicas · Existencia de controles de seguridad · Identificación de activos críticos(documentos) · Conocimiento de seguridad digital de los colaboradores Existencia de un	Guía rápida NIST

	e Seguro Total?						
5	¿Cómo una arquitectura documental basada en los principios de la ISO 154891:2016 y los requisitos de la ISO 30301:2019, e integrada con controles de seguridad de la ISO 27001 y el Marco NIST de Ciberseguridad, permite desarrol	Evaluar una arquitectura de gestión documental alineada a los estándares de las ISO 154891:2016, ISO 30301:2019 y ISO27001 y bajo el Marco NIST de Ciberseguridad que sea resiliente, accesible y se integre con la gobernanza empresarial de Seguro Total. .	Cualitativo	Arquitectura de Gestión Documental	Procesos Administrativos Procesos Tecnológicos Eficiencia Operativa Accesibilidad Cumplimiento Normativo	· Nivel de adaptabilidad a la estructura actual · Integración a políticas corporativa · Definición de Roles y Privilegios	Entrevista semiestructurada Diagrama de procesos Matriz de análisis de datos

	lar un sistema seguro y escalable para Seguro Total?						

Fuente: Elaborado por autores

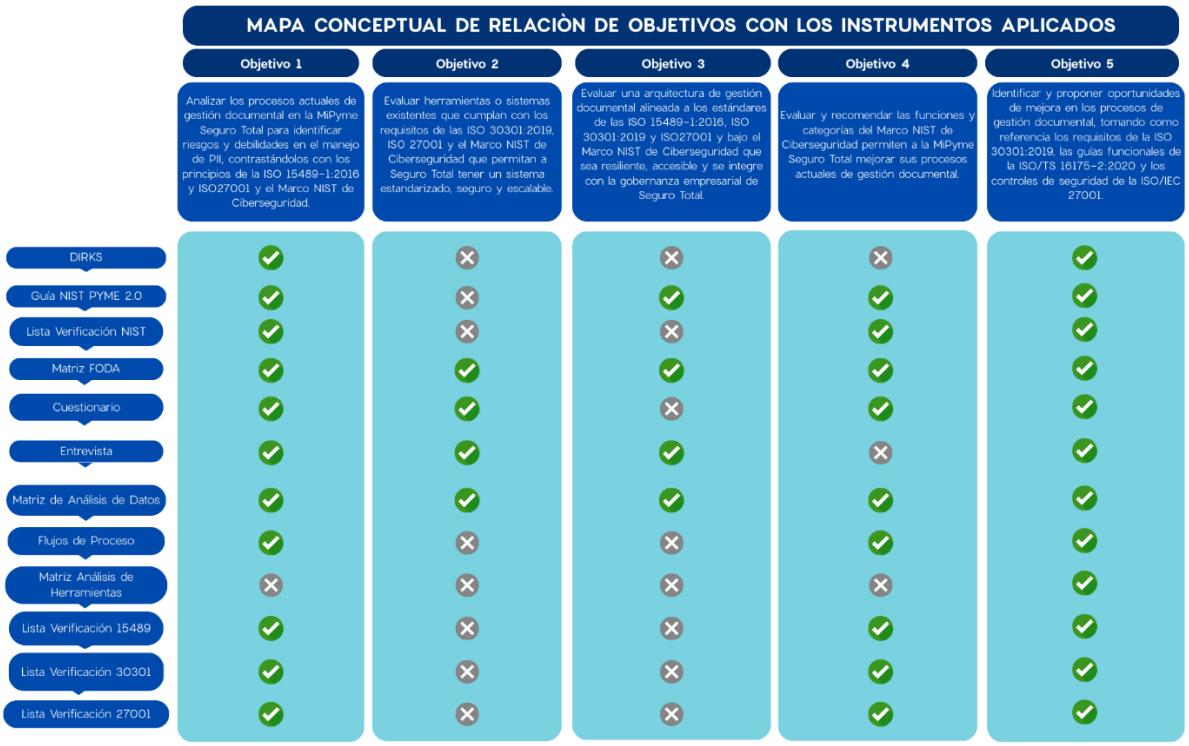
CAPÍTULO IV. RESULTADOS Y ANÁLISIS

En este capítulo se presentan y analizan los datos obtenidos mediante los instrumentos tanto temáticos como metodológicos, aplicados durante el desarrollo del trabajo de investigación del estudio de caso de la Correduría Seguro Total. Estos instrumentos han sido validados por nuestro asesor metodológico M. Sc. Jorge Madariaga y el asesor temático M. Sc. Juan Almendarez asegurando que los mismos contribuyan a obtener información relevante para el análisis de los objetivos específicos definidos para la investigación.

Por la facilidad que ofrece Google Forms, se ha decidido utilizarlo como método para realizar las encuestas a los colaboradores designados. Igualmente, la aplicación de la entrevista se ha realizado presencialmente en la oficina principal de la corredura en Tegucigalpa. Por último, los demás instrumentos se han llenado mediante el análisis, observación y conocimiento del negocio de los investigadores. Estos resultados nos permiten dar respuesta a nuestra pregunta principal de investigación: ¿De qué manera un sistema centralizado de gestión digital de documentación, basado en las Normas ISO y como referencia el Marco NIST de Ciberseguridad, logra contribuir a mejorar la seguridad, accesibilidad y trazabilidad de la información en la MiPymes de servicios profesionales Seguro Total?

La estructura de análisis del capítulo IV se distribuye mediante la descripción, análisis y hallazgos generales mediante la aplicación de los instrumentos para cada uno de los objetivos específicos de la investigación. En la siguiente figura se desglosan como los diferentes instrumentos temáticos y metodológicos que fueron aplicados en la investigación se relacionan con los diferentes objetivos específicos de la misma.

Figura 9: Mapa Conceptual de Relación de Objetivos con Instrumentos Aplicados



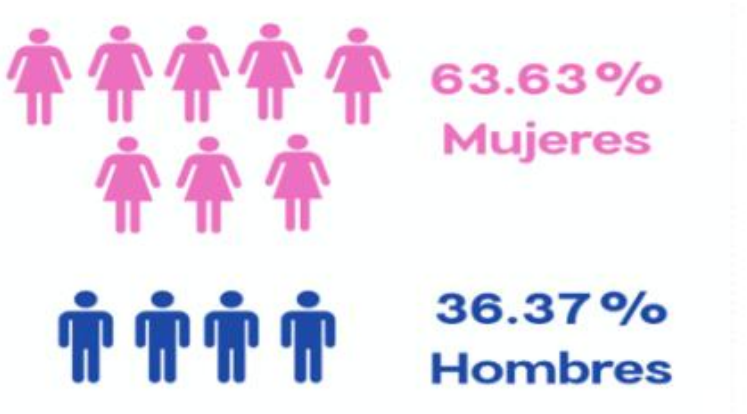
Nota: Elaborada por los autores

4.1 DESCRIPCIÓN GENERAL DE LOS INSTRUMENTOS

En la siguiente sección se describe la muestra o cómo se llenaron los instrumentos de la investigación. Encontramos primero la definición de los identificadores claves de la muestra aplicada al cuestionario, en el cual se aplican preguntas abiertas, cerradas (Si o No), preguntas de conocimiento general y preguntas con estilo de escala de Likert mediante la siguiente asignación de pesos:

- 1: Totalmente en desacuerdo
- 2: En desacuerdo
- 3: Neutral
- 4: De acuerdo
- 5: Totalmente de acuerdo

Figura 10: Distribución por Género

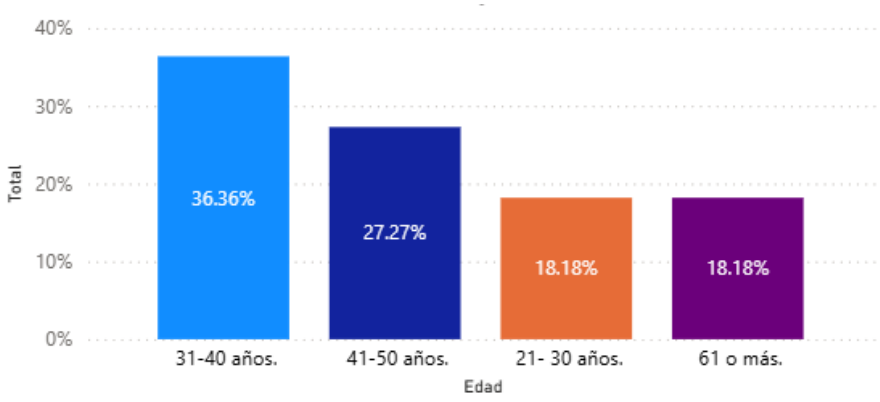


Nota: Elaborado por autores

La población está integrada por 13 colaboradores, luego de la definición y revisión de los criterios de inclusión y exclusión nuestra muestra del cuestionario se desglosa de la siguiente manera: cuatro directivos y siete colaboradores.

La muestra utilizada para la aplicación se puede visualizar en la imagen anterior se compone por siete colaboradores del género femenino y de cuatro hombres equivalentes a un total de 11 colaboradores que cumplieron con los criterios de inclusión y exclusión descritos en el capítulo III, los cuales tienen puesto directivos tanto como funcionales dentro de la organización.

Gráfico 3: Análisis de Distribución por Edad

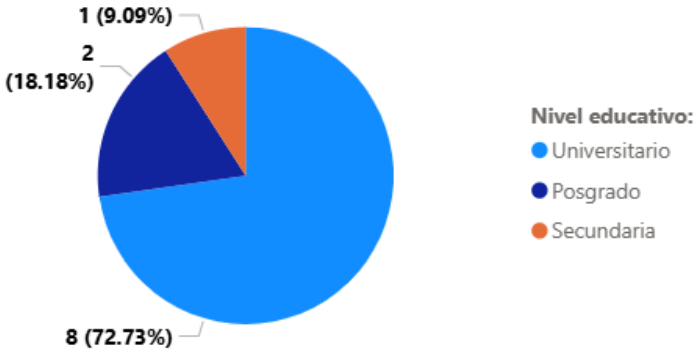


Nota: Elaborado por autores

De manera general podemos ver en la figura de Distribución por Edad que el 63.63% de la muestra se encuentra en un rango de edad de 3150 años, considerando el 36.36% del rango de 31 a 40 años y el 27.27% del rango de 41 a 50 años. Encontramos también el 18.18% entre

2130 años y 18.18% mayor a 61 años.

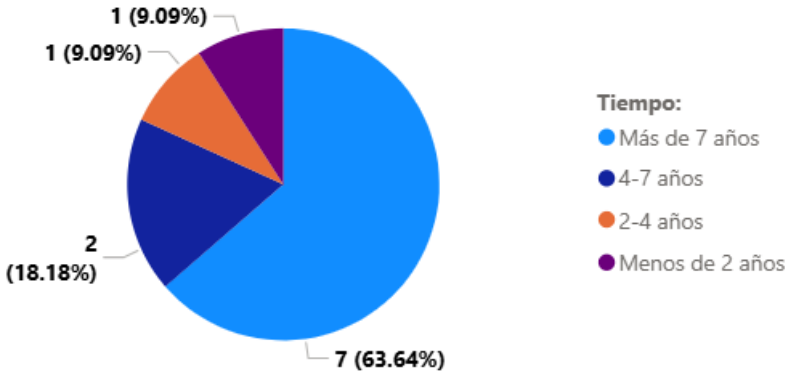
Gráfico 4: Análisis de Distribución por Nivel Educativo



Nota: Elaborado por autores

El 72.73% de los colaboradores posee estudios universitarios de pregrado como nivel máximo de estudio. Con solo un colaborador a nivel académico de secundario 9.09% y dos en estudios de posgrado equivalentes al 11.8.18%.

Gráfico 5: Tiempo de trabajar en la organización



Nota: Elaborado por autores

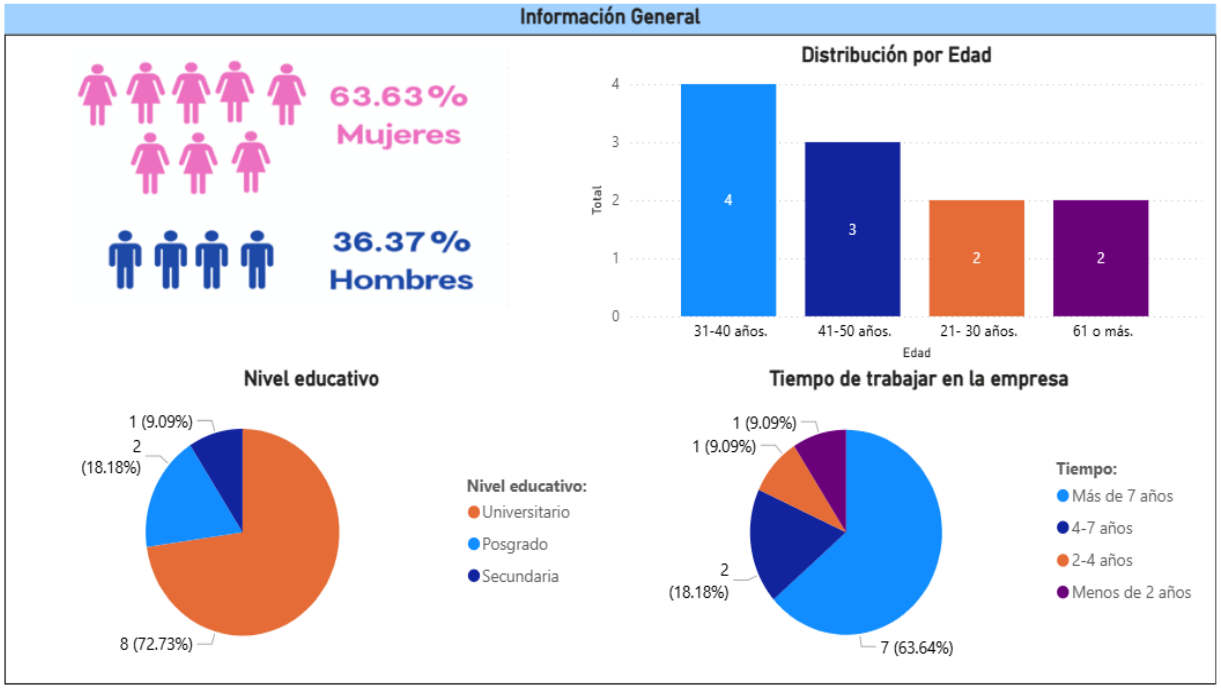
Podemos ver también que el 81.82% de los colaboradores tiene más de 4 años de laborar en la organización consideran los siete con más de siete años (63.64%) y dos con entre cuatro y siete años (18.18%) lo que muestra que los colaboradores tienen amplia experiencia en el rubro de servicios profesionales. Vemos también un colaborador (9.09%) entre dos a cuatro años y uno con menos de años (9.09%) dentro de la correduría.

Ha sido aplicada a los directivos de la organización para entender de qué manera sus directivos ven la situación actual de la gestión documental y hacia dónde quieren llevarla con base en su misión, visión y objetivos estratégicos. La misma fue aplicada a la Gerente General y Gerente de Operaciones del género femenino (50%) y a los gerentes de Mercadeo y Seguros

Nacionales del género masculino (50%).

La información de los instrumentos como ser las listas de verificación de las ISO 15486, 30301 y 27001 se han completado mediante la misma información obtenida de los instrumentos de la entrevista, cuestionario, observación y pláticas que los investigadores sostuvieron con los diferentes colaboradores durante las visitas físicas a la oficina principal de la correduría en la ciudad de Tegucigalpa. Esto mismo aplica para los instrumentos temáticos como ser del DIRKS, Guía NIST para Pymes 2.0, Flujos de Procesos, FODA y la lista de verificación del Marco NIST.

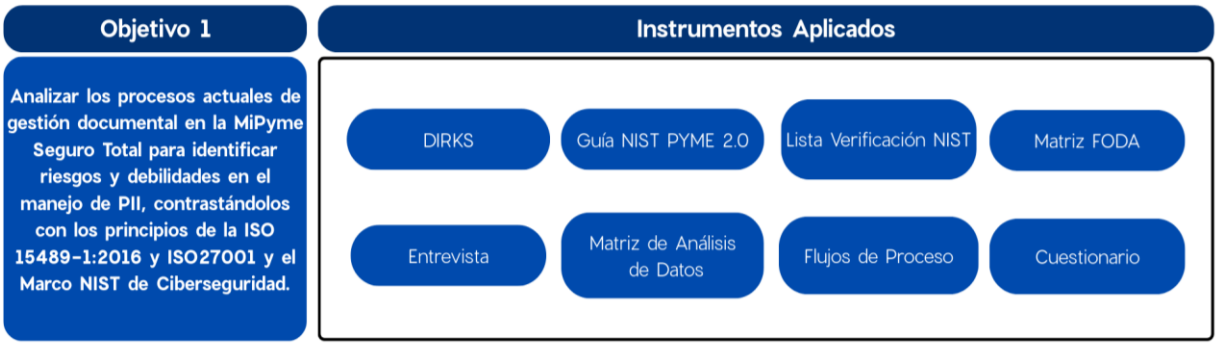
Figura 11: Información general de muestra del cuestionario



Nota: Elaborado por autores

4.2. ANÁLISIS DE LA GESTIÓN DOCUMENTAL Y SEGURIDAD DE LA INFORMACIÓN EN LA CORREDURÍA SEGURO TOTAL

Figura 12: Instrumentos aplicados relacionados al Objetivo 1



Nota: Elaborada por los autores

Como se muestra en la imagen anterior estos son los instrumentos que fueron utilizados para dar respuesta al objetivo 1 el cual consistente en: Analizar los procesos actuales de gestión documental en la MiPyme Seguro Total para identificar riesgos y debilidades en el manejo de PII, contrastándolos con los principios de la ISO 154891:2016 y ISO27001 y el Marco NIST de Ciberseguridad.

4.2.1 DESCRIPCIÓN DEL PROCESO DOCUMENTAL ACTUAL

Actualmente en la correduría se sigue el siguiente proceso para el alta de un cliente:

1. Contacto inicial

El cliente se comunica con el vendedor a través de WhatsApp, llamada, correo electrónico o mediante una visita presencial a la oficina o donde el cliente decida, para entender la necesidad inicial del servicio.

2. Levantamiento de información básica

El vendedor confirma qué tipo de seguro necesita el cliente y recopila datos generales como:

- Nombre completo
- Número de identidad
- RTN

3. Cotización con aseguradoras

El vendedor realiza la cotización en tres compañías diferentes. Para obtener la información:

- A veces ingresa directamente a la plataforma de la aseguradora, o
- Solicita la cotización por correo o a la aseguradora correspondiente.

4. Recepción de las cotizaciones

El vendedor recibe las propuestas de cada aseguradora y las envía al cliente.

5. Acompañamiento y asesoría

El cliente revisa las opciones y el vendedor brinda soporte con dudas, diferencias de coberturas, beneficios o condiciones.

6. Confirmación y envío de documentos del cliente

Cuando el cliente elige la aseguradora:

El cliente envía por WhatsApp o correo las imágenes de los documentos solicitados, según el tipo de seguro:

- Identidad (ID) y RTN
- Gastos médicos: registros médicos o diagnósticos previos en caso de enfermedades existentes
- Seguro vehicular: licencia, documentos del vehículo y, si es importado, fotografías detalladas
- Otros documentos solicitados según la póliza

7. Solicitud del medio de pago

El vendedor coordina con el cliente el método de pago:

- Botón de pago
- Transferencia bancaria

Una vez recibido el comprobante, se comparte la información a la aseguradora.

8. Emisión del documento oficial

El vendedor envía toda la documentación a la aseguradora.

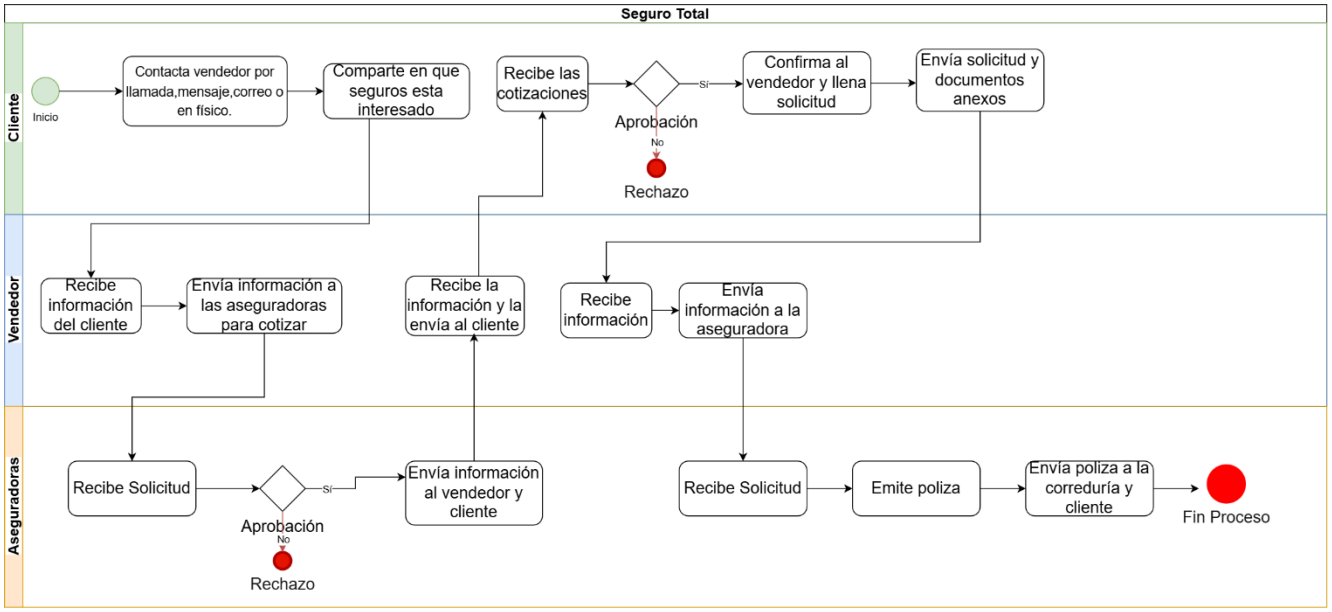
La aseguradora procesa la solicitud y emite el documento oficial de la póliza.

9. Entrega final al cliente

El vendedor comparte la póliza final al cliente y confirma que la información esté correcta.

10.Los documentos se descargan y se almacenan en los archiveros físicos de la empresa y todo lo digital queda en los correos y WhatsApp personales los cuales son números corporativos.

Figura 13: Mapa de Proceso Actual de Alta de pólizas

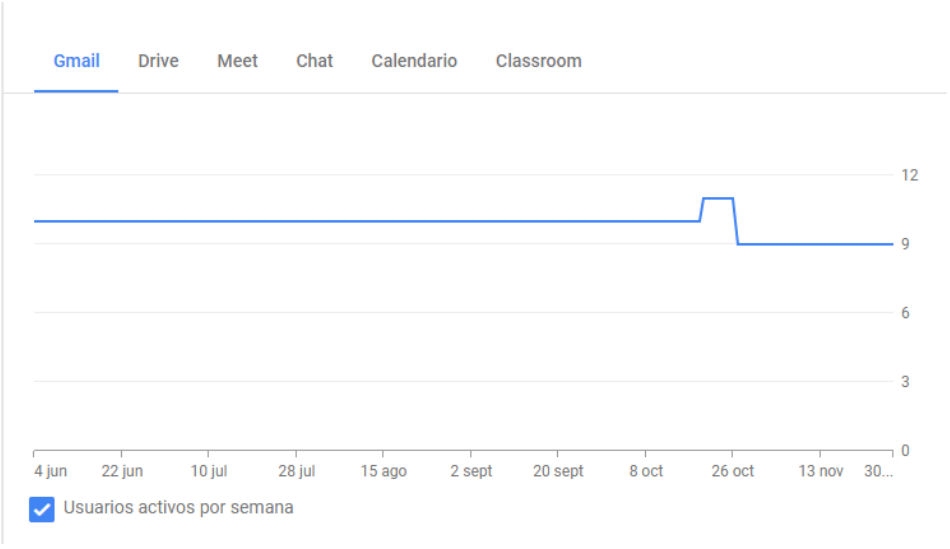


Nota: Elaborado por los autores

4.2.2 ANÁLISIS DE APLICACIONES EXISTENTES

Como parte integral de la investigación se comparten los siguientes gráficos uso el uso actual de Gmail y Google Drive, el cual es la base de la gestión documental digital de la correduría. Nos enfocamos en estas aplicaciones ya que la gestión física de documentos como se ha mencionado anteriormente se basa en la descarga de toda la información recibida por correo, WhatsApp o copias de documentos y se almacenan según el tipo de seguro y en orden alfabético en archivos físicos. En donde también al tener demasiadas copias físicas las mismas se gestiona mediante la empresa Ransa para almacenar dichos documentos muy antiguos o pólizas inactivas.

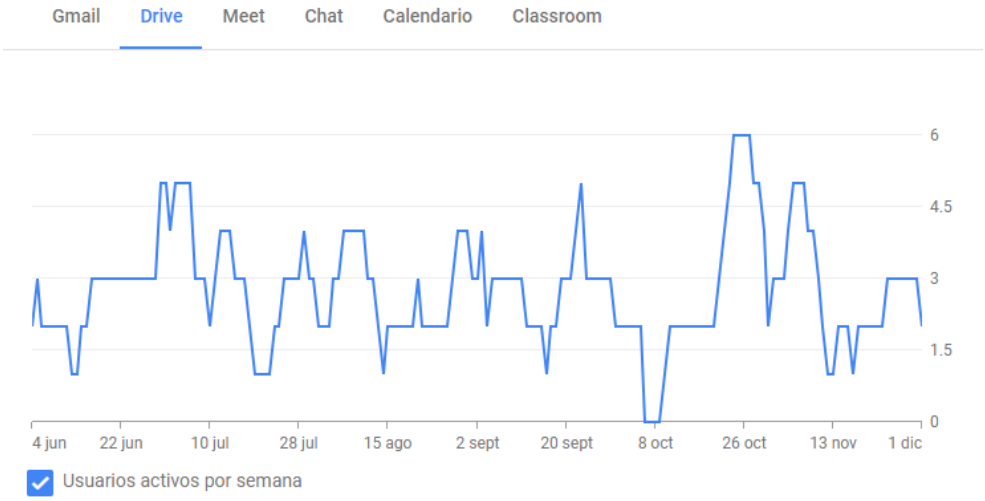
Gráfico 6: Análisis de Uso de Gmail



Nota: Obtenida de la consola de administración de G Suite de la correduría

Podemos ver en este gráfico que en promedio considerando el último semestre del año del 2025 nueve de los trece usuarios creados en G Suite utilizan la aplicación de Gmail de forma diaria. Este dato es interesante ya que, no todos los usuarios están utilizando los correos institucionales asignados por lo cual se debe validar que correos están utilizando para compartir información confidencial de la empresa y forzar el uso del correo institucional para asegurar la integridad y seguridad.

Gráfico 7: Análisis de Uso del Drive



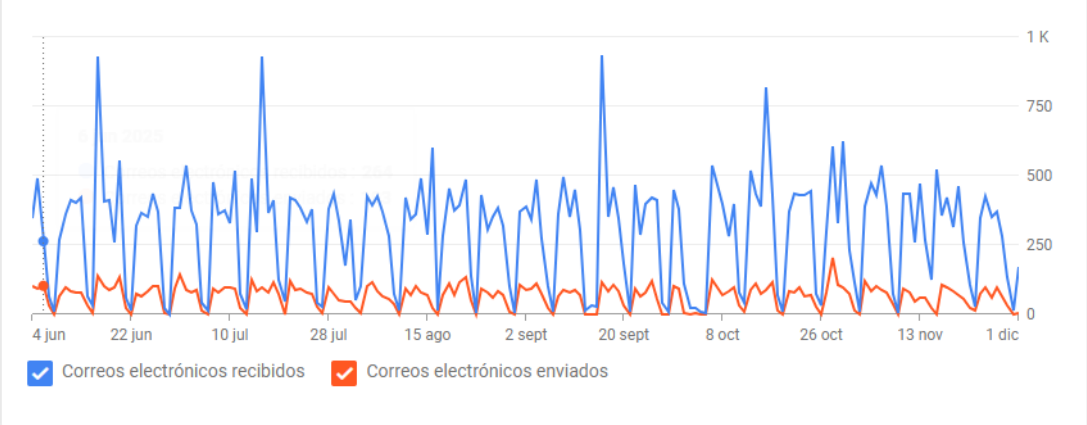
Nota: Obtenida de la consola de administración de G Suite de la correduría

Mediante este gráfico podemos ver que el promedio diario de usuarios que usan la herramienta de Google Drive es muy bajo siendo tres, con un pico máximo de seis usuarios y cero en algunas fechas. Esto es un indicador clave ya que nos demuestra que no se están almacenando las copias digitales de los documentos dentro del Drive y con base a las

observaciones hechas y platicas sostenidas en las visitas a la oficina principal contradice el uso de Google Drive como un SGD para la correduría.

Considerando estos gráficos es importante que entremos más a fondo para entender el uso actual de las diferentes aplicaciones para tener una mejor visión de si se están aprovechando y utilizando de manera eficiente las mismas.

Gráfico 8: Análisis de Entradas y Salidas de correos en Gmail



Nota: Obtenida de la consola de administración de G Suite de la correduría

Mediante el siguiente gráfico podemos ver que el promedio de correos que la correduría recibe y envía. De forma general podemos ver que el gráfico marca una tendencia promedio entre 250 y 500 correos recibidos diarios, con picos de más de 900 correos en fechas específicas. Para un mejor análisis se ha calculado los correos promedios mensuales recibidos que se pueden visualizar en la siguiente tabla:

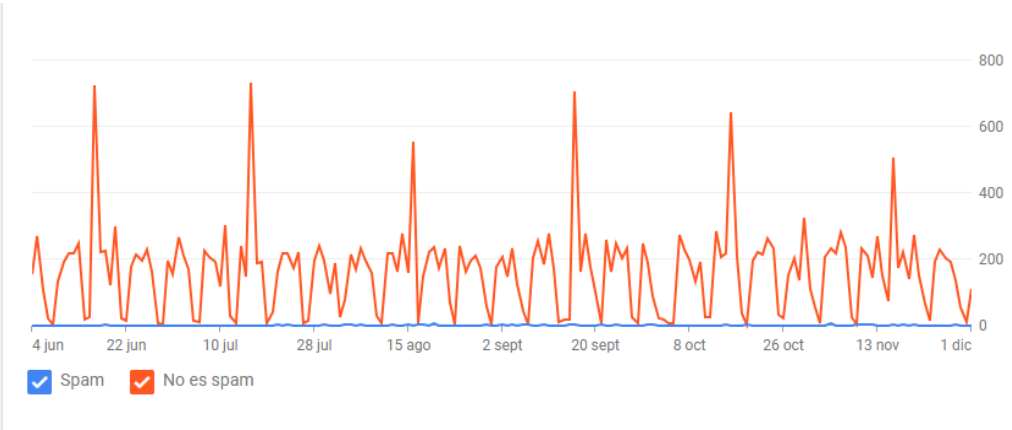
Tabla 32: Análisis de correos enviados y recibidos

Mes	Total, Recibidos	Total, Enviados	Promedio Diario Recibidos	Promedio Diario Enviados
2025-06	8,039	1,882	297.74	69.70
2025-07	9,813	2,223	316.55	71.71
2025-09	9,166	1,916	305.53	63.87
2025-10	9,340	1,986	301.29	64.06
2025-11	8,812	1,763	293.73	58.77

Nota: Elaborada por los autores

Vemos un alto nivel de correos recibidos de forma mensual lo que resalta el punto mencionado tanto por colaboradores y directivos de la correduría en donde la base de la gestión documental se realiza en la aplicación de Gmail, por lo cual se evidencia que no existe un gestiona adecuada de los documentos y no utilizan Google Drive para tener una estructura de almacenamiento de documentos. De la misma forma, esto demuestra el bajo uso de Google Drive dentro de la correduría y la dependencia en Gmail utilizando su buscador para encontrar archivos específicos sin un orden o control asociados.

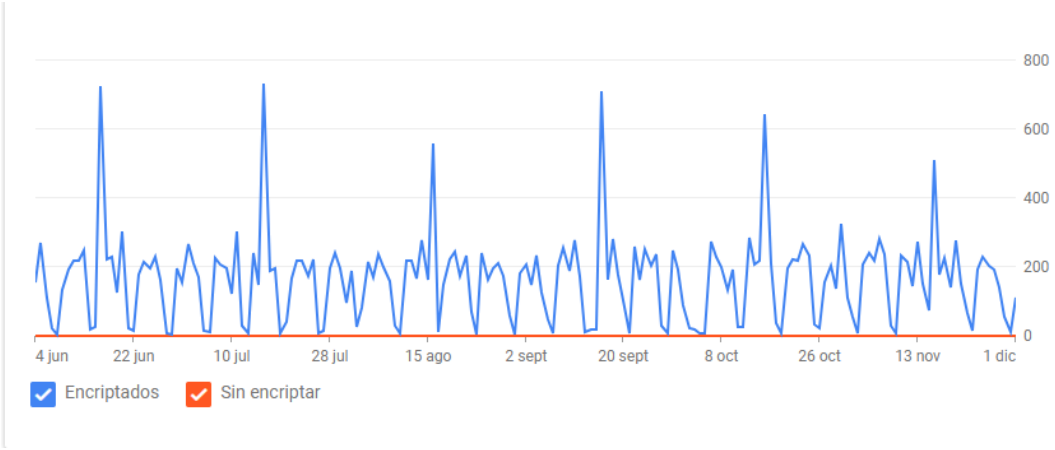
Gráfico 9: Análisis de Spams Recibidos



Nota: Obtenida de la consola de administración de G Suite de la correduría

En este caso se observa que las cuentas institucionales de Gmail reciben una cantidad prácticamente nula de correos no deseados, el cual se representa por la línea azul. De la misma forma, vemos que el promedio de correos que no son spam mantiene un volumen promedio entre cero a 200 correos. Esto constituye un indicador positivo, ya que sugiere que dichas cuentas no están siendo utilizadas en sitios web, suscripciones o plataformas externas que normalmente generan un mayor volumen de spam

Gráfico 10: Análisis de Encriptación de correos



Nota: Obtenida de la consola de administración de G Suite de la correduría

El gráfico nos muestra que existe un promedio bajo de correos encriptados que recibide la correduría en donde se ve que es menor a 200 correos recibidos que corresponde a la línea azul. De la misma forma, podemos ver que los correos sin encriptar recibidos son cero para la correduría.

Tabla 33: Análisis de correos encriptados recibidos

Mes	Promedio Diario de Correos Recibidos
2025-06	297.74
2025-07	316.55
2025-09	305.53
2025-10	301.29
2025-11	293.73

Nota: Elaborada por los autores

En este caso, a diferencia de la gráfica anterior que muestra el volumen total de correos recibidos, vemos un bajo promedio de correos encriptados que recibe la correduría. Esto puede deberse a varios factores. El más común es que no todos los servidores remitentes usan protocolos seguros como TLS para el envío, por lo que algunos correos llegan sin cifrado en tránsito. Otra posibilidad es que ciertos servicios o plataformas externas no soporten o no tengan habilitado el cifrado entre servidores.

Gráfico 11: Archivos compartidos de forma externa

Nota: Obtenida de la consola de administración de G Suite de la correduría

El gráfico muestra que, durante todo el periodo analizado, no se registraron archivos compartidos de forma externa bajo ninguna de las modalidades disponibles (público, usuarios con enlace o dominios externos). Esta ausencia total de actividad indica que la información institucional no está siendo divulgada fuera del dominio, lo cual reduce significativamente el riesgo de exposición no autorizada y sugiere un uso restringido de la publicación de archivos de Google Workspace.

Sin embargo, este comportamiento también puede reflejar la falta de lineamientos claros para compartir documentos, un uso limitado de prácticas colaborativas controladas o la preferencia por canales alternos como correo personal o mensajería instantánea, lo que sí podría representar un riesgo. En conjunto, los datos evidencian tanto un nivel bajo de exposición externa positivo para la seguridad como una oportunidad para fortalecer políticas, procesos y capacitación en gestión documental y uso adecuado de herramientas digitales.

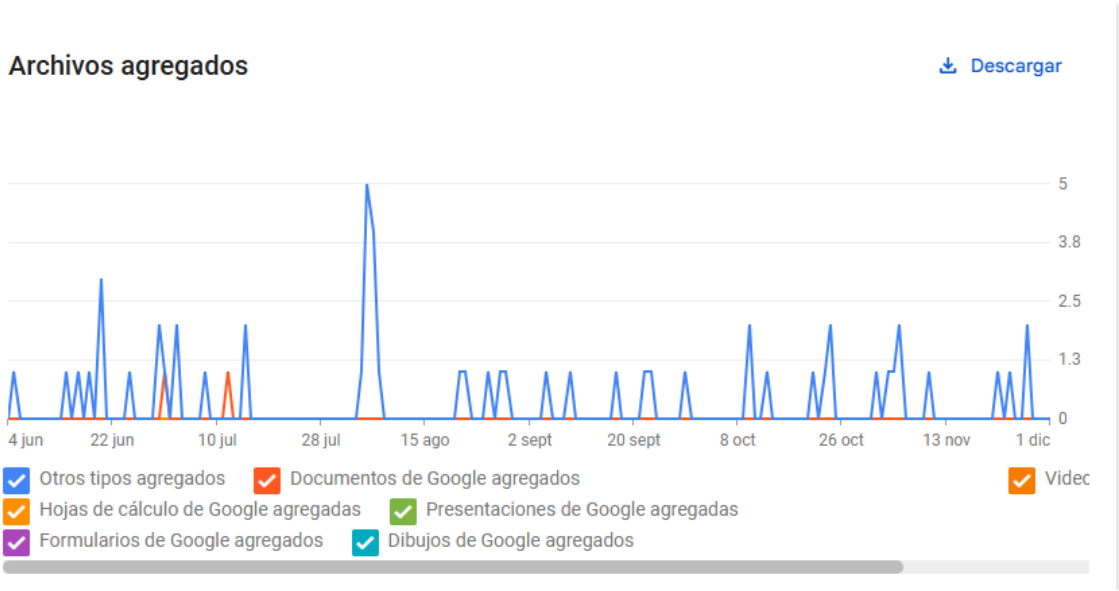
Gráfico 12: Archivos compartidos de forma interna

Nota: Obtenida de la consola de administración de G Suite de la correduría

El gráfico muestra la actividad de archivos compartidos internamente bajo la modalidad "Cualquier miembro del dominio que tenga el vínculo". Se observa una frecuencia baja de documentos compartidos entre los miembros pertenecientes al dominio del correo de la correduría. Este comportamiento indica que los colaboradores no utilizan el método de compartir mediante enlace interno, lo que dificulta la colaboración y el acceso a la información dentro de la organización.

Eso evidencia también la ausencia de controles más granulares o restricciones basadas en roles, algo que sería recomendable desde la perspectiva de gestión documental e ISO 27001. Aunque estos accesos no representan un riesgo externo, sí pueden limitar la trazabilidad sobre quién accede, modifica o distribuye documentos.

Gráfico 13: Archivos agregados al Google Drive



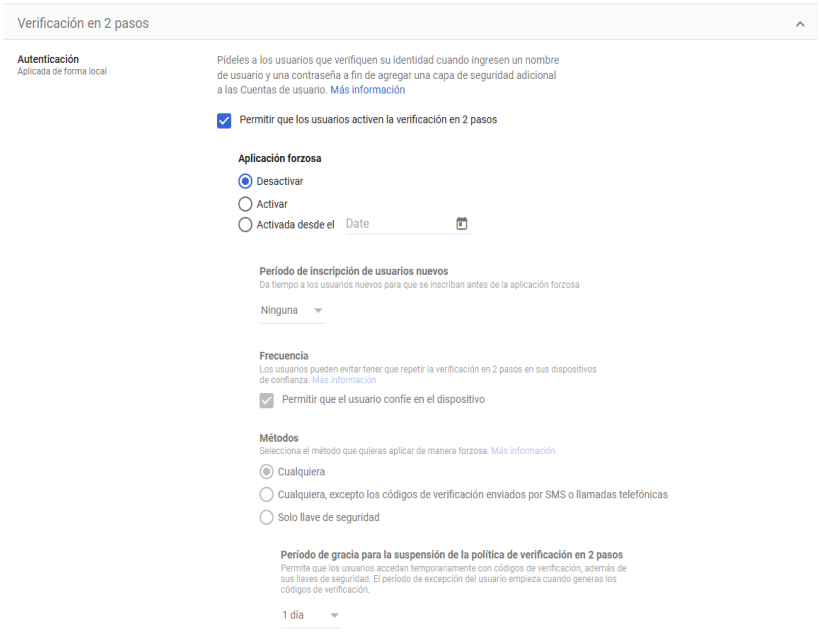
Nota: Obtenida de la consola de administración de G Suite de la correduría

El gráfico muestra el comportamiento de los "archivos agregados" en Google Workspace, donde se observa una actividad baja a lo largo del periodo analizado. Se identifican picos bajos o ningunos, lo que demuestra el bajo uso de Google Drive al promediar menos de un documento y el pico más alto entre el 28 de julio y el 15 de agosto de apenas cinco documentos.

La baja cantidad de documentos agregados indican que los colaboradores no utilizan de forma continua la plataforma para almacenar o incorporar nuevos documentos. Sin embargo, también revela una falta de estandarización en el uso de plantillas y tipos de archivo, lo que puede afectar la homogeneidad documental y la trazabilidad. En conjunto, los datos evidencian un bajo crecimiento o nulo de la información sin un control formal del ciclo de vida documental,

lo que representa una oportunidad para fortalecer políticas de clasificación, ordenamiento y conservación según los lineamientos de ISO 15489.

Figura 14: Configuración de MFA G-Suite Consola de administración



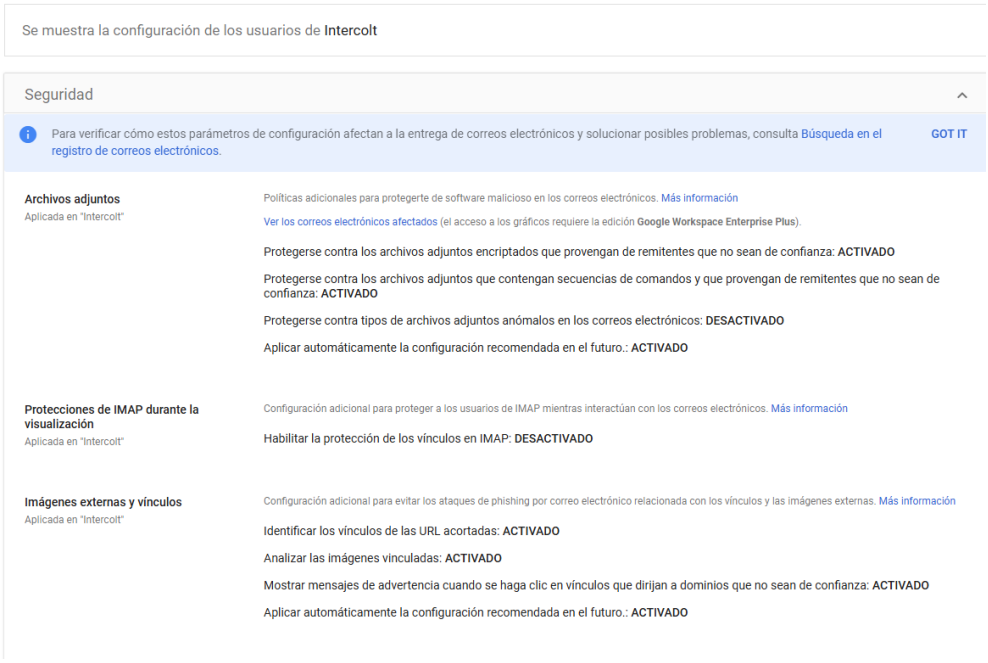
Nota: Obtenida de la consola de administración de G Suite de la correduría

La configuración de Google Workspace muestra que la verificación en 2 pasos está habilitada como opción, pero no se encuentra activada de forma obligatoria para todos los usuarios. Esto significa que cada colaborador puede decidir si la utiliza o no, dejando la seguridad de las cuentas sujeta a la elección personal en lugar de una política institucional. Además, los métodos permitidos no están restringidos, lo que limita el control sobre qué mecanismos de autenticación se consideran seguros para la organización.

Esta configuración representa una brecha importante en términos de seguridad, ya que la autenticación multifactor es uno de los controles fundamentales recomendados por ISO 27001 para proteger el acceso a información sensible. Al no exigirla de forma forzosa, la empresa queda expuesta a riesgos asociados al uso de contraseñas débiles, suplantación de identidad o accesos no autorizados. Implementar la verificación en 2 pasos obligatoria fortalecería significativamente la postura de ciberseguridad y el cumplimiento normativo.

- Configuraciones de seguridad básicas en Gmail.

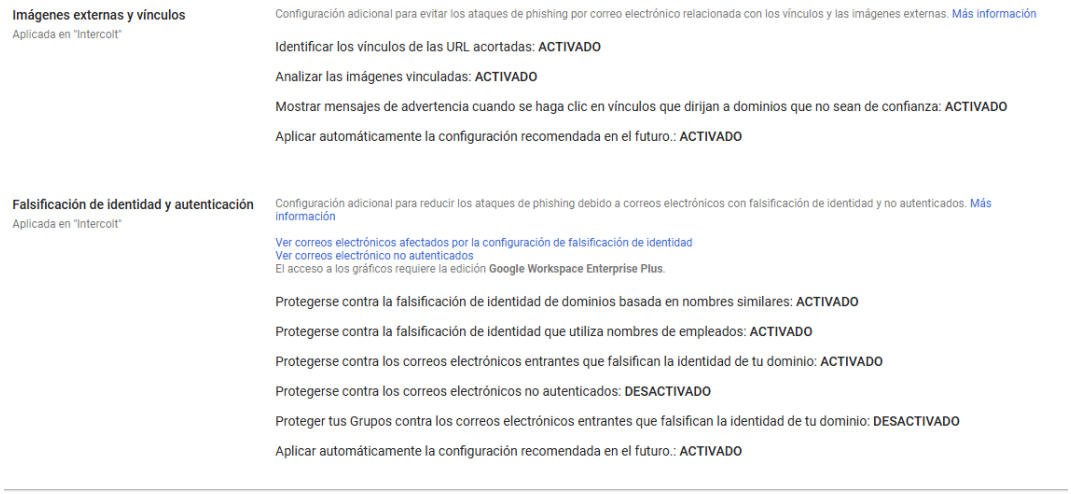
Figura 15: Configuración de Seguridad Gmail parte 1 Consola de Administración



Nota: Obtenida de la consola de administración de G Suite de la correduría

La configuración de seguridad muestra que existen buenas prácticas activadas, como la protección contra archivos adjuntos sospechosos, comandos incrustados e imágenes potencialmente maliciosas, así como el análisis automático de vínculos y advertencias ante enlaces no confiables. Sin embargo, también se evidencia que ciertas protecciones clave permanecen desactivadas, como el bloqueo de tipos de archivos anómalos y la protección de vínculos en IMAP, lo que deja brechas que podrían ser explotadas en escenarios de phishing o programa maligno. En conjunto, la empresa cuenta con un nivel básico de defensa, pero aún requiere fortalecer configuraciones críticas para alinearse mejor con los controles de seguridad recomendados por ISO 27001.

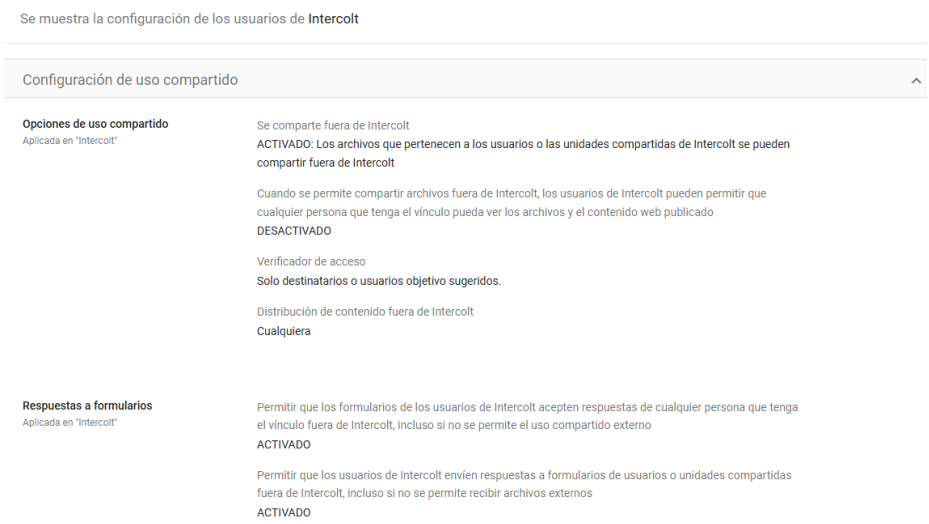
Figura 16: Configuración de Seguridad Gmail parte Consola de Administración



Nota: Obtenida de la consola de administración de G Suite de la correduría

La configuración refleja un nivel adecuado de protección frente a intentos de phishing e impersonación, ya que se encuentran activadas las defensas contra dominios similares, nombres de empleados falsificados y correos que intentan suplantar la identidad del dominio. No obstante, persisten brechas relevantes al tener desactivada la protección frente a correos no autenticados y la defensa de grupos frente a mensajes que falsifican la identidad del dominio, lo que expone a la organización a ataques más sofisticados. En conjunto, existe una base de seguridad bien establecida, pero aún es necesario activar los controles faltantes para reducir riesgos y alinearse plenamente con los criterios de autenticación reforzada sugeridos por ISO 27001.

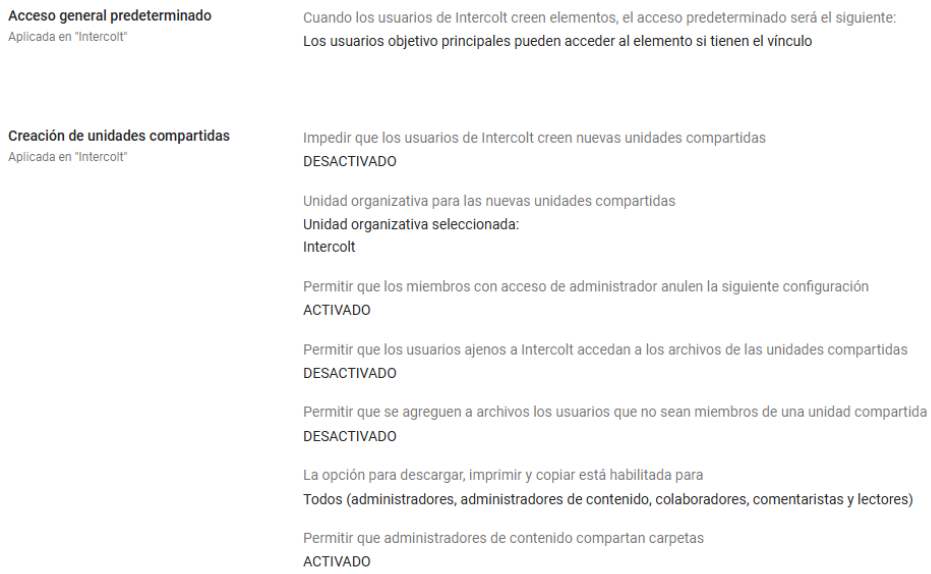
Figura 17: Configuración de Seguridad Drive & Documentos parte Consola de Administración



Nota: Obtenida de la consola de administración de G Suite de la correduría

La configuración muestra que el uso compartido externo está permitido para los archivos del dominio, lo cual facilita la colaboración con terceros, pero también incrementa el riesgo de exposición si no se controla adecuadamente quién accede o recibe la información. Aunque la opción que permite compartir con “cualquier persona con el vínculo” está desactivada, lo cual reduce accesos indiscriminados, la distribución fuera del dominio sigue abierta para “cualquier” destinatario y los formularios aceptan respuestas externas sin restricciones. En conjunto, esto refleja un entorno flexible para el trabajo colaborativo, pero con una necesidad clara de establecer políticas más estrictas y alineadas a ISO 15489 e ISO 27001 para evitar fugas de información o usos indebidos del contenido compartido.

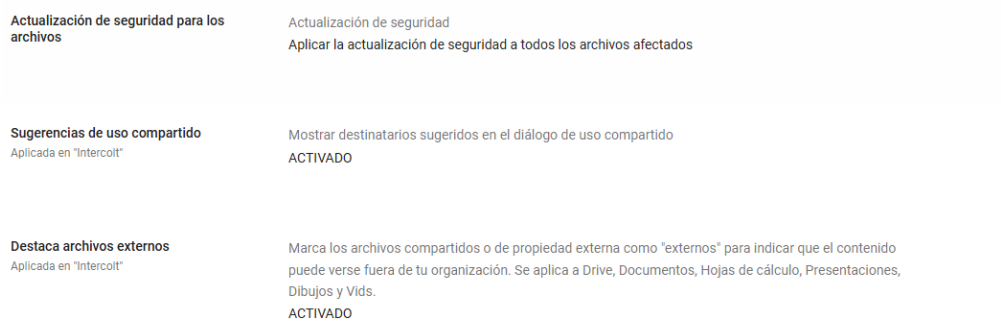
Figura 18: Configuración de Seguridad Drive & Documentos parte Consola de Administración



Nota: Obtenida de la consola de administración de G Suite de la correduría

La configuración muestra que los usuarios pueden crear y administrar unidades compartidas sin restricciones, y que el acceso predeterminado permite que cualquier usuario del dominio acceda al contenido si posee el vínculo, lo que facilita la colaboración interna pero también incrementa el riesgo de que información sensible circule sin control. Aunque el acceso externo y la agregación de archivos por usuarios ajenos al dominio están desactivados lo cual protege frente a fugas hacia terceros, la posibilidad de descargar, imprimir y copiar está habilitada para todos los roles, lo que limita la trazabilidad y el control documental. En general, la configuración promueve flexibilidad operativa, pero requiere ajustes para alinearse a buenas prácticas de seguridad y gestión documental establecidas por ISO 15489 e ISO 27001.

Figura 19: Configuración de Seguridad Drive & Documentos parte Consola de Administración

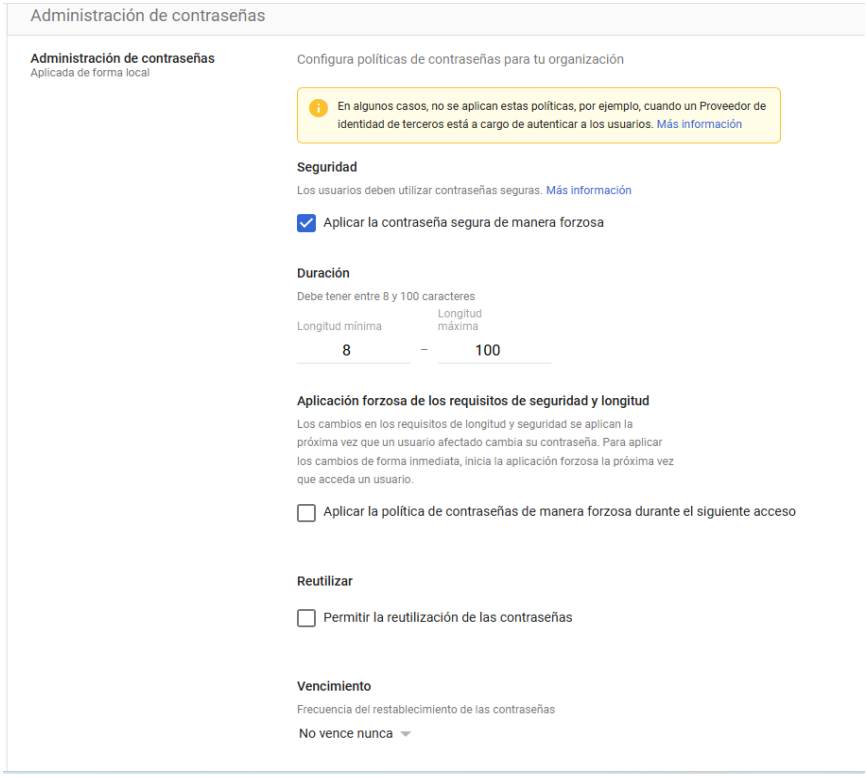


Nota: Obtenida de la consola de administración de G Suite de la correduría

La configuración evidencia buenas prácticas para reforzar la seguridad documental, ya que la actualización de seguridad se aplica automáticamente a los archivos afectados y se destacan los que han sido compartidos externamente, facilitando su identificación y control. Además, las sugerencias de uso compartido están activadas, lo que apoya a los usuarios en seleccionar destinatarios adecuados y reduce el riesgo de compartir información de manera accidental. Aunque estas medidas contribuyen a una mayor visibilidad y gobernanza sobre los archivos, aún deben complementarse con políticas más estrictas de acceso y clasificación para alinearse completamente con los lineamientos de ISO 15489 e ISO 27001.

- No se almacenan versiones de los documentos en formato digital solamente en físico.
- Bajos controles de creación de contraseñas

Figura 20: Configuración de Contraseñas Consola de Administración



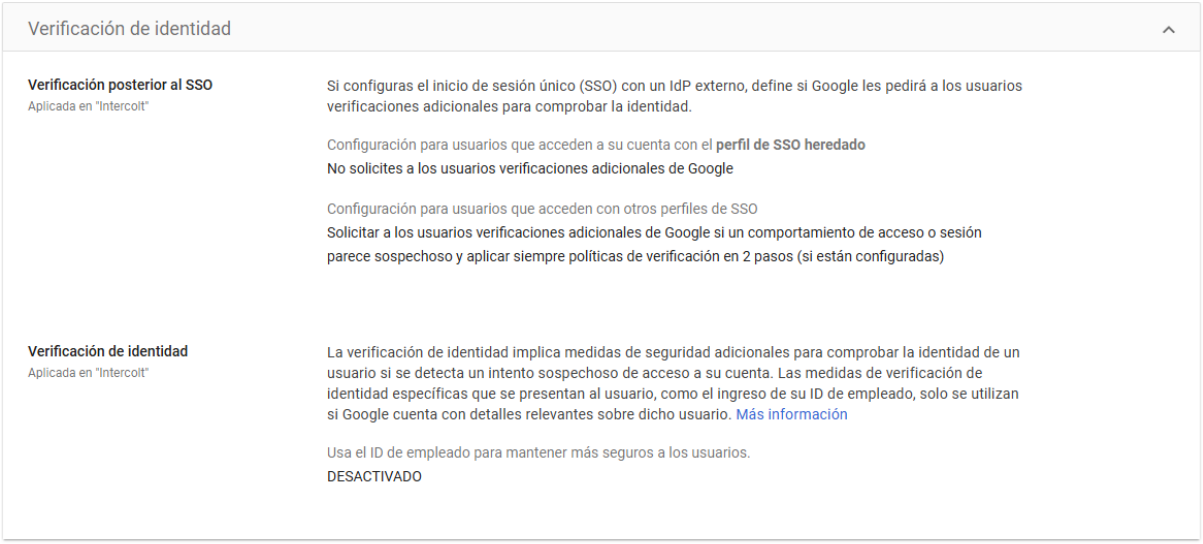
Nota: Obtenida de la consola de administración de G Suite de la correduría

La configuración de administración de contraseñas muestra que la organización exige el uso de contraseñas seguras con un mínimo de ocho caracteres, lo cual es positivo y contribuye a establecer una base de protección frente a accesos no autorizados. Sin embargo, no se ha habilitado la aplicación forzosa inmediata de nuevos requisitos de seguridad, ni se han establecido políticas de vencimiento o rotación de contraseñas, lo que limita significativamente la efectividad de esta medida. Además, la opción que permitiría bloquear el uso de contraseñas antiguas sigue desactivada, reduciendo la robustez del control.

Estas configuraciones representan riesgos importantes, ya que los usuarios podrían mantener contraseñas durante largos periodos sin actualización, incrementando la probabilidad de que sean vulneradas por ataques de fuerza bruta, filtraciones o suplantación de identidad. La falta de expiración periódica y la posibilidad de reutilizar contraseñas pueden facilitar accesos indebidos y comprometer la seguridad de la información, especialmente si tampoco se ha activado la autenticación multifactor obligatoria. Para cumplir con ISO 27001, sería necesario reforzar estos controles estableciendo políticas de rotación, complejidad y uso único de contraseñas, acompañadas de medidas adicionales como MFA.

- No se utiliza la verificación por identidad de los colaboradores

Figura 21: Configuración de Verificación de Seguridad Consola de Administración



Nota: Obtenida de la consola de administración de G Suite de la correduría

La configuración de verificación de identidad muestra que las medidas de seguridad adicionales no están plenamente habilitadas, ya que Google no solicita verificaciones adicionales para usuarios con perfiles de SSO heredados y la verificación basada en ID de empleado permanece desactivada. Aunque se aplican verificaciones adicionales solo cuando se Detectara un comportamiento sospechoso, la falta de controles más estrictos incrementa el riesgo de accesos no autorizados o suplantación de identidad, especialmente si no se complementa con autenticación multifactor obligatoria.

Figura 22: Configuración de Protección de Datos G-Suite Consola de administración

Nota: Obtenida de la consola de administración de G Suite de la correduría

La estadística evidencia un riesgo considerable para la organización, ya que el 55% de los mensajes de Gmail que contienen datos sensibles fueron enviados a destinatarios externos durante los últimos 30 días, lo que indica un nivel elevado de exposición y una falta de controles efectivos para proteger información crítica. Aunque la plataforma ofrece recomendaciones y opciones para restringir el uso compartido externo, actualmente la organización no cuenta con mecanismos automáticos que bloqueen o supervisen este tipo de contenido, lo que incrementa el riesgo de fugas accidentales o intencionales.

4.2.3 INFORMACIÓN PERSONAL IDENTIFICABLE DE LA CORREDURÍA

La siguiente información personal identificable es recolectada para los procesos de venta y renovación de pólizas. La cual se almacena en la misma cotización, póliza, mensajes de WhatsApp y correo electrónico.

1.Información Personal Identificable (PII): Datos que identifican directamente a una persona.

- Nombre completo
- Número de identidad (DNI)
- RTN
- Fecha de nacimiento

- Dirección
- Número de teléfono
- Correo electrónico

2.Información Financiera: Datos relacionados con medios de pago y transacciones.

- Comprobantes de transferencia
- Información de tarjetas
- Recibos de pago
- Historial de pagos del cliente

3.Información Médica:

- Diagnósticos médicos
- Expedientes clínicos
- Certificados médicos
- Medicamentos recetados
- Registros de enfermedades preexistentes
- Resultados de exámenes clínicos
- Precertificaciones
- Facturas de procedimientos y medicamentos
- Formulario de Reclamos llenados por los médicos

4. Información Vehicular:

- Documentos del vehículo
- Número de chasis y motor
- Factura del vehículo
- Licencia del conductor
- Fotos del vehículo
- Documentos de importación

5. **Información Contractual:**
   - Contratos de póliza
   - Condiciones particulares
   - Endosos
   - Solicitudes de seguro

- Formularios de reclamo
- Documentos de renovación o cancelación
- Documento de cambio de corredor

4.2.4 ANÁLISIS DE LA APLICACIÓN DEL CUESTIONARIO

Del instrumento de cuestionario las siguientes preguntas serán utilizadas para analizar el objetivo correspondiente, de la misma forma para un mejor análisis de han definido categorías para agrupar y analizar el objetivo principal de la pregunta.

Tabla 34: Agrupación de preguntas para análisis del objetivo 1

Categoría / Tema de análisis	Descripción del enfoque	Preguntas incluidas
1. Conocimiento y percepción sobre las normas ISO y seguridad de la información	Evalúa qué tanto los colaboradores conocen las normas ISO (27001, 30301, etc.) y su relación con la protección documental.	1, 2, 3, 5, 6, 12
2. Organización y gestión documental interna	Analiza cómo la empresa organiza, guarda y controla sus documentos, así como la existencia de reglas, procedimientos y accesibilidad.	4, 7, 8, 9, 10
3. Uso de plataformas y herramientas digitales	Mide la facilidad de uso, aprendizaje, acceso y funcionalidades (búsqueda, versiones, permisos) de las plataformas de gestión documental.	11, 13, 17, 19
4. Seguridad, control y respaldo de la información	Evalúa las medidas de seguridad, control de accesos, respaldo y confianza frente a pérdidas o incidentes.	14, 15, 16, 18,20,21
5. Mejora continua, participación del personal y confianza organizacional	Considera la opinión de los empleados y la aplicación de mejoras para optimizar los procesos documentales.	25,26,27,28
6. Procedimientos y planes ante incidentes	Evalúa si la empresa cuenta con medidas de recuperación, respaldo y detección oportuna ante	22,23,24

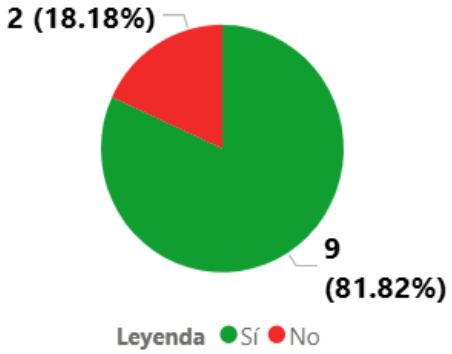
Categoría / Tema de análisis	Descripción del enfoque	Preguntas incluidas
	problemas de información.	
7. Experiencia práctica (preguntas abiertas)	Profundiza en la experiencia del personal: dificultades y beneficios percibidos con la digitalización documental.	30, 31

Nota: Elaborada por los autores

4.2.4.1 CONOCIMIENTO Y PERCEPCIÓN SOBRE LAS NORMAS ISO Y SEGURIDAD DE LA INFORMACIÓN

Los resultados de esta sección están vinculados a la aplicación del cuestionario en el cual se buscó evaluar qué tanto los colaboradores conocen las normas ISO (27001, 30301, etc.) y su relación con la protección o gestión documental.

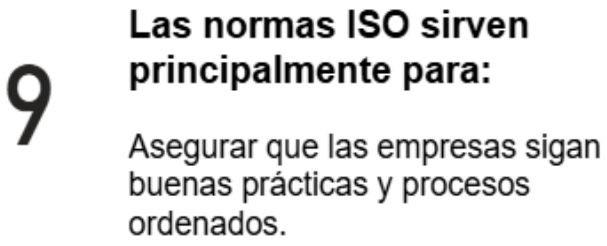
Gráfico 14: ¿Ha escuchado hablar de las normas ISO relacionados con empresas y organizaciones?



Nota: Elaborada por autor

Como se muestra en la imagen anterior podemos ver en esta sección que 81.82 de los colaboradores conoce o ha escuchado sobre las Normas ISO, mientras que el 18.18% no conoce sobre ellas. Teniendo en este caso ninguna distinción en esta pregunta hacia las normas asociadas a la investigación.

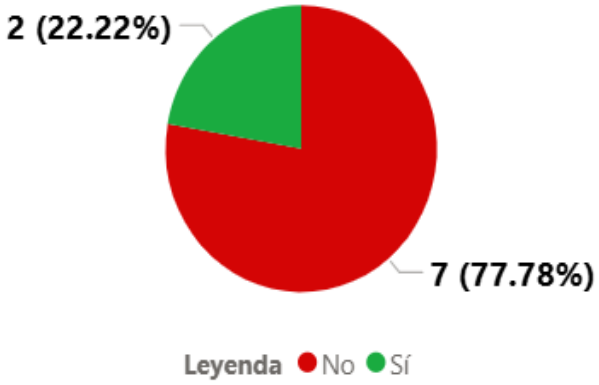
Figura 23: Conocimiento sobre Normas ISO



Nota: Elaborada por los autores

Mediante la siguiente pregunta podemos ver nueve de once colaboradores (81.82%) identifica de forma correcta el concepto de las normas ISO, mientras que solo dos colaboradores (18.18%) no conocen sobre las Normas ISO. Esto es importante ya que muestra un alto porcentaje de conocimiento general frente a lo que son las Normas ISO que son base para nuestra investigación.

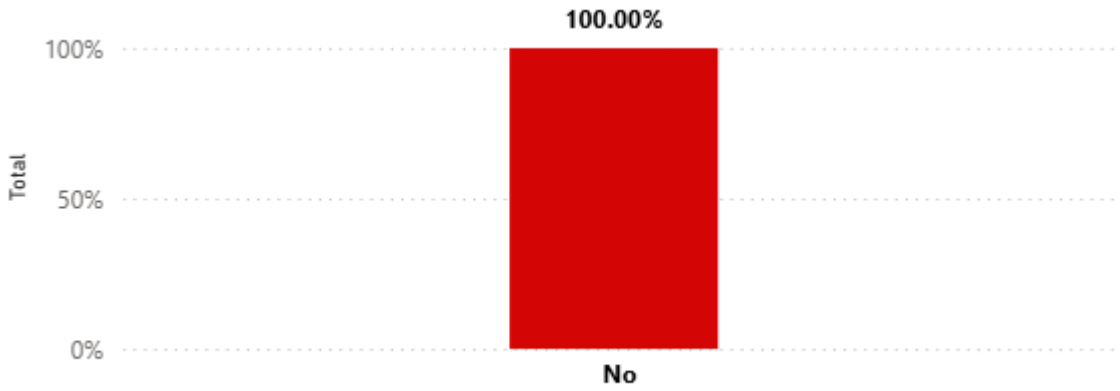
Gráfico 15: ¿Sabe que existe una norma llamada ISO 27001 que ayuda a proteger la información de las empresas?



Nota: Elaborada por los autores

Considerando el resultado anterior y el enfoque de esta investigación vemos que, aunque obtuvimos una respuesta positiva frente a la definición de las normas ISO, encontramos que el conocimiento de la norma ISO 27001 que es un pilar de la seguridad de la información hoy en día solo dos de los nueve colaboradores equivalente al 77.78% que respondieron que han escuchado sobre las normas ISO han escuchado sobre la ISO 27001.

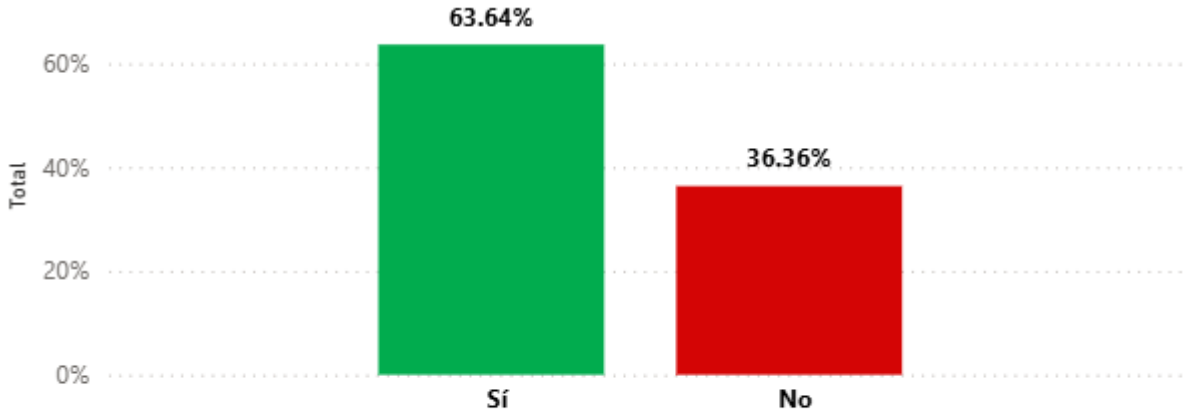
Gráfico 16 ¿Cree que la seguridad de la información protege únicamente los documentos en papel?



Nota: Elaborada por los autores

A pesar de tener esta respuesta mencionada anteriormente vemos que los 11 colaboradores (100%) distinguen que la seguridad de la información no está asociada solamente a la protección de los documentos físicos, si no más también para los digitales. Lo que es muy importante al momento de implementar un SGD debido a que se estará impactando tanto los documentos físicos como los digitales dentro de la correduría.

Gráfico 17: ¿Sabe cómo navegar de forma segura en internet (evitar descargas peligrosas, no compartir información sensible, etc.)?



Nota: Elaborada por los autores

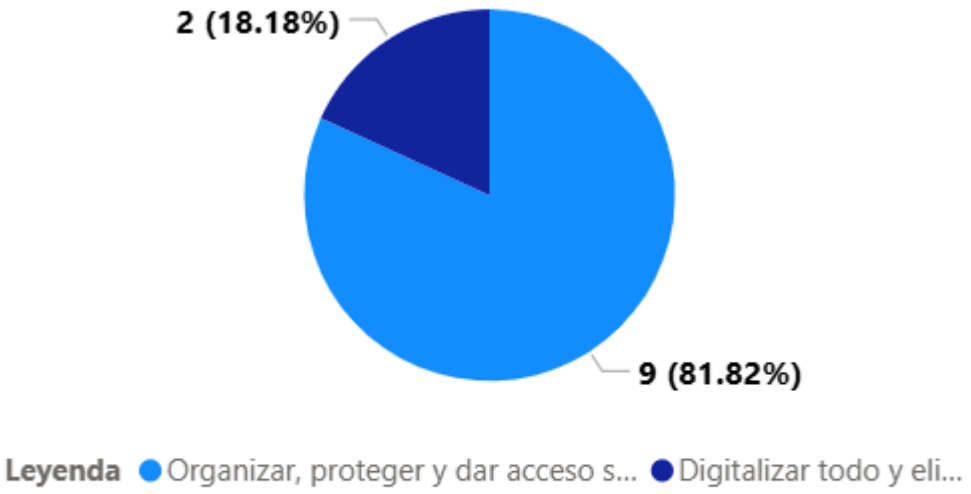
A nivel de seguridad podemos ver que es necesario fortalecer a la organización en temas de prevención de ataques en ciberseguridad debido a que el 36.36% de la fuerza laboral (cuatro personas) no conocen cómo distinguir o navegar de forma segura sin comprometer los datos sensibles de la organización. Este es un indicador clave para tener en cuenta para tener en consideración para desarrollar un plan de capacitación en temas de seguridad, debido a que este indicador de forma ideal debe ser al 100% para reducir o evitar brechas o ataques a la

información de la correduría, en donde vemos actualmente que solo ocho de los once colaboradores (63.64%) conoce como navegar de forma segura identificando potenciales brechas o intentos de ataque cibernéticos.

4.2.4.2 ORGANIZACIÓN Y GESTIÓN DOCUMENTAL INTERNA

Los resultados de esta sección analizan cómo la empresa organiza, guarda y controla sus documentos, así como la existencia de reglas, procedimientos y accesibilidad.

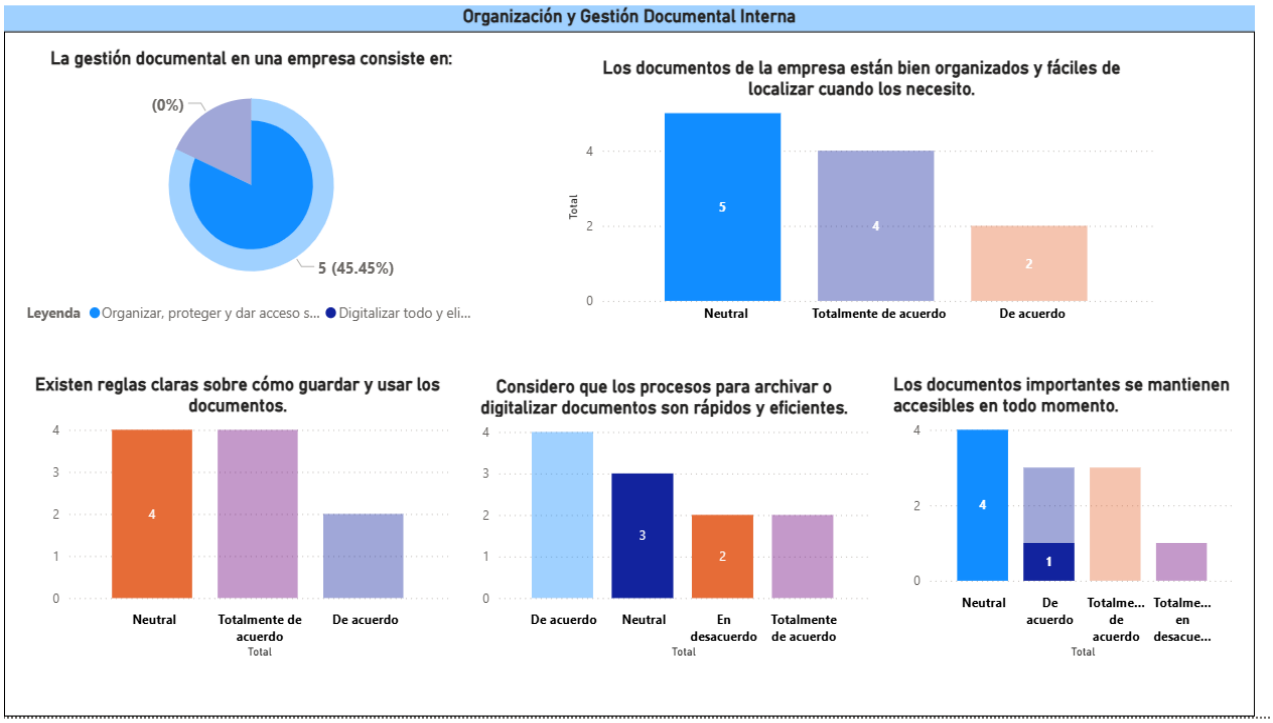
Gráfico 18: La gestión documental en una empresa consiste en:



Nota: Elaborada por los autores

Como vemos en la imagen anterior el 81.82% de los colaboradores identifica de forma correcta la definición o función de la gestión documental al seleccionar la opción de "Organizar, proteger y dar acceso seguro a la información cuando se necesita". Solamente dos colaboradores (18.18%) seleccionaron la opción de "Digitalizar todo y eliminar documentos físicos sin control", aunque no está incorrecta la percepción debido a que parte de la gestión de documental digital es eliminar la dependencia de documentos físicos, optimizar espacios físicos y mejorar la accesibilidad de la documentación. Este es un punto importante en donde podemos ver que existe en la correduría la definición de la importancia de organizar, proteger y dar acceso seguro a la información lo que es vital para iniciar un proyecto de un SGD dentro de la organización.

Figura 24: Organización y Gestión Documental Interna parte 2



Nota: Elaborada por los autores

Al analizar los gráficos anteriores sobre la gestión documental, se observa en dimensiones críticas como políticas, organización, localización, procesos y accesibilidad de los documentos predomina la opción de “Neutral”. Este análisis se considera la respuesta “Neutral” frente a la interrogante si los documentos de la empresa son bien organizados y fáciles de localizar, por lo que todos los gráficos de la figura se filtran con base en esa selección.

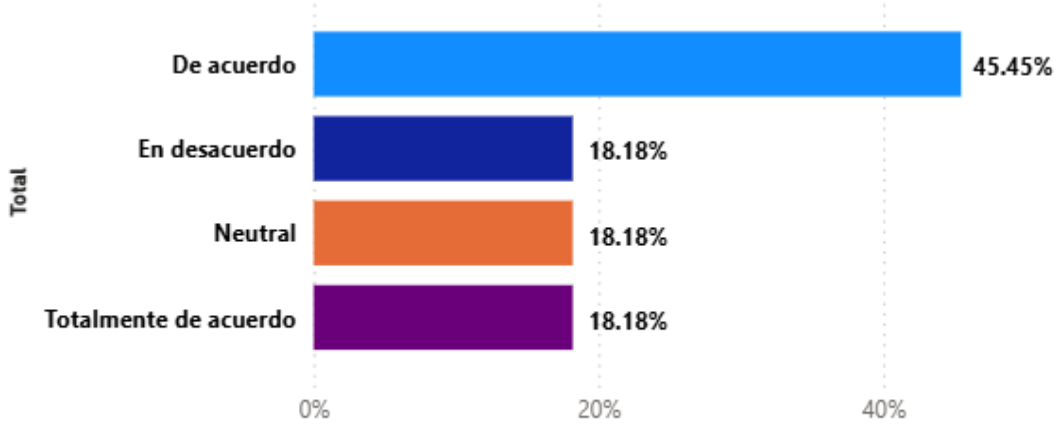
Esto nos permite ver una tendencia de una percepción general de que existe una conformidad, pero la organización no llega a establecer una satisfacción completa, lo que se traduce en un cumplimiento básico de los procesos, pero con un llamado de atención a revisar oportunidades claras de mejora.

Como se muestra en la imagen superior al filtrar el gráfico con base a la organización y localización de documentos cuando lo necesitan tomando en consideración los resultados generales de la figura 15 vemos que los mismos usuarios Responden o mantienen su visión neutral a lo largo de los siguientes gráficos. Esto nos demuestra que los procesos internos de gestión documental deben ser revisados y optimizados impactando de esta manera la satisfacción de los colaboradores y lograr consolidar una cultura organizacional orientada a la gestión efectiva de la documentación al ser una pieza clave y obligatoria para todos sus procesos de alta, actualización y baja de sus diferentes tipos de pólizas.

4.2.4.3 USO DE PLATAFORMAS Y HERRAMIENTAS DIGITALES

En esta sección se mide la facilidad de uso, aprendizaje, acceso y funcionalidades (búsqueda, versiones, permisos) de las plataformas de gestión documental.

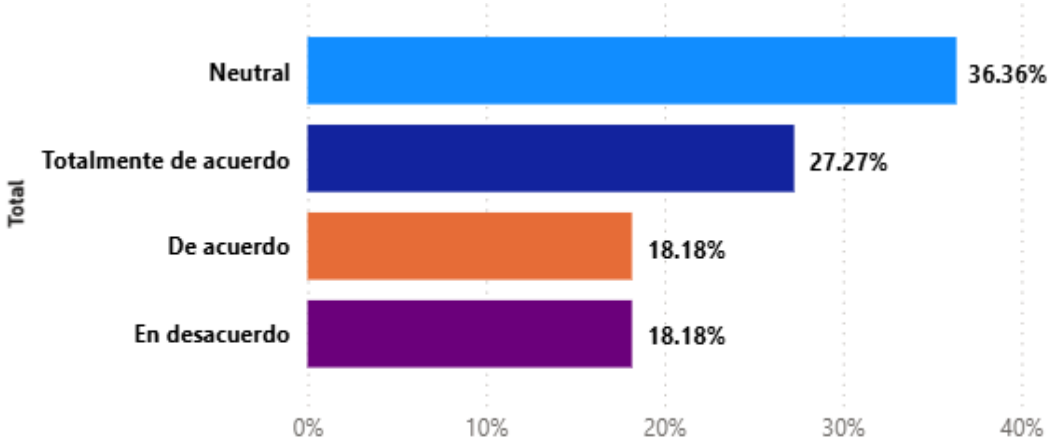
Gráfico 19: El sistema o plataforma Google Drive que usamos para manejar documentos es fácil de aprender y utilizar



Nota: Elaborada por los autores

Podemos observar que el 63.33% de los colaboradores se encuentra “De acuerdo” (45.45%) o “Totalmente de acuerdo” (18.18%) en que la herramienta actual, Google Drive, cumple con la funcionalidad básica esperada de un sistema de gestión documental, especialmente en cuanto a facilidad de uso y aprendizaje. Mientras que el 36.36% tienen una posición “Neutral” (18.18%) o “En desacuerdo” (18.18%). Esto indicador permite evaluar si la insatisfacción es con base a la falta de capacitación sobre la herramienta o limitantes técnicas de la misma.

Gráfico 20: El sistema tiene funciones útiles como búsqueda rápida, control de versiones y permisos de acceso.

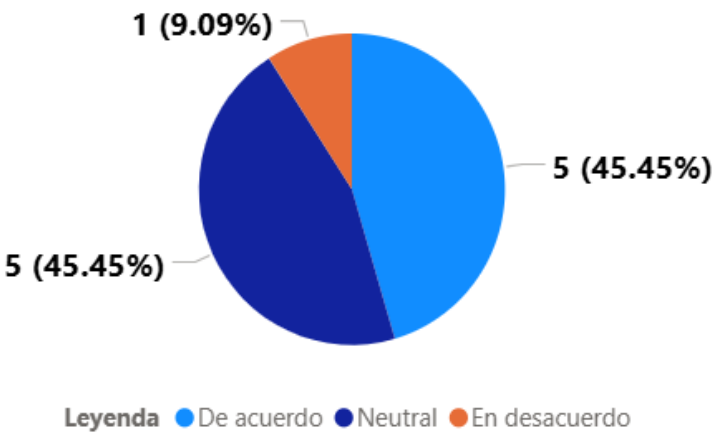


Nota: Elaborada por los autores

Sin embargo, en el siguiente gráfico el cual evalúa las funciones de búsqueda rápida, control de versiones y gestión de accesos evidencia que el 54.54% mantiene una posición "Neutral" y dos "En desacuerdo" (18.18%). Se obtuvo un resultado favorable del 45.45% mediante respuestas obtenidas de "Totalmente de acuerdo" (27.27%) y "De acuerdo" (18.18%) frente a las funcionalidades de la herramienta. Este resultado debe analizarse, ya que Google Drive, de manera inherente, ofrece dichas funcionalidades: permite la búsqueda rápida por nombre de documento o carpeta, mantiene un historial de versiones de los archivos modificados y permite configurar permisos de acceso tanto internos (utilizando el dominio corporativo) como externos (asignando roles de "Lector", "Comentarista" o "Editor").

Esto nos demuestra que es necesario dar una nueva capacitación técnica sobre la herramienta para que los colaboradores aprovechen al máximo estas funciones, mejorando la gestión y seguridad de los archivos. Además, se podría optimizar el uso de la herramienta mediante la creación de una estructura base o repositorio centralizado de clientes, administrado desde una cuenta institucional, lo que permitiría mayor orden y agilidad operativa.

Gráfico 21: El manejo de documentos está bien coordinado con otras áreas de la empresa.

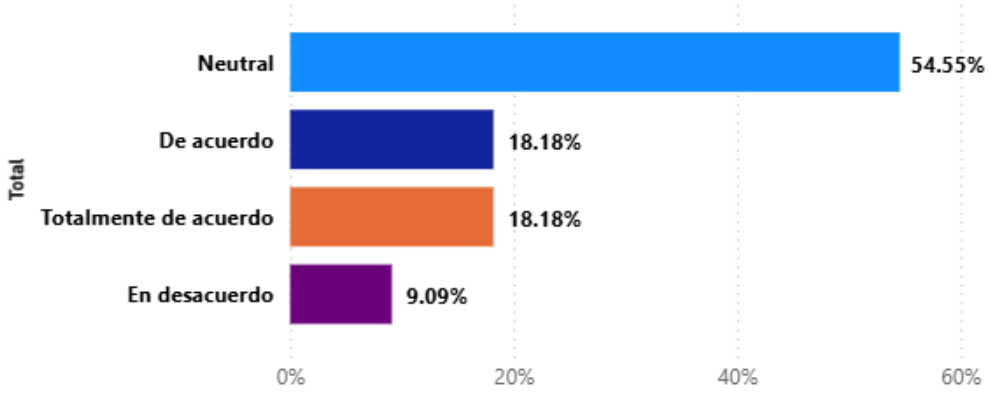


Nota: Elaborada por los autores

Por otra parte, los resultados también reflejan que existe una tendencia hacia respuestas "Neutrales" (45.45%) o "En desacuerdo" (9.09%) respecto a la coordinación del manejo documental entre áreas obteniendo un resultado combinado de 54.54%, siendo este mayor al porcentaje del 45.45% que está "De acuerdo" con que la coordinación de los documentos entre las diferentes áreas es eficiente.

Este resultado es preocupante, dado que la mayoría de los usuarios trabajan en el mismo espacio físico y podrían comunicarse fácilmente. Esto sugiere que, a pesar de contar con registros de documentos y pólizas, la comunicación y el intercambio de información entre equipos se están convirtiendo en un cuello de botella que afecta las operaciones diarias.

Gráfico 22: La forma en que manejamos documentos ayuda a mantener la continuidad del trabajo en caso de problemas.



Nota: Elaborada por los autores

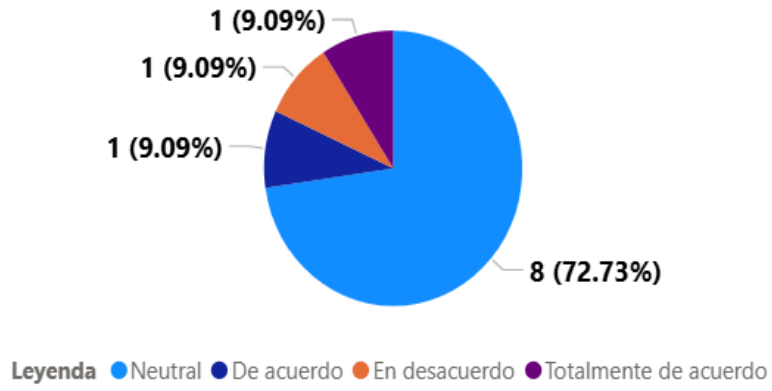
Asimismo, el 72.73% de los colaboradores considera que la forma actual de gestionar los documentos no contribuye a la continuidad del negocio frente a eventualidades o problemas referenciando las respuestas obtenidas como “Neutral” (54.55%) y “Totalmente en desacuerdo” (18.18%), frente a una respuesta más favorable de “De acuerdo” (18.18%) o “Totalmente de acuerdo” (18.18%) obteniendo un total entre ambas respuestas del 36.36%.

Lo que refuerza la necesidad de definir una estructura clara de gestión documental, acompañada de procedimientos formales y una estrategia de comunicación interna más efectiva.

4.2.4.4 SEGURIDAD, CONTROL Y RESPALDO DE LA INFORMACIÓN

En esta sección se evalúan las medidas de seguridad, control de accesos, respaldo y confianza frente a pérdidas o incidentes.

Gráfico 23: Confío en que la información almacenada está protegida frente a pérdidas o accesos indebidos.

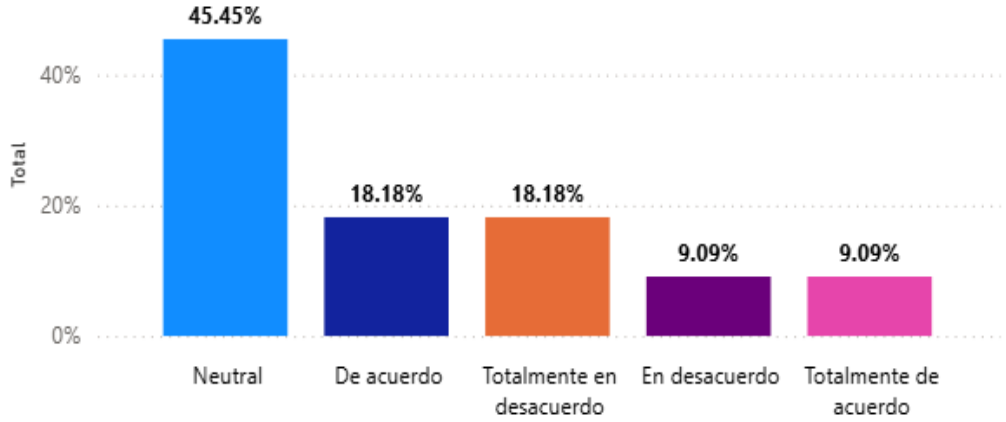


Nota: Elaborada por los autores

A nivel de seguridad, control y respaldo de la información, se observa que más del 80% de los colaboradores manifiestan poca o nula confianza en que la información esté protegida frente a pérdidas o accesos indebidos, considerando las respuestas de “Neutral” (72.73%) y “En desacuerdo” (9.09%). Obteniendo dos respuestas positivas equivalentes al 11,8.18% estando “De acuerdo” (9,09%) o “Totalmente de acuerdo” (9,09%).

Este resultado es relevante, ya que evidencia la necesidad de reforzar las medidas de seguridad informática en la organización. En este sentido, se recomienda implementar mecanismos de autenticación multifactor, mantener los antivirus actualizados, utilizar las versiones más recientes del sistema operativo y, de manera complementaria, capacitar al personal en temas de ciberseguridad.

Gráfico 24: Cuando surge un problema con la plataforma, recibimos apoyo oportuno.

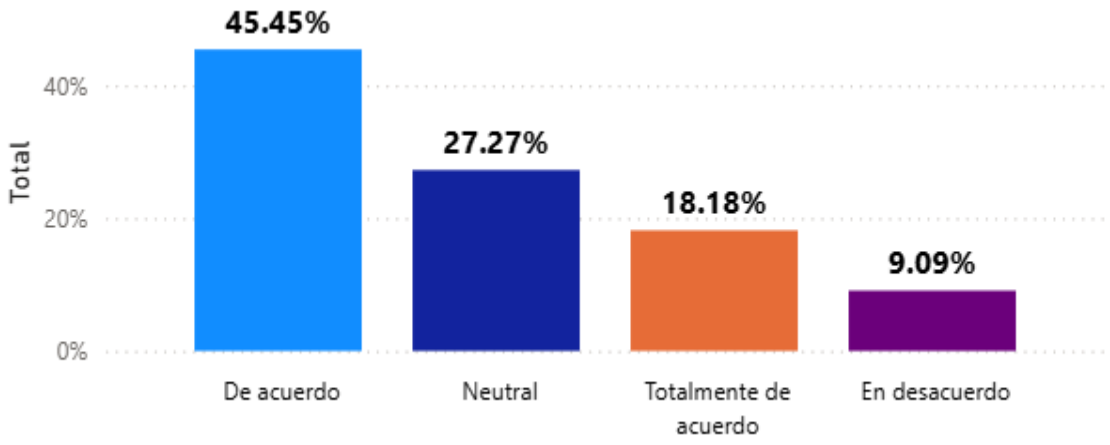


Nota: Elaborada por los autores

Considerando los análisis realizados antes estos resultados, se identifica que, ante la ocurrencia de fallas o problemas en la plataforma, las respuestas “Neutral” (18.18%) y “En desacuerdo” (9.09%) representando ocho de los once colaboradores equivalentes al 72.72%, lo cual indica tiempos de resolución elevados o falta de comunicación del responsable de la herramienta. Mientras que el 27.27% considera que ha recibido el apoyo oportuno ante errores o incidentes relacionados al Google Drive, considerando el 9.09% que está “Totalmente de acuerdo” y el 18.18% “De acuerdo”.

Esto sugiere la necesidad de establecer acuerdos de niveles de servicio (SLA) y mecanismos de monitoreo y seguimiento continuo, con el fin de asegurar la integridad, disponibilidad y funcionalidad de la plataforma. Asimismo, se recomienda realizar una revisión interna que permita identificar los errores más recurrentes y determinar si estos provienen de fallos técnicos o de un uso inadecuado de las funcionalidades por parte del equipo.

Gráfico 25: La empresa define claramente quiénes son responsables de manejar los documentos.

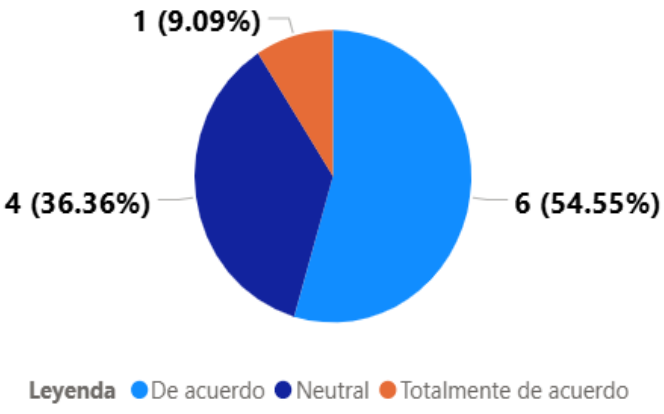


Nota: Elaborada por los autores

Por otra parte, en el ámbito de responsabilidades, se evidencia que no existe una definición clara sobre quién o quiénes son los encargados de la creación, actualización o eliminación de documentos, ya que podemos ver que solamente el 45.45% esta "De acuerdo" o el 18.18% como "Totalmente de acuerdo" equivalente a un 63.63%, frente a un 36.36% que se considera como "En desacuerdo" (9.09%) o "Neutral" (27.27%) frente a la definición de responsabilidades.

Por ello, resulta indispensable designar formalmente a una persona o comité responsable de la gestión documental, así como comunicarlo al resto del equipo para garantizar la trazabilidad y el control de los registros.

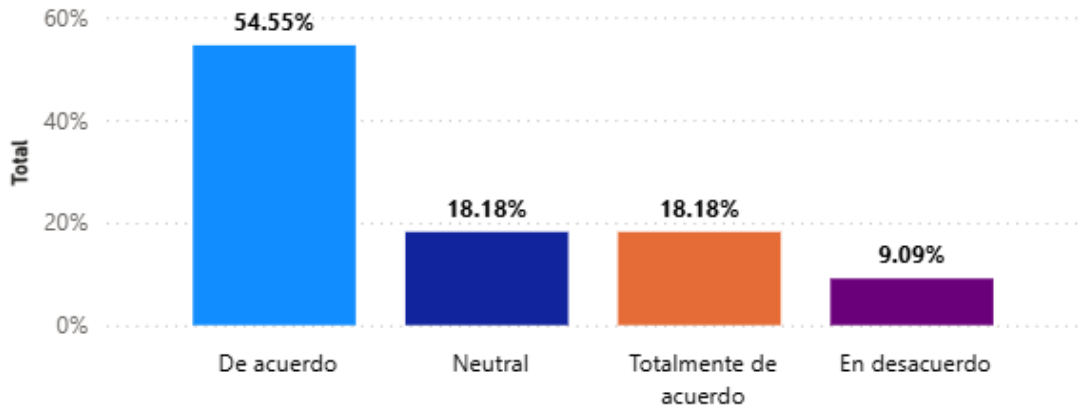
Gráfico 26: Los procesos actuales permiten que la empresa pueda crecer sin perder control de la información.



Nota: Elaborada por los autores

Finalmente, sí bien el 63.64% de los colaboradores considera estar “Totalmente de acuerdo” (9.09%) y “De acuerdo” (54.55%) que los procesos actuales de gestión documental contribuyen al crecimiento de la organización sin comprometer el control de la información, la presencia de cuatro respuestas neutrales (36.36%) sugiere que es necesario evaluar si los procesos vigentes son realmente los más adecuados, especialmente frente a las proyecciones de expansión de la correduría.

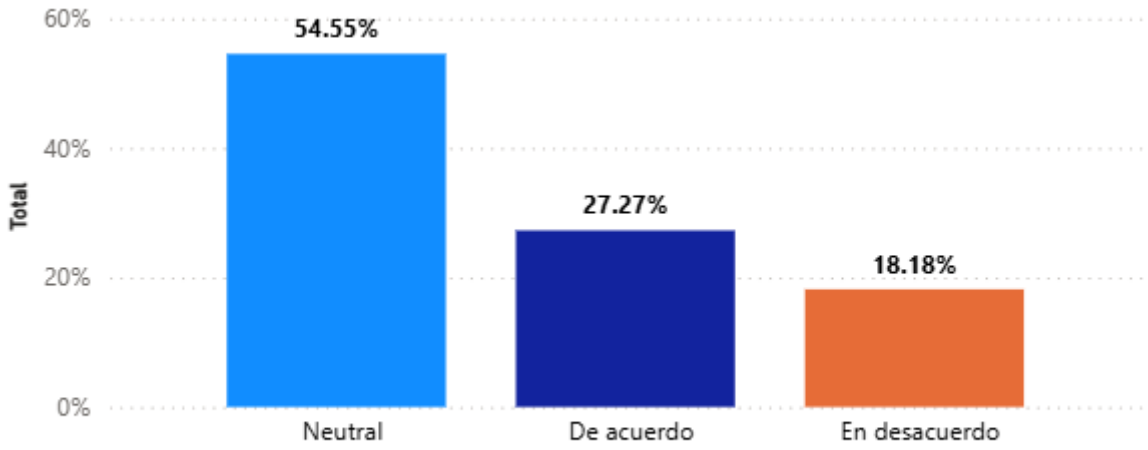
Gráfico 27: La empresa mantiene un inventario de los documentos e información más importantes.



Nota: Elaborada por los autores

Como parte del seguimiento y control de los documentos e información relevante para la correduría, se observa que ocho colaboradores (equivalentes al 72.73%) manifestaron estar “De acuerdo” (54.55%) o “Totalmente de acuerdo” (18.18%) con la afirmación de que se lleva un control adecuado de la documentación. Aunque este resultado puede considerarse un indicador positivo del funcionamiento del sistema actual, vemos que el 27.27% de los colaboradores no comparte esta visión al Responder estar “En desacuerdo” (9.09%) y “Neutral (18.18%). En donde el caso ideal sería alcanzar una valoración unánime de “Totalmente de acuerdo”, lo que refleja la existencia de un inventario documental integral, actualizado y accesible para todos los usuarios, respaldado por una definición clara de permisos y niveles de acceso.

Gráfico 28: Existen medidas para proteger la información frente a accesos no autorizados.



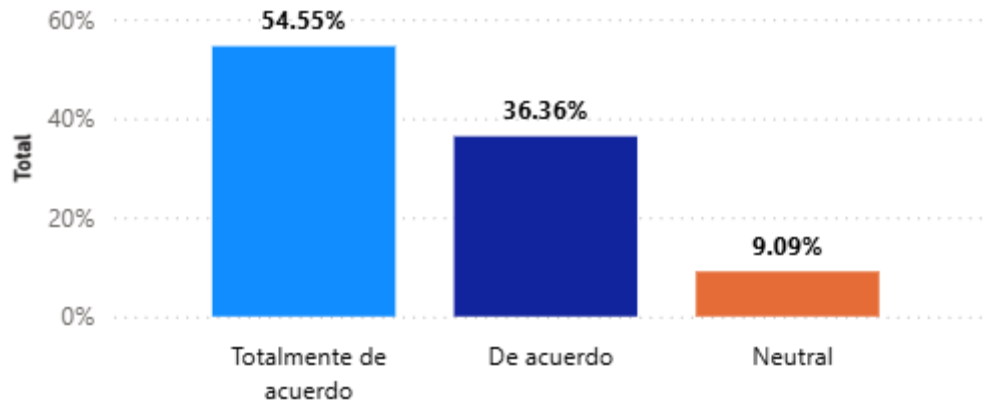
Nota: Elaborada por los autores

En cuanto a las medidas y políticas de seguridad, los resultados muestran una alerta que requiere atención inmediata, dado que únicamente tres colaboradores (27.27%) seleccionaron la opción "De acuerdo". Esto evidencia que no existen políticas internas formalmente establecidas en materia de seguridad de la información al obtener el 72.73% de colaboradores con opiniones desfavorables teniendo los siguientes resultados "Neutral" (54.55%) y "En desacuerdo" (18.18%) o bien que estas no han sido comunicadas ni aplicadas de manera efectiva. Es importante destacar que esta debilidad no solo se refiere al control de accesos no autorizados, sino también a la protección general de los datos, la gestión de respaldos, el uso de contraseñas seguras y la prevención de incidentes de seguridad.

4.2.4.5 MEJORA CONTINUA, PARTICIPACIÓN DEL PERSONAL Y CONFIANZA ORGANIZACIONAL

En esta sección se considera la opinión de los empleados y la aplicación de mejoras para optimizar los procesos documentales.

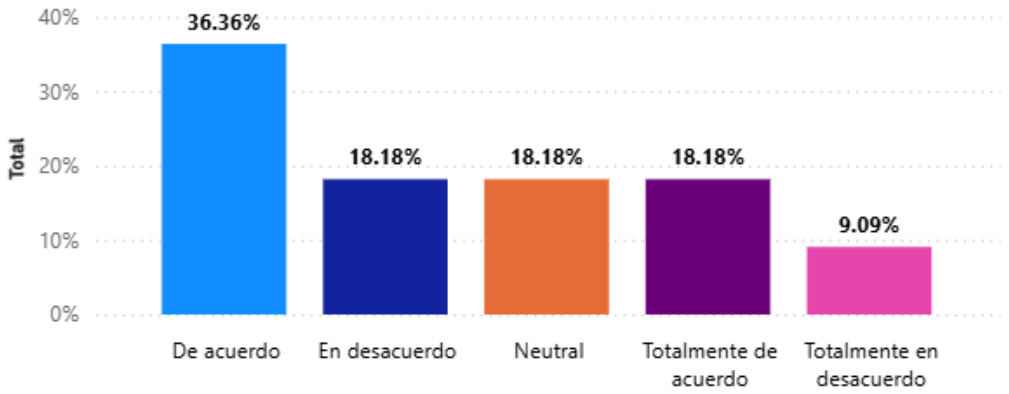
Gráfico 29: Considero que existen aspectos que podrían mejorarse en el manejo actual de documentos.



Nota: Elaborada por los autores

Como parte integral de toda organización, la mejora continua y la participación de los colaboradores son elementos fundamentales para promover una cultura de crecimiento, escucha y compromiso institucional. En este sentido, se observa que el 90.91% de los colaboradores considera que existen oportunidades de mejora y crecimiento relacionadas con la gestión actual de documentos, al obtener resultados favorables estando el 54.55% "Totalmente de acuerdo" y el 36.36% "De acuerdo". Teniendo solamente el 9.09% con una posición "Neutral", lo cual representa un hallazgo valioso para la definición de planes de acción y estrategias de revisión, los cuales se detallarán en el Capítulo VI: Aplicabilidad, como base de fortalecimiento para la correduría.

Gráfico 30: Se toma en cuenta la opinión del personal para identificar mejoras en la gestión de documentos.

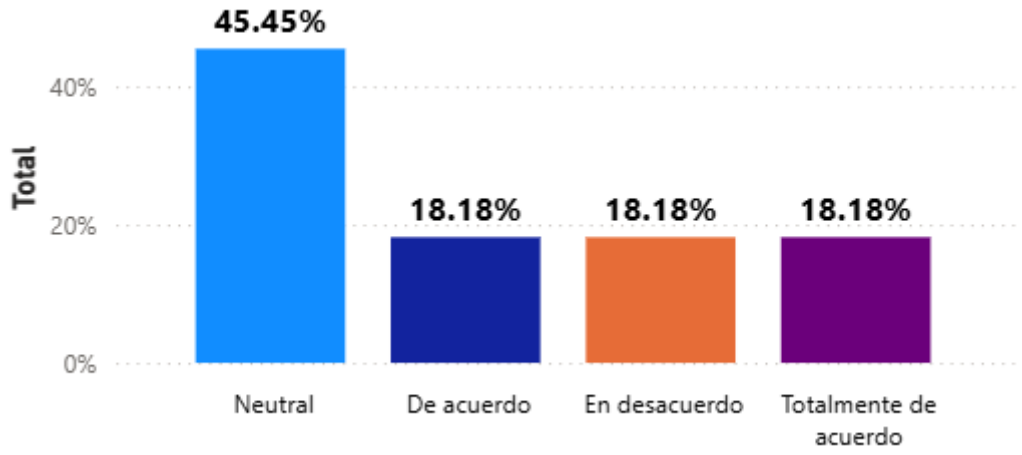


Nota: Elaborada por los autores

Asimismo, se evidencia una percepción interna mixta respecto a la cultura de escucha y participación, dado que únicamente el 54.54% de los colaboradores manifestaron estar “De acuerdo” (36.36%) y el (18.18%) como “Totalmente de acuerdo” en que los directivos brindan apertura para comunicar ideas orientadas a mejorar la gestión documental. Mientras que el 18.18% respondieron “En desacuerdo”,18.18% “Neutral” y el 9.09% como “Totalmente en desacuerdo”.

Este resultado es relevante, refleja la necesidad de evaluar la cultura organizacional de comunicación y mejora continua, para fomentar espacios que incentiven la participación de los colaboradores en la optimización de procesos y herramientas clave. La incorporación activa de los empleados en estas iniciativas puede traducirse en mayor sentido de pertenencia, eficiencia operativa y generación de valor para la organización.

Gráfico 31: He visto que se aplican cambios o mejoras en la forma de manejar los documentos.



Nota: Elaborada por los autores

De igual manera, los resultados del siguiente gráfico muestran una tendencia predominante hacia a visión negativa respecto a si se han observado mejoras o cambios aplicados en la gestión documental, mediante el 45.45% como “Neutral” y el 18.18% como “De acuerdo”. De la misma forma vemos que solamente el 36.36% tiene una visión favorable frente a los cambios al obtener el 18.18 en “De acuerdo” y el 18.18 como “Totalmente de acuerdo”.

Esto sugiere que no se han implementado acciones visibles o significativas en los últimos períodos, lo que reafirma la necesidad de establecer mecanismos formales de retroalimentación, seguimiento y comunicación de resultados dentro de los procesos de mejora.

Gráfico 32: El buen manejo de documentos ayuda a que los clientes confíen más en la empresa.

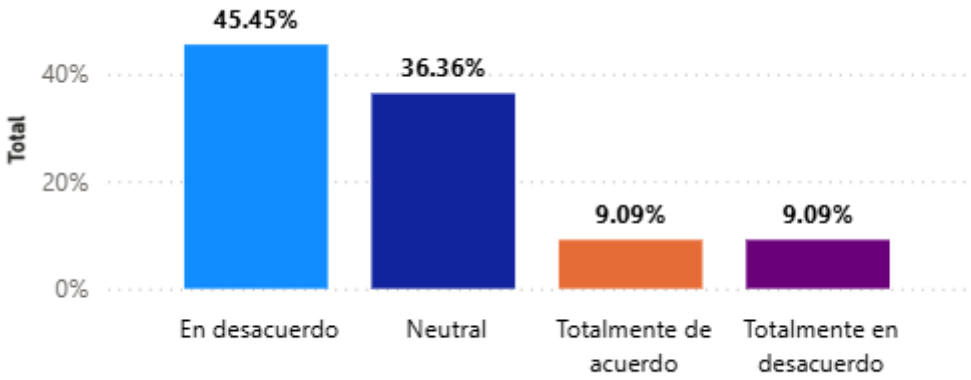
Nota: Elaborada por los autores

Por último, de manera unánime, el 100% de los colaboradores manifestaron estar "Totalmente de acuerdo" en que mejorar la gestión documental contribuiría a fortalecer la imagen de la correduría frente a clientes y proveedores, traduciéndose en una mayor fidelidad hacia la misma. Este consenso evidencia una conciencia colectiva del valor estratégico que tiene la gestión documental, la cual, una vez optimizada, podría convertirse en una ventaja competitiva sostenible frente a otras corredurías del sector.

4.2.4.6 PROCEDIMIENTOS Y PLANES ANTE INCIDENTES

En esta sección se evalúa si la empresa cuenta con medidas de recuperación, respaldo y detección oportuna ante problemas de información.

Gráfico 33: Si ocurre un problema con la información, la empresa cuenta con formas de Detectarlo a tiempo.



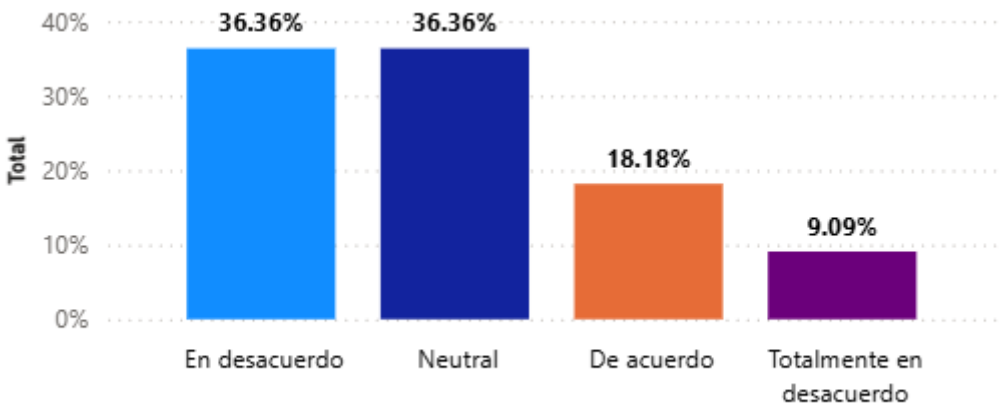
Nota: Elaborada por los autores

Podemos ver a nivel de prevención de incidentes que existe una visión negativa

predominante al obtener un total de 90.9% mediante las respuestas de “En desacuerdo” (45.45%),” Neutral” (36.36%) y el 9.09% “En desacuerdo”, obteniendo solo una respuesta favorable como “Totalmente de acuerdo” equivalente a un 9.09%:

Como parte integral del análisis de esta pregunta es necesario implementar una estructura de riesgos organizacional, buscando crear planes de respuesta ante incidentes, planes de contingencia y planes de acción que permitan reaccionar de manera oportuna ante cualquier brecha o situación imprevista, incluso aquellas no contempladas en la documentación existente.

Gráfico 34: Hay procedimientos para actuar en caso de incidentes relacionados con los documentos.



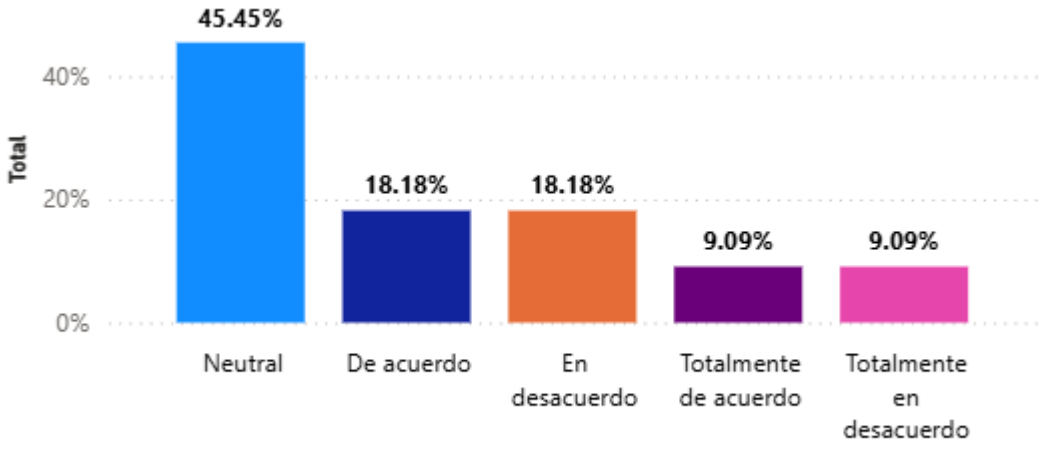
Nota: Elaborada por los autores

Sin embargo, los resultados reflejan que el 81% de los colaboradores se encuentra “En desacuerdo” (36.36%),” Totalmente en desacuerdo” (9.09%) o mantiene una posición “Neutral” (36.36%) respecto a la existencia de estos mecanismos. En donde solo se obtuvo un 18.18% con respuesta favorable equivalente al 18.18%: Lo que evidencia que la correduría no cuenta actualmente con los controles ni con las acciones necesarias para Detectar brechas de seguridad y Responder adecuadamente ante ellas. Por tanto, resulta prioritario diseñar, documentar e implementar planes de acción específicos orientados a la identificación, mitigación y recuperación ante incidentes.

De manera complementaria, se observa una correlación directa con los resultados del primer gráfico, en el cual el 73% de los colaboradores manifestó estar “En desacuerdo” o “Neutral” frente a la afirmación de que existen procedimientos establecidos para tomar acciones correctivas ante incidentes relacionados con documentos. Este hallazgo refuerza la conclusión de que no se han definido protocolos formales de actuación ni mecanismos de control que

permitan dar seguimiento y resolución a los incidentes documentales o de seguridad de la información.

Gráfico 35: La empresa tiene planes para recuperar la información y continuar operando si ocurre una pérdida.



Nota: Elaborada por los autores

Finalmente, este último gráfico evidencia de manera consistente que la organización carece de planes de acción y recuperación formalmente establecidos, al obtener respuestas del 45.45% como “Nuestra”, el 18.18% “En desacuerdo”, 9.09% en “Totalmente en desacuerdo”, lo que da un total del 72.72%. De forma contrario vemos un bajo porcentaje de respuestas negativas con un total del 27.27% mediante las respuestas de “De acuerdo” (18.18%) y “Totalmente en desacuerdo” con el 9.09%.

Esto cual representa una brecha crítica dentro de la gestión de riesgos. En consecuencia, se recomienda elaborar matrices de riesgos, planes de contingencia y estrategias de recuperación post-incidente, asegurando su difusión y capacitación interna para fortalecer la resiliencia y continuidad operativa de la correduría.

4.2.4.7 EXPERIENCIA PRÁCTICA (PREGUNTAS ABIERTAS)

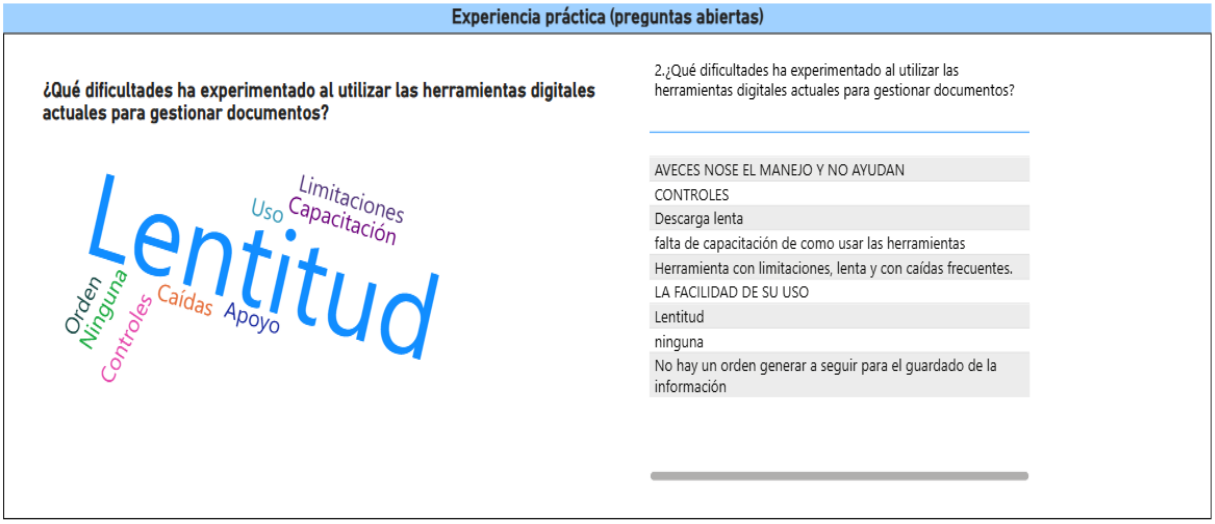
En esta sección se profundiza en la experiencia del personal: dificultades y beneficios percibidos con la digitalización documental.

Los siguientes gráficos se componen de dos partes:

- **Gráfico ubicado a la izquierda:** Presenta una nube de palabras elaborada a partir de las respuestas de los encuestados. En ella, los investigadores analizaron y sintetizaron los términos más frecuentes utilizados por los participantes, para identificar las palabras que describen las percepciones expresadas en la encuesta.

- **Gráfico ubicado a la derecha:** Muestra las respuestas textuales exactas proporcionadas por los encuestados, permitiendo una interpretación más cualitativa y detallada de las opiniones obtenidas.

Figura 25: Análisis de Experiencia Practica



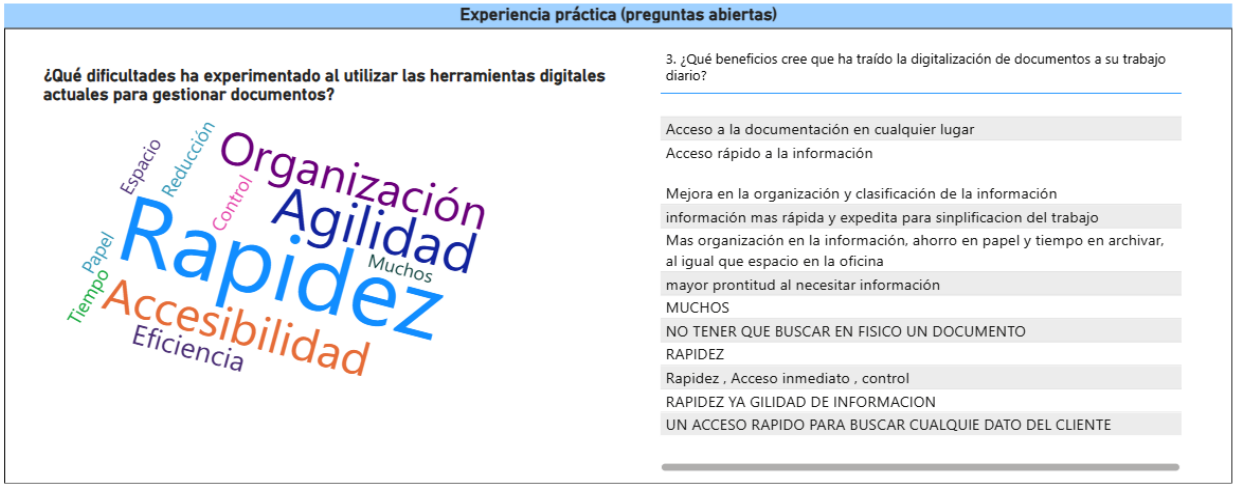
Nota: Elaborada por los autores

En cuanto a las dificultades identificadas, se observa que la lentitud es la principal percepción manifestada por los colaboradores respecto al uso de la herramienta Google Drive. Esta situación puede deberse a dos factores que la correduría debería evaluar:

1. Tamaño y tipo de archivos: cuando los documentos contienen imágenes de alta resolución o son archivos extensos, es comprensible que el proceso de carga o descarga sea más lento. En estos casos, se recomienda optimizar los formatos y pesos de los archivos, especialmente aquellos que se consultan con frecuencia.
2. Conectividad y ancho de banda: es necesario verificar que no existan problemas a nivel de conexión de red, ya que una conexión inestable o con poco ancho de banda puede impactar directamente los tiempos de carga y descarga de documentos en la plataforma.

De igual forma, los resultados continúan evidenciando la necesidad de fortalecer la capacitación interna sobre el uso eficiente de Google Drive, brindando mayor apoyo técnico y acompañamiento al personal. Además, se recomienda crear un repositorio centralizado para el almacenamiento de la documentación institucional, lo que permitirá mejorar la organización, accesibilidad y control de la información.

Figura 26: Análisis de Experiencia Practica parte II



Nota: Elaborada por los autores

A nivel de beneficios, se observa que, a pesar de las dificultades previamente mencionadas, la herramienta Google Drive ha aportado ventajas significativas al equipo, entre ellas la rapidez, agilidad, organización, accesibilidad y eficiencia en la gestión de documentos. Estos aspectos representan fortalezas que deben preservarse y potenciarse, reconociendo que la herramienta cumple con varias de las funcionalidades básicas esperadas de un sistema de gestión documental.

No obstante, es importante considerar las percepciones mixtas identificadas a lo largo de los distintos análisis realizados en esta sección, ya que reflejan diferencias entre los beneficios y cómo se sienten al utilizarla. Por ello, estos beneficios deben tomarse como punto de partida para optimizar el uso de la herramienta actual o, en su caso, evaluar la implementación de una nueva solución tecnológica que fortalezca la gestión documental dentro de la correduría.

4.2.5 ANÁLISIS DE LISTAS DE VERIFICACIÓN ISO

El análisis comparativo de las listas de verificación aplicadas bajo la Norma ISO 15489, 30301 y 27001 permite identificar los niveles de madurez tanto en gestión documental como en seguridad de la información. Los resultados reflejan la inexistencia de políticas formalmente aprobadas, falta de responsables definidos y la ausencia de procedimientos documentados bajo la captura, clasificación, respaldo y protección de datos. Así mismo, se evidencia un cumplimiento parcial en la estructuración del sistema de gestión documental donde la alta dirección muestra disposición y liderazgo, pero sin traducirse aun en lineamientos operativos o indicadores medibles.

4.2.5.1 LISTA VERIFICACIÓN ISO 15489

La lista de verificación aplicada bajo la Norma ISO 15489 permite evaluar el nivel de madurez del proceso de gestión de documentación dentro de la empresa Seguro Total, considerando los principios de fiabilidad, integridad y disponibilidad de los documentos.
El instrumento analiza aspectos como la existencia de políticas institucionales, responsables designados, procedimientos de captura y clasificación, uso de metadatos, así como la aplicación de reglas de acceso y seguridad.

Tabla 35: Lista de Verificación ISO 15489

N.º	Elemento por verificar	Cumple (Sí/No/En Proceso)	Comentarios / Evidencias
1	La organización tiene una política de gestión documental aprobada por la dirección.	No	No existe dentro de la organización una política definida o aprobada con respaldo sobre la gestión documental.
2	Se identifican los requisitos legales, regulatorios y normativos aplicables.	No	No existen en Honduras regulaciones sobre el almacenamiento, seguridad y distribución sobre documentos digitales o físicos.
3	Existen responsables designados para la gestión documental en todas las áreas.	En proceso	Existen personas asignadas que reciben, solicitan documentos físicos y electrónicos, los cuales también digitalizan documentos. Pero no se encuentran definidas en las funciones o responsabilidades de sus puestos.
4	Los documentos creados son completos, auténticos y fiables.	En proceso	El 100% de los documentos creados no son completos o no están actualizados al no existir procesos definidos.
5	Los procedimientos para la captura y registro de documentos están implementados.	En proceso	Existe un proceso, sin embargo, no está estructurado o está diagramado para su consulta o revisión.
6	Los documentos tienen metadatos asignados (autor, fecha, asunto, clasificación).	No	Inexistente, actualmente no se lleva esta información complementaria de los documentos digitales. Los documentos físicos solamente se reconocen dónde está almacenados debido a que el archivo tiene una calcomanía con el tipo de seguro y letra que indica que apellidos están almacenados en ese archivero.
7	Existe un esquema de clasificación	En Proceso	Como se menciona en el punto anterior existe un esquema de clasificación para documentación

N.º	Elemento por verificar	Cumple (Sí/No/En Proceso)	Comentarios / Evidencias
	documental aprobado y actualizado.		física pero el mismo puede ser más eficiente. La documentación digital se almacena en las carpetas de Google Drive de cada colaborador y la mayoría de los registros de la documentación sólo vive en el correo de Gmail.
8	Se aplican reglas de acceso y confidencialidad a los documentos.	En proceso	Solo existen los controles de acceso realizados mediante las credenciales de Google.
9	Los documentos son recuperables de manera eficiente por usuarios autorizados.	En proceso	Lo pueden recuperar solo si existe en el correo o fue almacenado en el Drive, pero no existen roles definidos de acceso y control.
10	Los documentos están protegidos contra pérdida, acceso no autorizado o destrucción.	En proceso	El acceso de los documentos físicos puede ser realizado por cualquier colaborador, los archiveros no tienen llave para cerrar. Los documentos están parcialmente protegidos con las credenciales de Google.
11	Se mantienen copias de seguridad y planes de contingencia para documentos críticos.	En proceso	Solo aquellos documentos que han sido almacenados en el Google Drive tienen copias de seguridad, no existe como tal un plan de contingencia ante brechas de seguridad y recuperación de la documentación.
12	Almacenamiento físico y digital cumple condiciones de seguridad y conservación.	No	Se cumplen funciones muy básicas de seguridad y conservación como se menciona en el punto 10.
13	Existe un calendario de conservación y disposición documental.	No	Inexistente actualmente en la organización.
14	Se aplican procesos documentados para eliminación o transferencia a archivo histórico.	En proceso	En caso de baja de un colaborador se envía una copia de seguridad a la gerente de operaciones para acceder al correo y Drive para recuperar información y documentación necesaria.
15	Se realizan auditorías o revisiones periódicas del sistema de gestión documental.	No	Inexistente actualmente en la organización.
16	Política y procedimientos de gestión documental se revisan y actualizan	No	Inexistente actualmente en la organización.

N.º	Elemento por verificar	Cumple (Sí/No/En Proceso)	Comentarios / Evidencias
	regularmente.		
17	El personal recibe capacitación en gestión de documentos.	No	No se realiza capacitación en términos de la gestión de documentos.
18	Se utilizan indicadores o métricas de eficacia en la gestión documental.	No	No existen indicadores actualmente de seguimiento de la eficacia de la gestión documental.
19	Se fomenta la mejora continua en la gestión documental.	En proceso	La junta directiva busca mejorar la gestión documental pero no se ha concretado una revisión.

Nota: Elaborada por los autores

La norma ISO 15489 permite evaluar las bases necesarias para establecer un sistema de gestión documental dentro de una organización. En este caso, podemos observar que dentro de la evaluación no se identificó ningún elemento marcado como “Sí”.

La distribución de resultados muestra que el 47% de los elementos se calificaron como “No” y el 53% como “En proceso”. Esto evidencia que, si bien la correduría ha iniciado acciones parciales, aún se encuentra en una etapa temprana de desarrollo de su sistema de gestión documental, sin alcanzar todavía un nivel de madurez suficiente.

En general, se identifica un nivel bajo de madurez en la gestión documental. La correduría utiliza actualmente Google Drive como herramienta de almacenamiento y gestión, lo cual representa una base funcional; sin embargo, existen múltiples oportunidades de mejora para lograr una gestión documental eficiente y conforme a estándares internacionales.

Entre los aspectos más relevantes, destacan la falta de formalización de políticas, la ausencia de roles y responsabilidades claramente definidos, la carencia de procedimientos actualizados, la insuficiente seguridad de la información, la no asignación de metadatos a los documentos digitales y la inexistencia de planes digitales de contingencia o respaldo.

Por lo tanto, se recomienda:

1. Crear y aprobar políticas de gestión documental, alineadas con la dirección de la organización.
2. Definir roles y responsabilidades específicas para la administración de documentos.
3. Estructurar y comunicar el proceso de gestión documental, estableciendo flujos claros desde la creación hasta la disposición final de los documentos.

4. Fortalecer la capacitación del personal en temas de seguridad de la información y buenas prácticas documentales.
5. Implementar indicadores de seguimiento y control, así como revisiones periódicas que permitan medir la eficacia del sistema y promover la mejora continua.

Es importante agregar que con base a los principios de la ISO 15489 encontramos los siguientes resultados:

1. Autenticidad: No hay políticas, metadatos ni controles de identidad; los documentos no pueden verificarse como auténticos ni confiables.
2. Fiabilidad: Los documentos no están completos ni actualizados, los procesos no están estructurados y la captura documental no está formalizada, afectando su consistencia.
3. Integridad: No existen controles de acceso adecuados, los documentos físicos no tienen protección y no hay auditorías ni calendarios de conservación, lo que compromete la preservación.
4. Usabilidad: La recuperación depende de Drive o del correo, no hay clasificación digital, no existen metadatos y el archivo físico es básico, lo que limita la localización y uso de información.

En conclusión, aunque la correduría muestra una disposición positiva hacia la mejora, es necesario consolidar una estructura formal de gestión documental que garantice la autenticidad.

4.2.5.2 LISTA VERIFICACIÓN ISO 30301

La lista de verificación aplicada bajo la norma 30301 tuvo como objetivo evaluar la implementación de un sistema digital de gestión documental dentro de Seguro Total, considerando su alineación con la estrategia organizacional y la gobernanza de la información.

El análisis permite identificar el grado de cumplimiento en cuanto a liderazgo, asignación de roles, definición de objetivos medibles, comunicación interna y control de riesgos asociados a la gestión documental.

Tabla 36: Lista verificación ISO 30301

N.º	Elemento por verificar	Cumple (Sí/No/En Proceso)	Comentarios / Evidencias
1	Se ha definido el contexto interno y externo de la	En proceso	Se conoce el contexto interno y externo de la empresa y

N.º	Elemento por verificar	Cumple (Sí/No/En Proceso)	Comentarios / Evidencias
	organización en relación con los documentos.		regulaciones, pero están asociadas más a la operatividad de la empresa frente a la CNBS.
2	Se han identificado las partes interesadas y sus requisitos respecto a los documentos.	Sí	Se ha identificado, pero no se ha puesto en marcha un proyecto para mejorar la gestión documental.
3	Está definido el alcance del Sistema de Gestión de Documentos (SGD).	No	El alcance del sistema de gestión documental actual no se encuentra definido o documentado.
4	Existe una política de gestión documental comunicada en toda la organización.	En proceso	Existe una política de gestión básica de solicitud, revisión y almacenamiento de documentación.
5	La alta dirección demuestra liderazgo y compromiso con el SGD.	Sí	Pudimos ver en las entrevistas y las pláticas con los líderes que están comprometidos a mejorar la gestión documental dentro de la organización.
6	Roles, responsabilidades y autoridades para el SGD están claramente definidos.	No	No existe actualmente una clara definición de roles y responsabilidades asociadas al SGD.
7	Se han identificado riesgos y oportunidades relacionados con la gestión documental.	Sí	Si se han identificado desde antes de la investigación puntos por mejorar y la investigación actual lo está complementando.
8	Existen objetivos medibles para la gestión documental y planes para lograrlos.	No	No existen objetivos establecidos asociados a la gestión de documentación por lo cual no se pueden medir o tomar acciones de corrección.
9	Se asignan recursos suficientes (humanos, tecnológicos, financieros).	Sí	La empresa ha asignado los recursos necesarios para mejorar la gestión documental y otras áreas para mejorar su competitividad.
10	El personal tiene competencia y recibe formación en gestión documental.	En proceso	El personal tiene experiencia en la gestión documental, pero necesita capacitaciones extras para ser más eficientes.
11	Existe concientización sobre la importancia de los documentos.	Sí	La documentación al ser una parte integral de la correduría concientiza a los internos y expresa la importancia de su gestión.

N.º	Elemento por verificar	Cumple (Sí/No/En Proceso)	Comentarios / Evidencias
12	Se definen y mantienen los canales de comunicación interna y externa sobre gestión documental.	En proceso	Existen canales parciales de comunicación, pero no una definición formal.
13	Se mantiene la documentación necesaria para el SGD (‘información documentada’).	En proceso	Si existe actualmente la documentación necesaria para el SGD, pero se debe revisar igualmente que esté actualizada.
14	Los procesos de gestión documental están planificados y controlados.	En proceso	Se encuentran parcialmente controlados, sin un proceso de revisión o verificación. Sí se encuentran planificados en cómo deben realizarse en el día a día.
15	Se determinan los documentos que deben crearse, conservarse y cómo hacerlo.	Sí	Si existe un control de cuáles documentos deben crearse, conservarse y cómo hacerlo.
16	Se implementan controles y sistemas para la gestión documental de forma efectiva.	En proceso	Se revisa de forma anual o cuando son las renovaciones de las pólizas que la información esté actualizada.
17	Se monitorean y miden los procesos del SGD.	No	Actualmente no se realiza.
18	Se realizan auditorías internas al SGD.	No	Actualmente no se realiza.
19	La alta dirección revisa regularmente el sistema de gestión documental.	No	Actualmente no se realiza.
20	Se gestionan no conformidades y acciones correctivas para el SGD.	No	Actualmente no se realiza.
21	Se promueve la mejora continua del SGD.	En proceso	Si se promueve a lo interno mejorar la gestión documental.

Nota: Elaborada por los autores

Podemos ver que la organización presenta ciertos avances importantes en la gestión documental, pero aún no tienen una madurez alta o completa con relación a esto. Se logra observar un correcto conocimiento del contexto interno y externo que afecta a la empresa en términos de gestión documental, pudiendo vincular esto que la dirección de la empresa está comprometida al identificar la gestión documental como un punto de mejora para realizar los cambios correspondientes para mejorar su efectividad.

Es importante resaltar que existen brechas relacionadas con una definición formal del alcance de un SGD, en donde podemos ver la falta de roles y responsabilidades en conjunto

con la ausencia de objetivos medibles para evaluar el desempeño de la gestión documental actual. Se logra visualizar también que existen procesos básicos, pero estos no están documentados o actualizados y en donde la comunicación interna entre los equipos no es la mejor.

Por último, podemos ver la ausencia de auditorías internas, revisiones por parte de la dirección, seguimiento de incidentes, por lo cual se limita la posibilidad de Detectar aquellos problemas con antelación para tomar acciones correctivas y aún más importantes acciones preventivas.

4.2.5.3 LISTA VERIFICACIÓN ISO 27001

La lista de verificación aplicada bajo la norma 27001 se aplicó con el propósito de analizar los controles de seguridad de la información presentes en Seguro Total, en relación con la confidencialidad, integridad y disponibilidad de los datos. Este instrumento evaluó la existencia de políticas de seguridad, roles definidos, inventarios de sistemas críticos, autenticación multifactor, gestión de vulnerabilidades y registro de incidentes.

Tabla 37: Lista verificación ISO 27001

N.º	Control adaptado	Aplicado (Sí/No)	Observaciones
1	La empresa cuenta con políticas internas de confidencialidad y resguardo de datos de clientes asegurados.	No	No existen actualmente políticas internas que los colaboradores firmen con respaldo legal para temas de confidencialidad y resguardo de la información.
2	Se han definido roles de seguridad de la información, incluyendo al responsable ante la CNBS.	No	No existe un rol como tal de la seguridad de la información.
3	Existe un inventario actualizado de sistemas críticos: plataforma de emisión de pólizas, CRM, bases de datos de clientes.	No	No se lleva un inventario de sistemas críticos. Internamente la correduría solo depende de Gmail, Google Drive, Microsoft Word, Microsoft Excel, PowerPoint y Adobe Acrobat.
4	El acceso a sistemas de pólizas y bases de datos está restringido por roles y autenticación multifactorial.	No	MFA no se utiliza.

5	Se gestionan vulnerabilidades en aplicaciones de clientes (web y móviles) y se validan con pruebas periódicas de seguridad.	No	No se realizan pruebas de vulnerabilidad y tampoco pruebas periódicas de seguridad.
6	Los datos personales y financieros de los asegurados se encuentran cifrados en reposo y en tránsito.	Parcial	Se utilizan los protocolos de seguridad inherentes de Google.
7	Se realizan pruebas de penetración enfocadas en portales de clientes y sistemas de pago electrónico.	No	No se realizan este tipo de pruebas.
8	Se cuenta con un registro de incidentes relacionados con fraude digital, fuga de datos o caídas de sistemas.	No	No se lleva un control o seguimiento de incidentes.
9	La organización revisa periódicamente los controles de seguridad conforme a ISO 27001, Ley de Protección de Datos y normativa CNBS.	No	Al no ser requisitos legales en Honduras aún no se emplean los controles de seguridad mencionados.

Nota: Elaborada por los autores

El análisis de la verificación ISO 27001 muestra que la correduría presenta un nivel de cumplimiento bajo en materia de seguridad de la información. No existen políticas formales de confidencialidad ni un responsable asignado para la gestión de la seguridad ante la CNBS. Asimismo, no se lleva un inventario actualizado de sistemas críticos ni se aplican controles de acceso mediante autenticación multifactor, lo que deja vulnerabilidades en los sistemas internos. Las pruebas de vulnerabilidad y de penetración tampoco se realizan, lo que limita la capacidad de Detectar riesgos y prevenir incidentes.

Por otro lado, aunque se utilizan algunos protocolos de seguridad provistos por las herramientas de Google, esto resulta insuficiente para garantizar la protección integral de los datos financieros y personales de los asegurados. No se cuenta con registros formales de incidentes ni con revisiones periódicas de los controles de seguridad conforme a la norma ISO 27001 o la Ley de Protección de Datos. En conjunto, estos resultados evidencian la necesidad urgente de establecer un sistema de gestión de seguridad de la información estructurado, con políticas, roles y procedimientos definidos que fortalezcan la confianza y el cumplimiento regulatorio.Con base a los controles oficiales de la Norma ISO 27001 encontramos los siguientes resultados generales:

A.5 – Políticas de seguridad: La empresa no posee políticas internas de seguridad ni acuerdos de confidencialidad, lo que incumple el marco mínimo requerido para proteger información sensible.

A.7 – Recursos humanos: No se han definido roles de seguridad de la información y el personal no recibe capacitación formal, lo que incrementa el riesgo de errores y fugas de datos.

A.8 – Gestión de activos: No hay inventario de sistemas críticos ni de activos tecnológicos; el entorno opera solo con herramientas básicas sin un control formal de los recursos que manejan datos sensibles.

A.9 – Control de accesos: No existe MFA, no hay restricciones por roles y no se gestionan vulnerabilidades, lo que permite accesos débiles y expone los datos de asegurados.

A.10 – Criptografía: El cifrado depende únicamente de los mecanismos nativos de Google, sin políticas adicionales que aseguren cifrado reforzado para datos personales y financieros.

A.11 – Seguridad física: No se mantiene control sobre dispositivos físicos ni sobre acceso a documentación, y los archivos físicos pueden ser manipulados libremente.

A.12 – Seguridad de operaciones: No se realizan pruebas de vulnerabilidad, no hay registro de incidentes y no se aplica monitoreo continuo, dejando sin control actividades críticas de operación.

A.18 – Cumplimiento legal: No se revisan controles ni cumplimiento regulatorio, y no existen mecanismos para atender requerimientos de una futura Ley de Protección de Datos o ante la CNBS, lo que genera riesgo de incumplimiento.

4.2.6 ANÁLISIS INSTRUMENTO DIRKS

La siguiente tabla presenta el inventario preliminar de documentos clave asociados a los procesos operativos, administrativos y de soporte de la correduría. Su elaboración tiene como objetivo identificar los tipos de documentos generados, sus responsables, formatos, tiempos de retención y disposición final, de acuerdo con las buenas prácticas establecidas por las normas ISO 15489 e ISO 30301.

Tabla 38: Análisis de Procesos y Documentación de Seguro Total

Proceso / Actividad	Tipo de Documento	Responsable de Generación	Formato	Tiempo de Retención	Disposición Final	Norma / Referencia
Emisión de pólizas	Póliza de seguro, anexos y	Asesor de seguros / Área	Digital (PDF), físico	10 años	Archivo histórico digital	CNBS, ISO 15489

	recibos	técnica				
Renovación de pólizas	Solicitud de renovación, cotización y confirmación del cliente	Asesor / Ejecutivo de cuentas	Digital (correo, PDF)	5 años	Eliminación controlada	ISO 15489
Gestión de siniestros	Formulario de reclamación, informes, resoluciones	Departamento de siniestros	Digital / físico según requerimiento	10 años	Archivo histórico	ISO 15489
Atención al cliente	Comunicaciones, reclamaciones, respuestas formales	Servicio al cliente	Digital (email)	3 años	Eliminación controlada	ISO 15489 / ISO 27001
Control contable y financiero	Comprobantes, facturas, recibos, conciliaciones	Contabilidad	Digital / físico	7 años	Archivo histórico	Normas tributarias, CNBS
Recursos Humanos	Expedientes de empleados, contratos, evaluaciones	RRHH	Digital / físico	5 años tras desvinculación	Eliminación controlada	Código Laboral / ISO 30301
Cumplimiento y auditoría	Reportes a la CNBS, políticas internas, registros de auditoría	Oficial de cumplimiento / Gerencia	Digital (PDF, Word)	Permanente	Conservación definitiva	CNBS / ISO 30301 / ISO 27001
Gestión comercial	Prospectos, cotizaciones, base de datos de clientes potenciales	Asesor comercial	Digital (Excel)	3 años	Eliminación controlada	ISO 15489

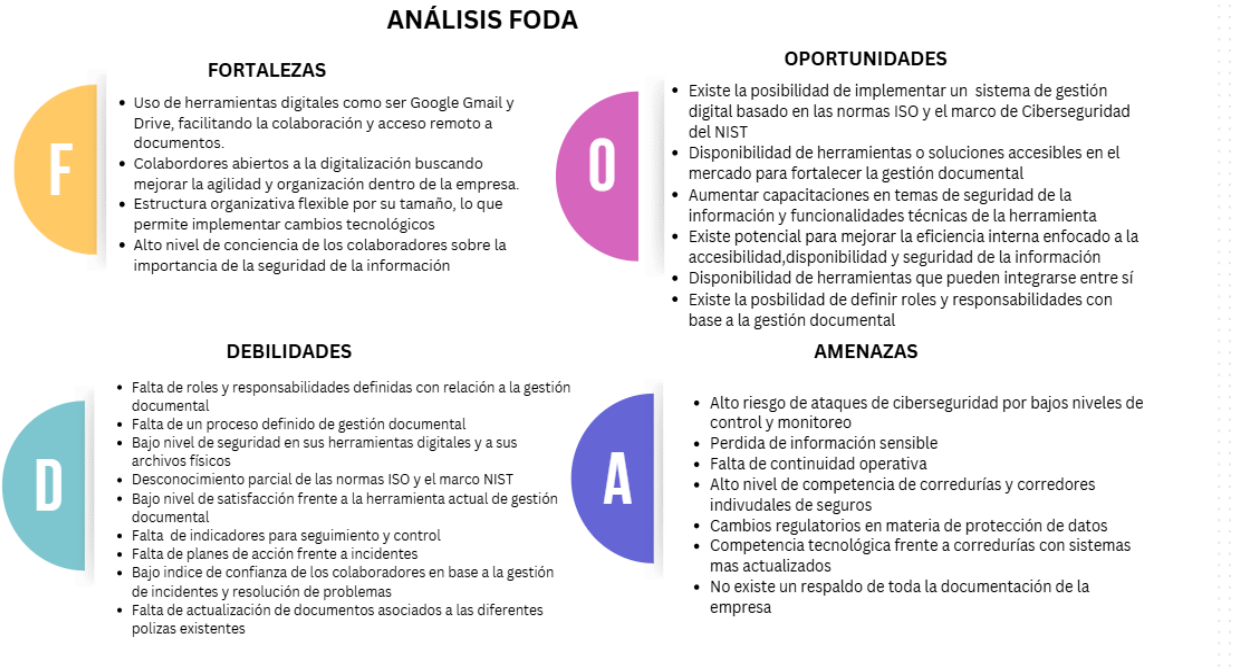
Gestión documental	Políticas, instructivos, formularios internos	Oficial administrativo	Digital	Permanente	Actualización continua	ISO 30301 / ISO 15489

Nota: Elaborada por los autores

4.2.7 HALLAZGOS PRINCIPALES FRENTE AL ANÁLISIS DE LA SITUACIÓN ACTUAL DE SEGURO TOTAL

Como parte fundamental de análisis de la situación actual de la correduría se creó la siguiente matriz FODA:

Figura 27: Matriz FODA



Nota: Elaborada por los autores

1. Nivel de conocimiento y cultura organizacional

- Conocimiento general sobre normas ISO relativamente alto (81.8%), pero muy limitado en normas aplicables, como ISO 27001, lo que evidencia una cultura informada pero no especializada.
- La mayoría comprende qué es gestión documental (81%), pero existe una percepción neutral o desfavorable sobre su aplicación práctica, lo que muestra una cultura organizacional que reconoce el concepto, pero que no vive los procesos.
- El personal cuenta con experiencia empírica, pero sin capacitación formal, reflejando un crecimiento no estructurado del conocimiento.

2. Procesos y prácticas actuales

- Procedimientos poco estructurados y falta de definición de roles y responsabilidades en el ciclo de vida documental (creación, actualización, eliminación).
- La gestión documental actual no contribuye de manera suficiente a la continuidad del negocio (63%), evidenciando ausencia de mecanismos de respaldo, planes de contingencia y manejo de incidentes.
- Las acciones de mejora son mínimas, poco comunicadas y con retroalimentación interna limitada.

3. Seguridad de la información

- Reconocimiento general de que la seguridad aplica a documentos físicos y digitales, pero sin controles concretos que lo acompañen.
- No existen mecanismos de autenticación reforzada (como MFA) ni revisiones periódicas, quedando la organización dependiente únicamente de la seguridad base de Google Drive.
- Falta de protocolos formales, lo cual deja brechas para accesos no autorizados, pérdida de información o alteración no trazada.

4. Tecnología y uso de herramientas

- A pesar de que la empresa ha invertido en recursos de transformación digital, no existe un sistema formal de gestión documental ni objetivos medibles para evaluar su eficiencia.
- El uso actual se limita a herramientas básicas, sin configuraciones avanzadas, auditorías, metadatos estándar ni políticas de conservación.

5. Colaboración y comunicación interna

- Baja coordinación y nivel de comunicación limitado entre colaboradores para la gestión documental, tanto digital como física, generando duplicidad, pérdida de documentos y retrasos.
- El 90% reconoce claramente que mejorar la gestión documental aportaría valor e impactaría positivamente en la imagen institucional, lo cual demuestra apertura al cambio y oportunidad para la adopción de un sistema más robusto.

6. Protección de la PII

- La empresa no aplica controles de seguridad sobre la PII almacenada en los documentos físicos y digitales.
- No se aprovechan al máximo los controles de seguridad de GSuite para fortalecer la protección del PII.

7. **Cumplimiento Normativo**
    - Alto riesgo de incumplimiento con estándares ISO 15489 e ISO 27001
8. **ISO 15489 — Gestión Documental (Procesos, Control, Organización)**
    - Ausencia de roles y responsabilidades documentales.
    - Procedimientos documentales no estandarizados.
    - Percepción neutral o negativa del sistema documental.
    - Uso no controlado y sin estandarización de archivos.
    - Gobernanza débil en unidades compartidas.
    - Colaboración interna sin control por roles o sensibilidad.
    - Falta de comunicación y coordinación en la gestión documental.
9. **ISO 30301 — Sistema de Gestión Documental**
    - Transformación digital sin métricas ni objetivos definidos.
    - Falta de políticas formales de uso y acceso.
    - No existe inventario ni control de dispositivos corporativos.
    - Personal sin capacitación formal en gestión documental.
    - Ausencia de mecanismos que garanticen continuidad del negocio.
    - Retroalimentación interna mínima y poca divulgación de mejoras.
10. **ISO 27001 — Seguridad de la Información**
    - Autenticación multifactor no obligatoria.
    - Políticas de contraseñas sin rotación ni restricciones de reutilización.
    - Verificación de identidad adicional desactivada.
    - Protecciones incompletas contra programa maligno, phishing y correos no autenticados.
    - Alto porcentaje de correos sensibles enviados a externos.
    - Falta de inventario de activos que acceden al sistema.
    - Permisos amplios en unidades compartidas y descargas.
    - Controles de phishing parcialmente activos.
11. **NIST CSF —Identificar**
    - Falta de inventario de activos tecnológicos.
    - Ausencia de clasificación y categorización de información.
    - Roles y responsabilidades no definidos.
    - Políticas de seguridad insuficientes o inexistentes.
12. **NIST CSF — Proteger**

- Autenticación multifactor no obligatoria.
- Controles de contraseñas incompletos.
- Configuraciones de uso compartido con baja restricción.
- Protección parcial contra phishing y programa maligno.
- Falta de control sobre dispositivos que acceden al sistema.
- Capacitación limitada en seguridad de la información.

13. **NIST CSF —Detectar**
    - Monitoreo limitado de accesos sospechosos.
    - Protecciones desactivadas para correos no autenticados.
    - Falta de alertas avanzadas para actividades inusuales.
14. **NIST CSF — Responder**
    - Ausencia de protocolos claros de respuesta a incidentes.
    - Comunicación interna débil para manejo de eventos.
15. **NIST CSF —Recuperar**
    - Falta de mecanismos formales para continuidad del negocio.
    - No existen lineamientos para recuperación ante pérdida o daño de información.

4.3 REVISIÓN DE PLATAFORMAS DOCUMENTALES: FUNCIONALIDAD, SEGURIDAD Y EFICIENCIA OPERATIVA

Figura 28: Instrumentos aplicados relacionados al Objetivo 2

Nota: Elaborada por los autores

Como se muestra en la figura 24, el objetivo 2 busca evaluar diferentes herramientas tecnológicas de gestión documental y seguridad de la información con el fin de identificar la solución más adecuada para la correduría Seguro Total. La evaluación se fundamente en

requisitos derivados de las normas ISO 30301, ISO 27001 y el marco NIST de ciberseguridad, los cuales permiten determinar que plataformas garantizan mayor trazabilidad, seguridad, automatización y gobernanza documental dentro de una MiPyme del sector asegurador hondureño.

4.3.1 METODOLOGÍA Y CRITERIOS UTILIZADOS PARA EVALUACIÓN

Para la identificación de la herramienta más adecuada, se aplicó una metodología comparativa que integra criterios normativos, técnicos y operativos, dicho proceso se desarrolla en tres etapas clave:

a) Etapa 1: Definición de criterios normativos internacionales

   Se analizaron los requisitos fundamentales de las normas ISO 30301 (Sistema de gestión para documentos), ISO 27001 y el marco NIST de Ciberseguridad. Estos estándares fueron seleccionados debido a su capacidad para orientas prácticas de gobernanza documental, trazabilidad, autenticidad, integridad de la información y protección de datos.

   A partir de ellos, se definen criterios que permitieron evaluar:

   - Eficiencia del ciclo de vida documental
   - Correcta gestión de versiones, retención y disposición
   - La existencia de trazabilidad y auditoria
   - Nivel de control de accesos, cifrado y protección contra incidentes
   - Capacidad de retención y recuperación ante fallas e incidentes

a) Etapa 2: Definición de criterios operativos

   Además del cumplimiento normativo, se consideran criterios operativos que impactan directamente en la adopción organizacional, lo cuales son:

   - Facilidad de uso y curva de aprendizaje
   - Invasión inicial y modelo de licenciamiento
   - Escalabilidad en almacenamiento y usuarios
   - Experiencia del usuario y accesibilidad
   - Frecuencia y tipo de actualizaciones
   - Integración con plataformas institucionales como Google Works pace o Gmail
   - Funcionalidad clave como OCR, Firma digital, automatización de flujos, auditoria y metadatos

a) Etapa 3: Construcción de la matriz comparativa

Se evaluaron soluciones como Google Drive, M-Files, DocuWare, Alfresco, OpenKM y SharePoint mediante:

- Matriz Cualitativa, que determina el nivel de cumplimiento por criterio
- Matriz ponderada, permite establecer rankings basado en pesos porcentuales asignado a cada dimensión

Dicha metodología permitirá comparar herramientas de manera equilibrada considerando las necesidades y la madurez operativa que ofrece como la viabilidad operativa.

4.3.2 ANÁLISIS DE MATRIZ DE EVALUACIÓN DE HERRAMIENTAS

El propósito de esta evaluación fue identificar las soluciones tecnológicas que integran de manera más eficiente los principios de gobernanza documental, seguridad de la información y automatización de procesos, con el fin de establecer una referencia sólida para el diseño del sistema digital propuesto en esta investigación.

El estudio consideró tanto plataformas comerciales (como M-Files, DocuWare, Alfresco, Google Drive, SharePoint y Dropbox Business) como alternativas de código abierto (como OpenKM), valorando su madurez tecnológica, nivel de cumplimiento con los estándares internacionales y su viabilidad de adopción en una MiPyme del sector asegurador hondureño.

Para garantizar un análisis integral, se establecieron siete criterios de evaluación:

1. Seguridad: mecanismos de cifrado, autenticación y trazabilidad.
2. Facilidad de uso: simplicidad de la interfaz y curva de aprendizaje.
3. Inversión inicial: requerimientos de licenciamiento e infraestructura.
4. Actualizaciones: periodicidad y tipo de mantenimiento.
5. Cumplimiento normativo: alineación con las normas ISO 30301, ISO/IEC 27001 y el Marco NIST.
6. Experiencia del usuario: adaptabilidad e integración con herramientas de trabajo colaborativo.
7. Funcionalidades clave: control de versiones, flujos de trabajo, auditoría, gestión de metadatos y políticas de retención.

La Tabla 36 sintetiza los resultados obtenidos, permitiendo contrastar las capacidades de cada sistema en función de los requerimientos de Seguro Total. Este análisis constituye una base de referencia para el diseño del modelo propuesto, orientado a garantizar la trazabilidad,

seguridad y eficiencia en la gestión documental conforme a las mejores prácticas internacionales

Tabla 39: Matriz de Análisis de Herramientas

Herramienta	Seguridad	Facilidad de uso	Inversión inicial	Actualizaciones	Cumplimiento normativo	Experiencia del usuario	Funcionalidades claves
Google Drive	Buena: cifrado en tránsito y reposo, permisos granulares; limitada trazabilidad para auditorías formales	Muy alta: interfaz sencilla y conocida por la mayoría de los usuarios.	Muy baja: ya está implementado; sólo implica ampliar almacenamiento o licencias	Automáticas, incluidas en Google Workspace	Cumple con ISO 27001, GDPR si se configura correctamente; carece de módulo de gestión de registros.	Excelente colaboración y trabajo remoto.	Almacenamiento en nube, control de versiones, uso compartido, comentarios, sincronización con Gmail y Docs.
M-Files	Excelente: cifrado, control de acceso, autenticación multifactor y registro de auditoría	Media-alta: interfaz profesional, requiere breve capacitación	Media-alta: licenciamiento empresarial por usuario	Frecuentes, controladas por el proveedor.	Cumple ISO 9001, ISO 27001, GDPR, HIPAA	Fluida tras adopción; integración con Outlook y procesos internos	Gestión basada en metadatos, automatización de flujos, búsqueda inteligente, auditoría
DocuWare	Muy alta: cifrado extremo, roles, autenticación segura,	Media: requiere entrenamiento, interfaz web amigable	Media: modelo SaaS con pago mensual o anual	Automáticas en la nube; mejoras de seguridad y flujos	Cumple ISO 9001, ISO 27001, SOC 2, GDPR	Fácil aprobación, firma y archivo de documentos	Captura de documentos, automatización de flujos, firma

Herramienta	Seguridad	Facilidad de uso	Inversión inicial	Actualizaciones	Cumplimiento normativo	Experiencia del usuario	Funcionalidades claves
	backup redundante						digital, indexación por cliente
Alfresco (Hyland)	Alta: cifrado, control de acceso, trazabilidad y registros detallados	Media: potente, pero requiere configuración técnica inicial.	Media-alta: software libre base con costos de implementación	Regulares; depende de versión instalada	Cumple ISO 15489, DoD 5015.02, ISO 16175).	Buena para usuarios técnicos o archivistas	Gestión de registros, flujos de aprobación, integración con CRM/ERP
OpenKM	Alta: control de usuarios, auditoría, cifrado, opción on-premise	Media: interfaz funcional, menos intuitiva que Drive.	Baja-media: opción open source o cloud con costos bajos	Actualizaciones comunitarias o contratadas	Cumple ISO 15489 y trazabilidad completa	Aceptable, interfaz básica pero estable	OCR, flujos de aprobación, clasificación por cliente, versionado
SharePoint (Microsoft 365)	Alta: cifrado, autenticación multifactor, permisos avanzados	Media-alta: interfaz moderna, requiere adopción inicial	Media: licenciamiento por Microsoft 365	Continuas, integradas con Microsoft 365	Cumple ISO 27001, SOC 12, GDPR	Buena integración con Teams y Office	Colaboración en línea, flujos Power Automate, control de versiones, búsqueda avanzada
Dropbox Business	Alta: cifrado AES256 y TLS, gestión de identida	Muy alta: interfaz intuitiva y conocida	Media: suscripción mensual o anual por usuario	Automáticas y frecuentes	Cumple ISO 27001, SOC 123, GDPR	Experiencia muy fluida, ideal para PYMEs.	Sincronización automática, historial de versiones, carpetas Smart

Herramienta	Seguridad	Facilidad de uso	Inversión inicial	Actualizaciones	Cumplimiento normativo	Experiencia del usuario	Funcionalidades claves
	d, control de acceso						Sync

Nota: Información obtenida de (Crest Infosolutions, 2025), (Pichur, 2017), (Schuckmann, 2021)

(DocuWare Europe GmbH, s.f.), (Dropbox, s. f.), (Dropbox, s.f.), *M-Files Security Insights: Simplified Overview*, 2025), (*Trust Center Security And Compliance*, s. f.), ((*Security, Privacy & Compliance for Government*, 2025), (Hyland Software, 20), (, (*Cloud Data Integrity and Compliance | Microsoft Trust Center*, s.f), (Paulhickey, 2025), (Novatech., 2025), (OpenKM, s.f.), (De Lucca Caetano, 2025).

Tabla 40: Matriz de Análisis de Herramientas Puntaje

Criterio	Peso (%)	Google Drive	M-Files	DocuWare	Alfresco	OpenKM
Seguridad	20 %	4	5	5	4	4
Facilidad de uso	15 %	5	4	4	3	3
Inversión inicial	10 %	5	3	3	3	4
Actualizaciones	10 %	5	5	5	3	3
Cumplimiento normativo	20 %	3	5	5	4	4
Experiencia del usuario	10 %	5	4	4	3	3
Funcionalidades clave (flujos, trazabilidad, firma, OCR, etc.)	15 %	3	5	5	4	4
Puntaje total ponderado (de 5)	**100 %**	**4.1**	**4.7**	**4.6**	**3.6**	**3.8**

Nota: Elaborada por los autores

Considerando la tabla 37, los resultados obtenidos mediante la evaluación ponderada de las herramientas de gestión documental muestran diferencias significativas en cuanto a madurez funcional y una clara facilidad de la adopción. En la primera fase del análisis se elaboró una

matriz comparativa cualitativa, donde se examinaron plataformas reconocidas como Google drive, M-Files, DocuWare, Alfresco (Hyland), OpenKM, SharePoint y Dropbox business. Criterios como seguridad, facilidad de uso, inversión inicial, actualizaciones, cumplimiento normativo, experiencia del usuario y funcionalidades clave.

La primera evaluación permitió identificar que Google Drive (actualmente utilizados) y Dropbox Business destacan claramente por su accesibilidad, facilidad de adopción y bajo costo inicial, presentan limitaciones importantes con trazabilidad, control de auditoría y gobierno de la información o gobierno en TI, lo cual es una clara desventaja y también una forma de restricción para ser aplicado en contextos donde se requiera evidencia documental y cumplimiento regulatorio. A su vez, soluciones como las que proporciona M-Files y DocuWare demostraron una mayor alineación con los principios de las normas ISO 15489, ISO 30301 e ISO 27001, al incorporar gestión basada en metadato, controles de versionamiento, autenticación multifactorial, registro de auditoría y automatización de flujos de trabajo.

De igual manera Alfresco y OpenKM, de código abierto ofrecen flexibilidad técnica y personalizable, pero demandan un esfuerzo grande en documentación y configuración, así como, soporte técnico específico y una constante capacitación al usuario lo que puede representar una limitante gradual para una MiPymes de servicios aseguradores como Seguros total. Los resultados mostraron que M-Files y DocuWare son las alternativas más completas y equilibradas, ya que integran altos niveles de seguridad, trazabilidad, automatización de flujos y controles normativos. Por su parte, Google Drive se mantiene como una opción práctica y fácil de usar, aunque con limitaciones en control de acceso y auditoría. En cambio, OpenKM y Alfresco, pese a ser flexibles y de código abierto, requieren configuraciones avanzadas, soporte técnico especializado y una constante capacitación al usuario, lo que puede representar una carga adicional para una MiPyME como Seguro Total.

En Términos de seguridad estas dos herramientas incorporan controles avanzados de cifrado en tránsito y reposo, autenticación multifactorial, gestión de permisos basados por roles y auditoria integral garantizando una trazabilidad completa y adecuada conforme a lo que hace mención la ISO 27001 y funciones de identificación, protección y detección del Marcos se ciberseguridad que ofrece el NIST.

Respecto al cumplimiento normativo, tanto M-Files como DocuWare cuentan con certificaciones que respaldan su conformidad con los estándares internacionales de calidad y seguridad (ISO 9001, ISO 27001, GDPR y HIPAA), lo cual les otorga una ventaja frente a soluciones genéricas. Basado en la facilidad de uso y experiencia del usuario, Drive por sus facilidades sigue siendo por decisión del usuario la opción más intuitiva y familiar para los

colaboradores, mientras que las otras herramientas mencionadas como M-Files y DocuWare ofrecen interfaces adaptables al negocio pero que requieren una capacitación y curva de aprendizaje mucho más amplia. De igual manera el factor inversión es un punto para considerar, se tienen herramientas basadas en licenciamiento empresarial donde el costo implicado es mayor que las opciones en la nube de suscripción individual pero este costo va basado en factores como capacidades avanzadas, automatización y trazabilidad, cosas que son fundamentales para una arquitectura sólida y certificable.

Finalmente, en cuanto a funcionalidades clave, las soluciones líderes integran flujos de aprobación, versionado, control de metadatos, firma electrónica, OCR y retención automatizada de documentos, elementos indispensables para una gestión documental conforme a la ISO 30301:2019 y para la transición hacia un sistema de gobernanza digital resiliente.

En síntesis, el análisis evidencia que M-Files y DocuWare constituyen referentes tecnológicos idóneos para el diseño del Sistema Digital de Gestión Documental de Seguro Total, al combinar altos niveles de seguridad, cumplimiento normativo, trazabilidad y automatización. Dicho esto, las características funcionales sirven como modelo base para la definición de la arquitectura propuesta en el objetivo 3, garantizando que el sistema final sea estandarizado, seguro, escalable y alineado con las mejores prácticas internacionales de gestión documental.

4.3.3 ANÁLISIS DE MATRIZ DE EVALUACIÓN DE HERRAMIENTAS

El análisis normativo y funcional permite determinar el grado en que cada herramienta evaluada se alinea con los requisitos de gestión documental, seguridad de la información y ciberseguridad establecidos por los estándares internacional ISO 30301, ISO 27001 y el marco de ciberseguridad NIST. Considerando eso, se presenta una síntesis comparativa de los hallazgos con respecto a las matrices.

1. Cumplimiento de la norma ISO 30301

- M Files y DocuWare presentan mayor nivel de alineación con ISO 30301, ya que soportan de manera completa el ciclo de ida documental, la gestión por metadatos, retención y disposición automatizada, así como, el control de versiones y trazabilidad. Sus módulos de auditoria permiten mantener evidencia verificable del acceso y modificación de registros
- Alfresco y OpenKM ofrecen capacidades avanzadas de gestión documental,

incluyendo clasificación, versionamiento y flujos de trabajo. Sin embargo, requiere configuraciones técnicas complejas y personal especializado para alcanzar un nivel de cumplimiento comparable con soluciones más comerciales

- Google Drive y Dropbox Business cumplen parcialmente con esta norma, si bien permiten colaboración eficiente, control básico de versiones y accesibilidad. Estas soluciones no integran módulos formales de retención, auditorio documental estructurada ni clasificación archivista, lo que impide su alineación directa con un sistema de gestión documental
- SharePoint ofrece una gestión solida en metadatos, versionamiento, flujos de aprobación y auditoria. Sin embargo, su implementación inicial puede ser compleja para una MiPymes sin soporte técnico especializado

2. Cumplimento de la norma ISO 27001

- M-Files, DocuWare y SharePoint cumplen de forma robusta los principales controles de ISO 27001:
    - A.9: control de accesos,
    - A.10: cifrado en tránsito y en reposo,
    - A.12: seguridad operativa y respaldo,
    - A.13: comunicaciones y transferencia segura de información,
    - A.23: seguridad en servicios cloud.
- Google Drive cumple con ISO 27001 y GDPR, pero sus capacidades avanzadas, permisos altamente granulares y trazabilidad requieren configuraciones adicionales o herramientas complementarias, lo que limita su aplicabilidad en entornos con alta exigencia regulatoria.
- Open KM y Alfresco su cumplimiento depende en gran medida del entorno donde se despliegue y la capacidad del personal técnico para implementar medidas de monitoreo, autenticación robusta y cifrado. Esto introduce riesgos operativos cuando no hay recursos especializados

4.3.4 RESULTADOS DEL CUESTIONARIO APLICADOS A LOS USUARIOS

Con base al cuestionario las siguientes preguntas fueron utilizadas y analizadas para tener un mayor entendimiento del funcionamiento y satisfacción del uso de la herramienta actual de gestión documental qué es “Google Drive” mediante su funcionalidad de “Google Docs”.

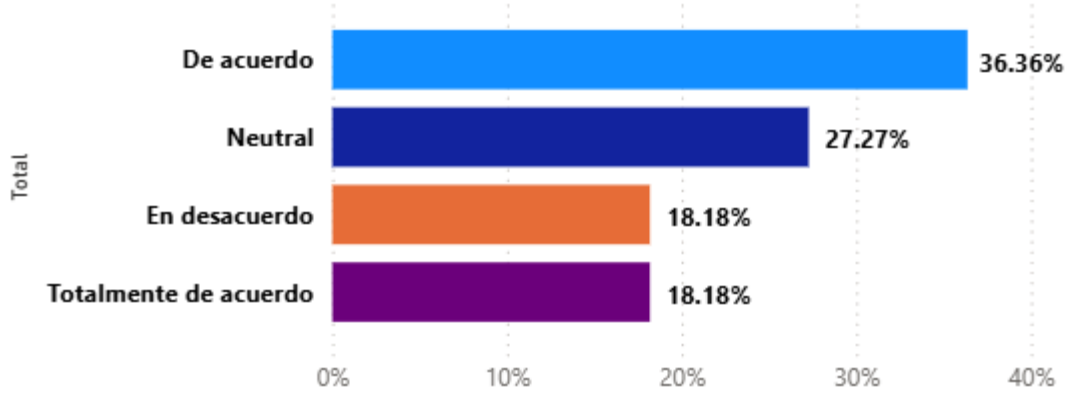
Tabla 41: Preguntas Cuestionario relacionadas al Objetivo 2

Objetivo 2
3. Considero que los procesos para archivar o digitalizar documentos son rápidos y eficientes.
4. Los documentos importantes se mantienen accesibles en todo momento.
5. El sistema o plataforma que usamos para manejar documentos es fácil de aprender y utilizar.
6. Puedo acceder a la información desde diferentes lugares o dispositivos cuando lo necesito.
7. El sistema tiene funciones útiles como búsqueda rápida, control de versiones y permisos de acceso.
8. Confío en que la información almacenada está protegida frente a pérdidas o accesos indebidos.

Nota: Elaborada por los autores

Para analizar la herramienta actual de gestión documental, se inició evaluando la eficiencia de los procesos de archivo y digitalización (pregunta tres), seguido de la facilidad de uso (preguntas cuatro y seis), las funcionalidades del sistema (pregunta siete) y la percepción sobre la seguridad de los datos (pregunta ocho). Este orden nos permite comprender de manera progresiva cómo los usuarios perciben actualmente el desempeño y funcionalidad de la herramienta. La de estas preguntas se utilizó una escala de Likert como se menciona en la sección de Descripción General de Instrumentos.

Gráfico 36: ¿Considero que los procesos para archivar o digitalizar documentos son rápidos y eficientes?

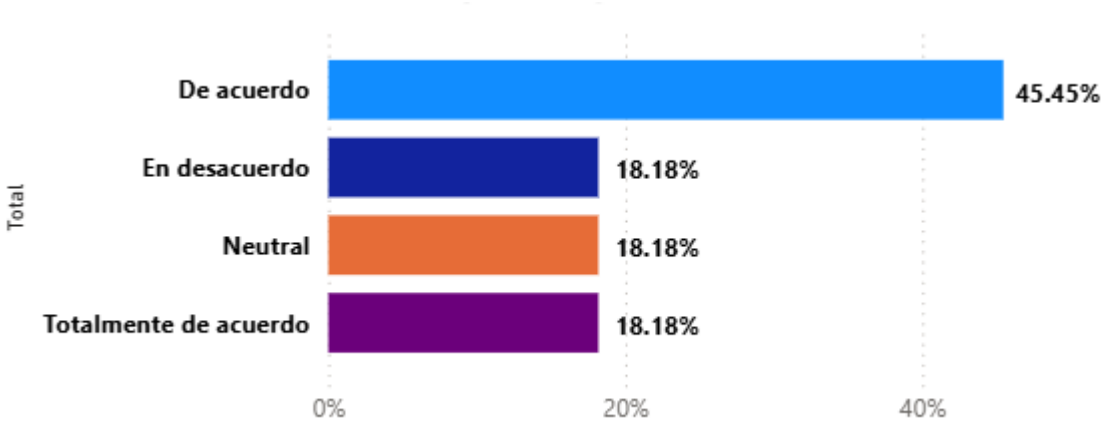


Nota: Elaborada por los autores

El gráfico presenta la distribución de las respuestas relacionadas con la eficiencia y rapidez en los procesos de digitalización. Se observa que el 36.36% de los colaboradores selecciono la opción “De acuerdo”, mientras que un 27.27% respondieron “Neutral”, Asimismo, un 18.18% indico estar “En Desacuerdo” y un 18.18% adicional selecciono la categoría “Totalmente en desacuerdo”

Como se observa en la imagen anterior, aproximadamente el 54 % de los usuarios dentro de la correduría considera que los procesos actuales relacionados con la documentación física y su digitalización son buenos o cumplen adecuadamente su función. Sin embargo, se evidencia que cinco usuarios mantienen una posición neutral o en desacuerdo, un 46 % que no está completamente satisfecho con la forma en que se están realizando los procesos actuales. Esto nos indica la necesidad de revisar los procedimientos actuales y explorar oportunidades de mejora en la eficiencia operativa.

Gráfico 37: El sistema o plataforma que usamos para manejar documentos es fácil de aprender y utilizar.

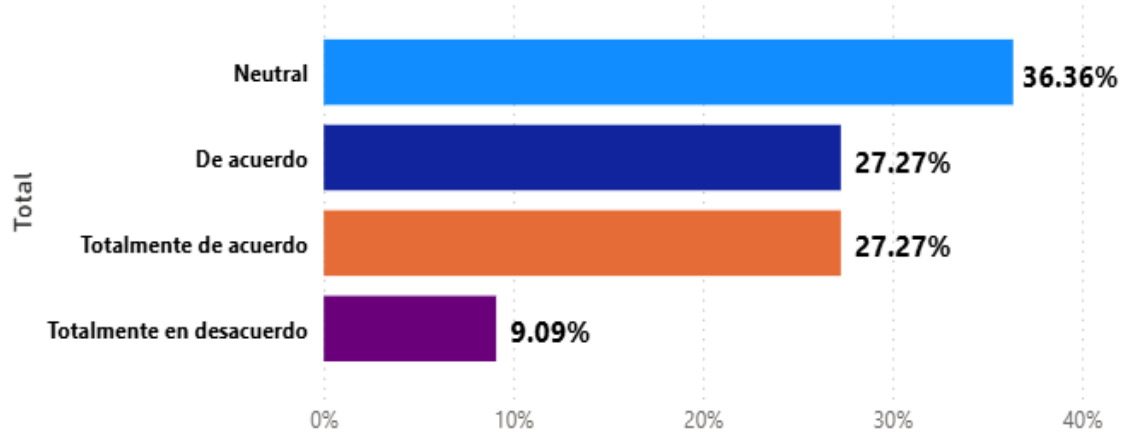


Nota: Elaborada por los autores

El gráfico presenta la distribución de las respuestas relacionadas con la facilidad de uso del sistema o plataforma utilizada para manejar documentos. El 45.45% de los colaboradores seleccionados “De acuerdo”, y un 18.18% respondieron “En desacuerdo”, como un 18.18% manifestó una postura “Neutral” y otro 18.18% indico estar en “Totalmente de acuerdo”.

Actualmente, la correduría utiliza Google Drive y el correo corporativo de Gmail como herramientas principales para almacenar y transferir información tanto entre los usuarios internos como con clientes y proveedores. En este sentido, el 63 % de los colaboradores manifestó estar de acuerdo o totalmente de acuerdo con la facilidad de uso y aprendizaje de la herramienta. Este resultado refuerza los hallazgos obtenidos en la matriz comparativa de herramientas, donde se destaca que Google Drive cumple con criterios críticos de usabilidad y simplicidad, factores determinantes para su adopción en organizaciones pequeñas y medianas.

Gráfico 38: Los documentos importantes se mantienen accesibles en todo momento.

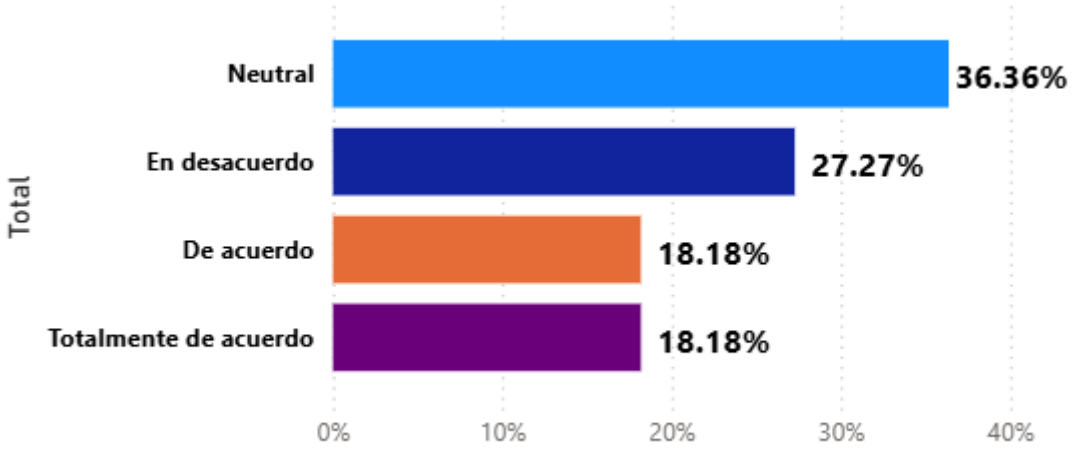


Nota: Elaborada por los autores

El gráfico presenta la distribución de las respuestas relacionadas con la accesibilidad de los documentos importantes dentro de la organización. Se observa que el 36.36% de los colaboradores seleccionaron la opción “Neutral”, mientras que un 27.27% indico estar “De acuerdo” y otro 27.27% eligió “Totalmente de acuerdo”. Finalmente, el 9.09% selecciono la categoría “Totalmente en desacuerdo”.

Con relación con la accesibilidad de la información, los resultados muestran que el 54 % de los usuarios percibe que los documentos importantes permanecen accesibles en todo momento, evidenciando una buena organización del almacenamiento digital.

Gráfico 39: Puedo acceder a la información desde diferentes lugares o dispositivos cuando lo necesito.



Nota: Elaborada por los autores

El gráfico presenta la distribución de respuestas relacionadas con la posibilidad de acceder a la información desde diferentes lugares o dispositivos cuando es necesario. Se observa que el 36.37% de los colaboradores selecciono la opción “Neutral”, mientras que un 27.27% indico estar “En desacuerdo”. Asimismo, el 18.18% eligió la categoría de acuerdo y otro 18.18% selecciono “Totalmente de acuerdo”.

Sin embargo, al analizar la posibilidad de acceder a la información desde diferentes lugares o dispositivos, el panorama cambia: el 63 % de los colaboradores se mostró neutral o en desacuerdo, lo que sugiere limitaciones en la movilidad y accesibilidad remota de los archivos.

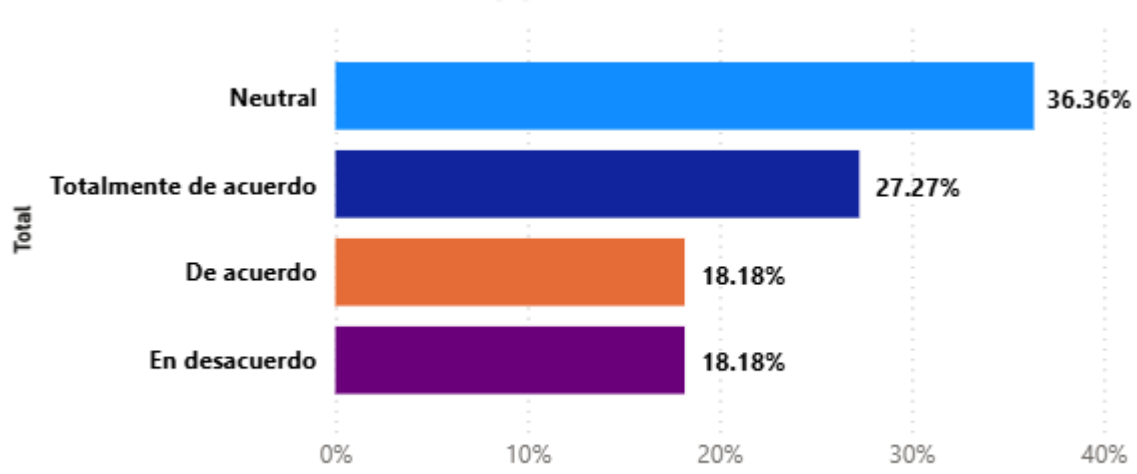
A pesar de estos resultados, es importante considerar dos factores contextuales:

1. Todos los usuarios trabajan de forma presencial en las oficinas de la correduría, por lo que no se requiere y no se permite acceso desde ubicaciones externas.
2. Por motivos de seguridad, los accesos desde dispositivos personales o no corporativos están restringidos, ya que los colaboradores cuentan con teléfonos y equipos institucionales para realizar sus tareas.

En conjunto, los resultados evidencian que la herramienta actual cumple adecuadamente con los aspectos básicos de usabilidad y accesibilidad local, aunque existen oportunidades de mejora en la eficiencia de los procesos y en la definición de políticas de acceso remoto seguras

que equilibren la productividad con la protección de la información.

Gráfico 40: El sistema tiene funciones útiles como búsqueda rápida, control de versiones y permisos de acceso.

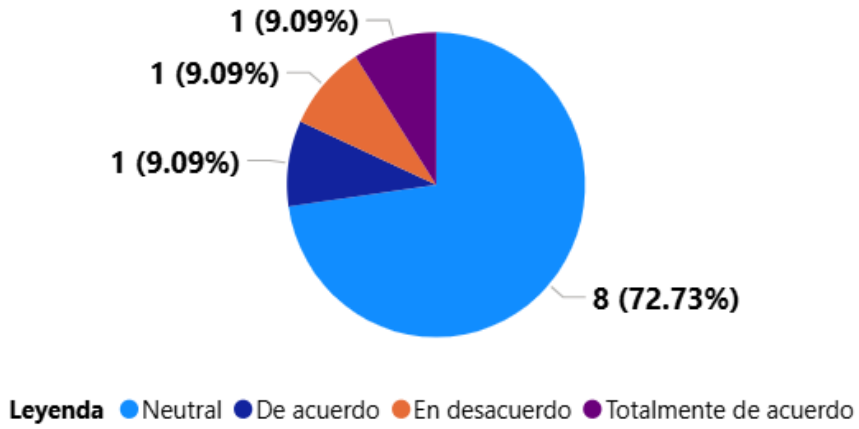


Nota: Elaborada por los autores

El gráfico presenta la distribución de las respuestas relacionadas a la percepción de los colaboradores respecto a las funciones disponibles en el sistema, tales como la búsqueda rápida, control de versiones y permisos de acceso. Se observa que el 36.36% selecciono la opción "Neutral", mientras que un 27.27% indico estar "totalmente de acuerdo". Por su parte, el 18.18% eligió "De acuerdo" y otro 18.18% selecciono la categoría "En desacuerdo".

De la misma forma, se observa que la percepción general sobre el sistema de Google Drive y Gmail es mixta entre los colaboradores. En los resultados, seis usuarios manifestaron una postura entre "Neutral" y "En desacuerdo", mientras que cinco usuarios indicaron estar "De acuerdo" o "Totalmente de acuerdo". Esta distribución refleja que no existe una opinión plenamente consolidada respecto a la satisfacción con las funciones actuales del sistema.

Gráfico 41: ¿Confío en que la información almacenada está protegida frente a pérdidas o accesos indebidos?



Nota: Elaborada por los autores

El gráfico presenta la distribución de las respuestas relacionada con la confianza de los colaboradores con la protección de la información almacenada frente a perdidas o accesos indebidos. Se observa que el 72.72% selecciono la opción “Neutral”, mientras que un 9.09% indico estar “De acuerdo”. Asimismo, un 9.09% eligió “En desacuerdo” y otro 9.09% selecciono “Totalmente de acuerdo”.

En cuanto a la seguridad de la información, el 72 % de los colaboradores mantiene una postura neutral sobre si la herramienta protege de permite y protege frente a pérdidas o accesos indebidos, lo cual resulta llamativo considerando la reconocida reputación de Google en materia de ciberseguridad. De acuerdo con la matriz comparativa de herramientas, Google Drive cumple con normativas internacionales como ISO 27001 y GDPR, y ofrece altos estándares de protección, incluyendo cifrado en tránsito y en reposo, así como permisos de acceso granulares.

Estos resultados sugieren que, aunque la plataforma brinda altos niveles de seguridad técnica, existe una brecha de percepción o desconocimiento entre los usuarios respecto a dichas capacidades. Por lo tanto, sería conveniente reforzar la comunicación interna y la capacitación sobre las políticas de seguridad implementadas y las funcionalidades que garantizan la protección de la información dentro de la correduría.

4.3.5 ANÁLISIS DE RESULTADOS DEL CUESTIONARIO APLICADO A LOS USUARIOS

Con el fin de complementar la evaluación técnica de las herramientas, se desarrolló un cuestionario a los colaboradores de Seguros total, para conocer su experiencia y percepción sobre la herramienta que se utiliza actualmente (Google Drive). Dichos resultados permiten identificar brechas reales en el uso cotidiano del sistema versus con los hallazgos en la matriz comparativa.

Mediante el cuestionario se pueden identificar factores como:

a. Eficiencia en procesos de digitalización
b. Facilidad de uso
c. Accesibilidad a la información
d. Acceso desde múltiples dispositivos
e. Funcionalidades percibidas
f. Seguridad percibida

4.3.6 HALLAZGOS PRINCIPALES RELACIONADOS AL ANÁLISIS DE HERRAMIENTAS DE GESTIÓN DOCUMENTAL

El análisis combinado de los instrumentos aplicados a los usuarios permite sintetizar los principales hallazgos que orientan la selección de la herramienta más adecuada para Seguros total. Estos hallazgos se agrupan dimensiones como:

a. Hallazgo de mercado

El análisis de mercado evidencia una clara diferencia entre las soluciones empresarial y las open source, las plataformas robustas como M-Files y DocuWare presentan un costo más elevado debido a que integran capacidades avanzadas de trazabilidad, automatización, auditoria, retención documental y seguridad. Estas funciones son indispensables para organizaciones que manejan información sensible y requiere una protección a la altura.

Por otro lado, herramientas de código abierto como OpenKM o Alfresco ofrecen flexibilidad técnica y posibilidades de personalización, pero demandan un amplio esfuerzo en configuración y mantenimiento lo que puede traducirse en una cara operativa gigante para un MiPyme.

b. Hallazgo de cumplimiento normativo

El cumplimiento normativo es uno de los aspectos más críticos del análisis, se observa un número reducido de plataformas cumplen de manera nativa y adecuada los requisitos de la ISO 30301 relacionado con gestión documental formal, trazabilidad, retención, autenticidad y control de versiones.

Las herramientas certificadas bajo ISO 27001 y alineadas al marco NIST de ciberseguridad ofrecen mayores garantías en cuanto a seguridad, auditoria, protección de datos y recuperación ante incidentes. En contrastes, Google Drive, si bien cumple con la norma ISO 27001 como infraestructura cloud, carece de mecanismos de gestión documental estructurada y depende de configuraciones adicionales para alcanzar un nivel de trazabilidad acorde a los requerimientos de una organización aseguradora.

c. Hallazgos sobre las necesidades específicas de Seguro total

El diagnostico muestra los que seguro total tiene múltiples necesidades y requiere una solución que brinde:

- Trazabilidad completa
- Meta data estructurada
- Automatización de flujos de aprobación
- Control de versiones adecuado
- Retención documental.

Asimismo, la solución seleccionada debe reducir al mínimo la dependencia de personal técnico ya que la empresa no cuenta con un departamento de TI especifico, se requiere una herramienta que permita mantenimiento sencillo.

d. Hallazgos de riesgo

Herramientas como OpenKm y Alfresco presentan riesgo debido a su alta dependencia de configuraciones manuales, lo cual incrementa la posibilidad de errores, inconsistencia o vulnerabilidades cuando la organización no cuenta con un equipo técnico especializado.

Las plataformas sin mecanismos nativos de monitoreo o alerta de seguridad dificultan la detección de incidente lo que presenta un riesgo para una empresa que maneja información sensible.

En el caso de drive presenta limitaciones como:

- Ausencia de auditoria granular
- Falta de retención estructurada

- Imposibilidad de garantizar evidencia documental

e. Hallazgos estratégicos

Desde la perspectiva estratégica, tanto M-Files como DocuWare destacan como las alternativas más equilibradas ya que combinan:

- Alto cumplimiento normativo
- Trazabilidad completa
- Escalabilidad a mediano y largo plazo
- Automatización de procesos

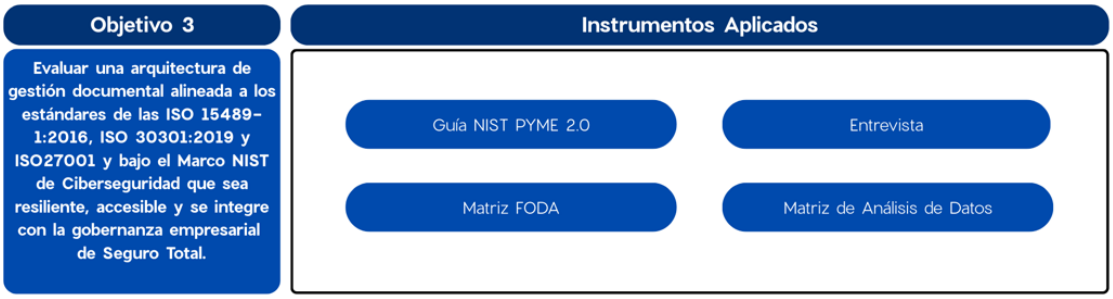
Estas capacidades posicionan a ambas herramientas como las opciones más adecuadas para sustentar una futura certificación de procesos documentales y para soportar el diseño de la arquitectura necesaria.

4.4 EVALUACIÓN DE LA ARQUITECTURA RESILIENTE DEL SISTEMA DE GESTIÓN DOCUMENTAL PARA SEGURO TOTAL

Con el propósito de cumplir con el objetivo específico número tres, orientado a evaluar una arquitectura de gestión documental alineada a los estándares de las normas ISO 154891:2016, ISO 30301:2019 y ISO/IEC 27001, y bajo el Marco NIST de Ciberseguridad que sea resiliente, accesible y se integre con la gobernanza empresarial de Seguro Total, se aplicaron diversos instrumentos técnicos y de análisis orientados a definir la estructura óptima del sistema propuesto.

Entre los instrumentos empleados se incluyen los flujos de procesos y la matriz de análisis de herramientas, los cuales permitieron identificar los componentes estructurales, las interacciones entre actores y los puntos críticos de la gestión documental dentro de la organización. Además, se usaron listas de verificación basadas en normas ISO 15489, ISO 30301 e ISO 27001. Dichas prácticas tienen el propósito de determinar el grado de cumplimiento y madurez de la organización respecto a los principios de gestión, control y seguridad de la información. Estos instrumentos facilitaron la evaluación integral de la arquitectura documental actual y el diseño de un modelo propuesto que incorpora controles de seguridad, lineamiento y gobernanza y mecanismos de trazabilidad conforme al marco NIST de ciberseguridad.

Figura 29: Instrumentos aplicados al Objetivo 3



Nota: Elaborada por los autores

Figura 30: Capas Arquitectura Empresarial

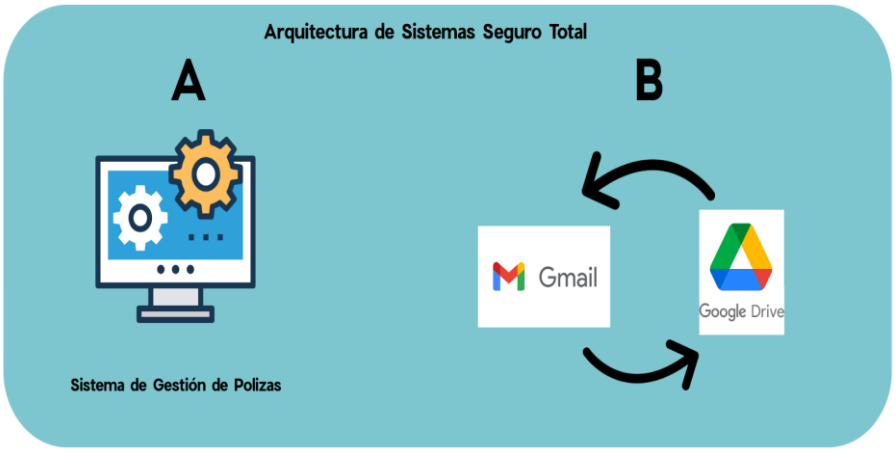
Nota: Obtenida de (Consultoriadeprocesos, 2015)

En la imagen anterior se puede ver para evaluar una arquitectura empresarial para la gestión documental alineada a las normas ISO y el Marco NIST hay que analizar primero los componentes que integran una arquitectura empresarial moderna. Como podemos ver en la imagen anterior, teniendo base como ser el Marco TOGAF, el mismo lo estructura la organización en cuatro principales pilares que son la Arquitectura de Información, Arquitectura de Negocio, Arquitectura de Aplicaciones y Arquitectura Tecnológica, en donde estos se alineando una visión estratégica que busca asegurar la coherencia entre los procesos, datos, las

soluciones de TI y la infraestructura que los soporta. De la siguiente manera se definen los pilares de una arquitectura empresarial:

1. **Arquitectura de la Información:** Define como se gestionan y estructuran los datos dentro de una organización. Se debe incluir la calidad, integridad, disponibilidad y gobierno de la información. En donde su propósito final es asegurar que los datos sean confiables, accesibles y útiles para la toma de decisiones y como apoyo para los procesos operativos.
2. **Arquitectura de Negocios:** Define como funciona la organización desde la perspectiva operativa, es decir como sus procesos, políticas y flujos de trabajo. Este pilar buscar garantizar que la estructura del negocio este alineada con los objetivos estratégicos y la eficiencia de los procesos.
3. **Arquitectura de Aplicaciones:** Define las aplicaciones y sistemas que soportan los procesos de negocios, en donde se incluyen como interactúan entre sí, como el intercambio de información y que funcionalidades aportan. Su objetivo es asegurar que el ecosistema de software sea integral y eficiente, buscando eliminar sistemas aislados. En la siguiente figura se pueden el sistema de gestión de pólizas y las aplicaciones de Gmail y Google Drive que utiliza actualmente la correduría en su arquitectura de aplicaciones. En este el sistema de gestión de pólizas no tiene ninguna integración directa con Gmail o Google Drive, por lo cual solamente se lleva el control de los metadatos de las pólizas en el mismo y toda la gestión de documentos o almacenamiento digital se realiza en la aplicación de Gmail, sin aprovechar la herramienta d Google Drive.

Figura 31: Arquitectura de Aplicaciones de Seguro Total



Nota: Elaborada por los autores

4. Arquitectura Tecnológica: Define la infraestructura tecnológica necesaria para soportar aplicaciones y datos. En este caso pueden ser servidores, redes, plataformas, almacenamiento, ciberseguridad, etc. Buscando que la base tecnológica sea estable, escalable, segura y capaz

de soportar el crecimiento y necesidades futuras.

Como parte integral de nuestra investigación estos pilares se conectan con nuestras normas ISO 15489,30301,27001 y el Marco NIST de la siguiente manera:

Tabla 42: Análisis de Alineación de la arquitectura actual con normas ISO y NIST.

Pilar de Arquitectura	Relación con Normas ISO/NIST	Estado Actual en Seguro Total	Brechas Identificadas	Riesgos Asociados	Riesgos Generales Detectados
Información (Datos)	ISO 15489: autenticidad, trazabilidad. ISO 30301: gobernanza documental. ISO 27001: protección de información. NIST CSF: Identificar–Proteger	Información recibida por WhatsApp, correo y llamadas sin clasificación ni repositorio central. No hay trazabilidad ni control de versiones. Documentos sensibles (ID, RTN, licencias, diagnósticos médicos) se gestionan informalmente.	• Falta de uso correcto del SGD actual. • No hay políticas de clasificación, retención, metadatos, ni controles de acceso. • Sin repositorio ni normas de integridad. • No existe un repositorio central.	Fuga de datos, alteración de documentos, duplicidad, pérdida de evidencia, incumplimiento normativo.	Exposición de datos personales, descontrol sobre la información, inconsistencias documentales que afectan decisiones y cumplimiento legal.
Negocio (Procesos)	ISO 15489/30301: procesos formales y auditables. NIST: Identificar–Proteger–Responder.	Procesos operativos ejecutados de forma manual y variable entre vendedores y usuarios funcionales. No existe un flujo definido y documentado para la	• Falta de estandarización ausencia de procedimientos, roles y métricas. • No hay una cadena de control o responsable de la documenta	Reprocesos, errores humanos, retrasos, pérdida de trazabilidad, dependencias individuales.	Baja eficiencia operativa, falta de control de calidad, dificultad para Responder incidentes o auditorías.

Pilar de Arquitectura	Relación con Normas ISO/NIST	Estado Actual en Seguro Total	Brechas Identificadas	Riesgos Asociados	Riesgos Generales Detectados
		gestión documental.	ción.		
Aplicaciones	ISO 15489/30301: soporte a documentos. ISO 27001: control de accesos, cifrado, auditoría. NIST: Detectar–Responder.	Uso de WhatsApp, correo, Excel y plataformas de aseguradoras sin integración ni controles. No existe un sistema centralizado ni auditoría.	• Falta de integración, ausencia de logs, • nulo control de accesos ausencia de cifrado, duplicidad de documentos.	Vulneraciones, falta de integridad documental, imposibilidad de auditar, pérdida de información.	Fragmentación tecnológica, Sistemas no conectados entre sí, alta exposición a incidentes y pérdida de control digital.
Tecnología	ISO 27001: infraestructura segura. NIST: Proteger–Detectar–Recuperar. ISO 15489: preservación.	No existen servidores propios ni repositorio documentado. No hay backups formales ni políticas de seguridad. Dispositivos personales sin medidas corporativas.	Falta de infraestructura segura, ausencia de recuperación ante desastres, falta de monitoreo y registros.	Ciberataques, pérdida total de información, indisponibilidad operativa, fallas sin recuperación.	Continuidad del negocio comprometida, incapacidad para recuperar información crítica, vulnerabilidad total ante incidentes.

Nota: Elaborada por los autores

4.4.1ANÁLISIS DE LA ARQUITECTURA EMPRESARIAL MEDIANTE APLICACIÓN DE LA ENTREVISTA

Para obtener una visión estratégica integral de la correduría, se realizó una entrevista a los principales directivos de la organización. Participaron dos profesionales del género femenino que ocupan los cargos de Gerente General y Gerente de Operaciones, así como dos profesionales del género masculino que desempeñan las funciones de Gerente de Mercadeo y Gerente de Seguros Nacionales. Esta diversidad de perspectivas permitió recopilar una visión

más completa sobre el estado actual de la gestión documental y los retos estratégicos que enfrenta la empresa. De la misma forma, este instrumento nos permite evaluar de mejorar manera la percepción y hacia donde se dirige la correduría para apoyar mediante el diseño y directrices de un SGD. Se han obtenido las siguientes respuestas durante la aplicación de la entrevista en la oficina principal de Tegucigalpa, Honduras de la correduría.

Tabla 43: Matriz de respuestas del instrumento la Entrevista

Preguntas	Gerente de Operaciones	Gerente de Seguros	Gerente de Mercadeo	Gerente General
¿Cuáles considera que son las principales fortalezas del sistema actual de gestión documental en la organización?	Facilidad de acceso a la información, digitalización, rapidez, ayuda para decisiones rápidas, mejor análisis de información	Nos ayuda en la toma de decisiones fácil obtención de datos desde cualquier pc Contiene la información más esencial para atender a cualquier cliente	Nos ayuda a tener un mejor Control de los Asegurados y así mejorar el servicio	Digital, acceso desde cualquier dispositivo
¿Qué debilidades o limitaciones observa en los procesos de gestión documental que deberían atenderse prioritariamente?	El orden de la información, actualización de información, seguridad	Mejorar la seguridad Clasificar de mejor forma	Se necesita un programa donde nos avise y pueda enviar correos a los asegurados cuando se renueven las pólizas. también un sistema de control de cumpleaños, Un sistema para promocionar la oficina	Falta de organización, falta de conocimiento de la herramienta
Desde su perspectiva, ¿cómo ha impactado la digitalización de documentos en la eficiencia de su área o de la organización en general?	Ha sido positiva, se utilización nos ayuda a la toma de decisiones más rápida, ágil y con mejores resultados	Es vital para la toma de decisiones y planeación dentro de la empresa	Lo mejor es la digitalización de los documentos, da más facilidad y control de la información y se puede tener acceso en diferente puerto para su uso.	Buena, permite a los colaboradores revisar y validar los documentos y nos ayuda a llevar control.
¿Qué riesgos de seguridad percibe en el manejo actual de documentos y qué medidas propondría para	Los riesgos son medio alto por la facilidad de acceso y manipulación, códigos de acceso y	Contiene información confidencial de los clientes por lo cual sugiero mejorar la seguridad y	El peligro es no tener buenas protecciones de la información y que cualquiera pueda ingresar. Adquirir	Perdida de información y falta de actualización de documentos. Medidas

reducirlos?	controles	manejo de documentos	tecnología para proteger la información	serían poner más controles para acceder a documentos físicos y digitales.
¿Qué indicadores o métricas considera más relevantes para evaluar la efectividad de la gestión documental?	Cantidad de documentos completos, actualización rápida, facilidad de ingreso de información	De seguridad y de Calidad	Acceso rápido a la Información Controles eficaces de Seguridad Tener la oportunidad de tener varias variables de investigación de los asegurados Tener Base datos con análisis de toda la información como ser cumpleaños, familia dirección etc.	Cantidad de documentos digitales, cantidad de documentos físicos, rapidez de acceso
¿Qué retos principales enfrenta la organización para lograr una gestión documental más eficiente?	La capacitación del personal para herramientas actualización	Mejoras en ventas y porcentajes de cierre, asimismo un mejor servicio al cliente	Tener un sistema confiable, rápido y tener acceso a la información necesaria para ofrecer un buen servicio postventa y así crecer más la cartera	Capacitación de colaboradores y recursos monetarios
¿Qué beneficios específicos ha observado en la implementación de sistemas digitales de gestión documental?	Incremento de ventas, mejoras de tomas de decisiones por la información para el crecimiento de la empresa	Mejor acceso a la información, conocimiento real de nuestra información para toma de decisiones a corto mediano y largo plazo	Acceso Inmediato a la información Controles de cobro, renovaciones	Incremento de ventas, reducción de documentos físicos almacenados
¿Qué nivel de inversión o recursos considera	L 100,000	$10,000	$10,000	L 50,000

necesarios para fortalecer la gestión documental en la organización?				
¿Qué acciones de capacitación cree necesarias para que el personal utilice de forma adecuada los sistemas de gestión documental?	Capacitaciones continuas	Programas capacitaciones periódicas	Mayor entrenamiento en el uso de sistemas. Entrenamiento en Inteligencia Artificial que asista al mercado de Seguros	Capacitaciones continuas, implementar nuevo sistema
¿Cómo imagina la gestión documental ideal en la organización dentro de los próximos 3 a 5 años?	digitalización a un 90%	Mucho más ágil y eficaz, con mayores recursos que nos permitan tener mejores decisiones	Tener sistemas que nos de toda la información del asegurado, que pueda autónomamente mandar email de recordatorios de renovaciones, de fechas especiales. Tener acceso con buenos sistemas de control a Celulares, Laptop en cualquier parte del Mundo.	100% digital eliminando dependencia de documentos físicos.

Nota: Elaborada por los autores mediante aplicación de la entrevista

4.4.1.1 PILAR DE LA INFORMACIÓN

Para el Pilar de Información (Datos) podemos ver en las respuestas que la digitalización y acciones relacionadas a la transformación digital que se han ejecutado dentro de la correduría han mejorado la rapidez, acceso y la disponibilidad de la información. Podemos destacar problema relacionados con el orden, gestión, actualización de los documentos digitales y tanto de físicos como he observado en las instalaciones. Se recalcan riesgos como ser la perdida de la información, manipulación de documentos, accesos no autorizados y ausencia de controles más robustos en términos de privilegios y de seguridad. Esto nos demuestra una madurez baja en nivel de la arquitectura de datos.

Podemos ver también que los datos sensibles o PII no se gestionan de manera centralizada o con los controles de seguridad, lo que contradice los requisitos de integridad, autenticidad y trazabilidad que establecen las normas ISO 15486 y la 30301, impactando también los principios de confidencialidad, integridad y disponibilidad de la ISO 270001.

El hallazgo principal para este pilar es que, aunque los directivos perciben beneficios mediante la digitalización como ser el acceso de la información y referenciando los beneficios que han percibido los colaboradores sobre el mismo, podemos ver claramente que la falta de estructuras, roles, y responsabilidades para proteger, organizar y actualizar la información está generando riesgos altos para la organización, afectando lo que es la confiablidad e integridad de los datos.

4.4.1.2 PILAR DEL NEGOCIO

Podemos ver de manera general una ausencia de estandarización dentro de la organización, mediante las respuestas repetitivas obtenidas relacionadas a la necesidad actual de mejorar la clasificación, orden, actualización y conocimiento de la herramienta, lo que nos indica que los procesos actuales no siguen un orden y están muy predispuesto a errores humanos.

Aunque existe un proceso de gestión documental dentro de la correduría podemos ver que no se encuentra directamente enlazada con los procesos operativos de alta, actualización o baja de documentos. Lo que llega afectar a la correduría en términos de actividades de control, renovaciones, cobros y servicio al cliente. Vemos que esto se alinea a la respuesta de los directivos sobre los retos actuales como ser la capacitación continua, la necesidad de procesos más agiles y eficientes y el impacto de mejorar las mejorar y aumentar la cantidad de clientes.

Con relación a la ISO 15489 y la 30301 como hallazgo principal todo proceso

documental debe ser estable, medible y auditable, pero mediante las respuestas podemos ver que los procesos no se siguen, comunicación o no están documentados. Desde el Marco NIST mediante Identificar y Responder la organización no tiene protocolos o planes de acción para identificar errores, registrar incidentes o Responder antes fallas relacionadas a la gestión documental.

4.4.1.3 PILAR DE APLICACIONES

Durante la realización de la entrevista pudimos ver que existe un sistema que gestiona el control de los clientes y pólizas, pero este no se integra con Google Drive. En las respuestas de los directivos pudimos ver que se necesitan sistemas más automatizados y funcionales. Se busca que la herramienta de SGD envié recordatorios de renovaciones, correos automáticos, alertas, análisis de los clientes y una base de datos consolidada. Esto nos confirma que las aplicaciones actuales no están cubriendo las expectativas y necesidades operativas de la organización y que no están funcionando de manera integral en un solo ecosistema tecnológico.

Se menciono también que se busca el principio de disponibilidad al buscar acceder desde cualquier dispositivo con una mayor control y rapidez lo que se traduce un mejor procesamiento de la información. Con base a la norma ISO 2700 vemos que no existe medidas de seguridad, mediante la ISO 30301 vemos que los sistemas no se conectan con el SGD actual y con base al NIST no existe protocolos de detección y de respuesta ante incidentes.

Como hallazgo principal vemos un ecosistema tecnológico empresarial muy disperso, evidencian que los sistemas viven separados creando silos de información, lo que reduce la eficiencia, incrementa los errores y aumenta riesgos operativos de continuidad del negocio.

4.4.1.4 PILAR DE TECNOLOGÍA

Los directivos identifican los riesgos más graves que los están afectando actualmente que son perdida de la información, accesos no autorizados, falta de actualización y mejorar los controles para los documentos digitales y también para los físicos. Los directivos mencionan invertir recursos monetarios desde 50 mil lempiras hasta 260 mil lempiras, mostrando la importancia y apoyo de la directiva por mejorar la gestión documental considerando la gran cantidad de documentación que manejan en su día a día.

Vemos una visión general consolidad en donde se busca superar o llegar a un 90% de digitalización en los próximos tres a cinco años mostrando un compromiso por la transformación digital, buscando que dicha información y documentación sea accesible desde diferentes dispositivos. Teniendo en consideración las respuestas frente a brechas y puntos de

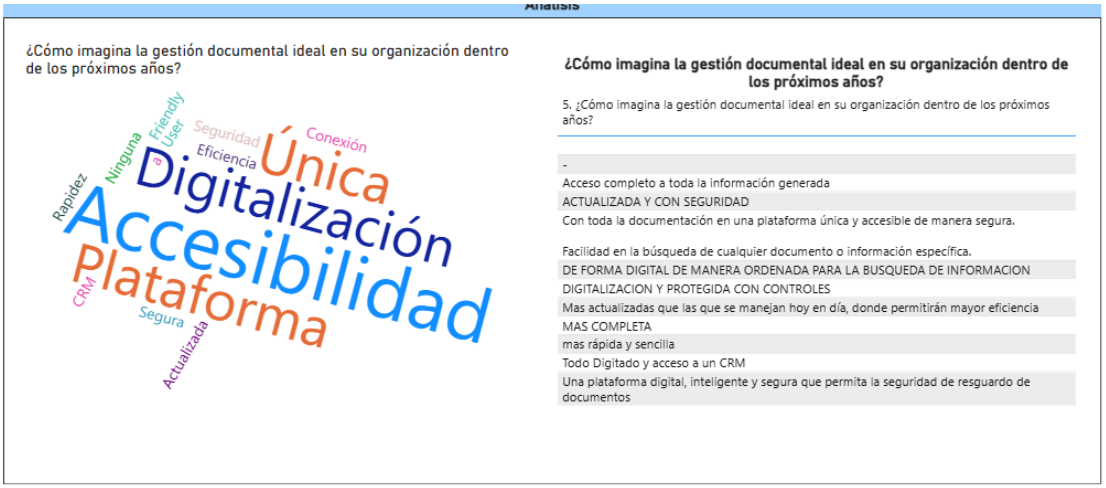
dolor vemos que la visión es la acertada pero la correduría tiene un camino largo por recorrer para mejorar su eficiencia con relación a la gestión documental. Se evidencia brechas respecto a la *ISO 27001,* la cual nos exige tener una arquitectura segura, controles de seguridad y monitoreo lo cual se relaciona también con los pilare del marco NIST.

En resumen, como hallazgo los directivos reconocen que la infraestructura actual no es la más eficiente para tener un SGD bien implementado y con un correcto funcionamiento, por lo cual se requieren estructuraciones, definición de políticas para lograr esa madurez que desean alcanzar en los próximos tres a cinco años.

4.4.2 ANÁLISIS DE PREGUNTAS ABIERTAS DEL CUESTIONARIO

Para complementar la evaluación de la arquitectura de gestión documental y su alineación con los estándares ISO 15489-1:2016, ISO 30301:2019, ISO/IEC 27001 y el Marco NIST de Ciberseguridad, se analizaron las percepciones de los colaboradores mediante preguntas orientadas a identificar tanto las recomendaciones para fortalecer la seguridad en el manejo de documentos y canales digitales, como la visión interna sobre la gestión documental ideal en los próximos años. Este análisis permite contrastar el estado actual con las expectativas organizacionales, evidenciar brechas de seguridad y madurez, y aportar insumos cualitativos esenciales para definir el diseño óptimo del sistema propuesto.

Figura 32: ¿Como se imagina la gestión documental ideal?

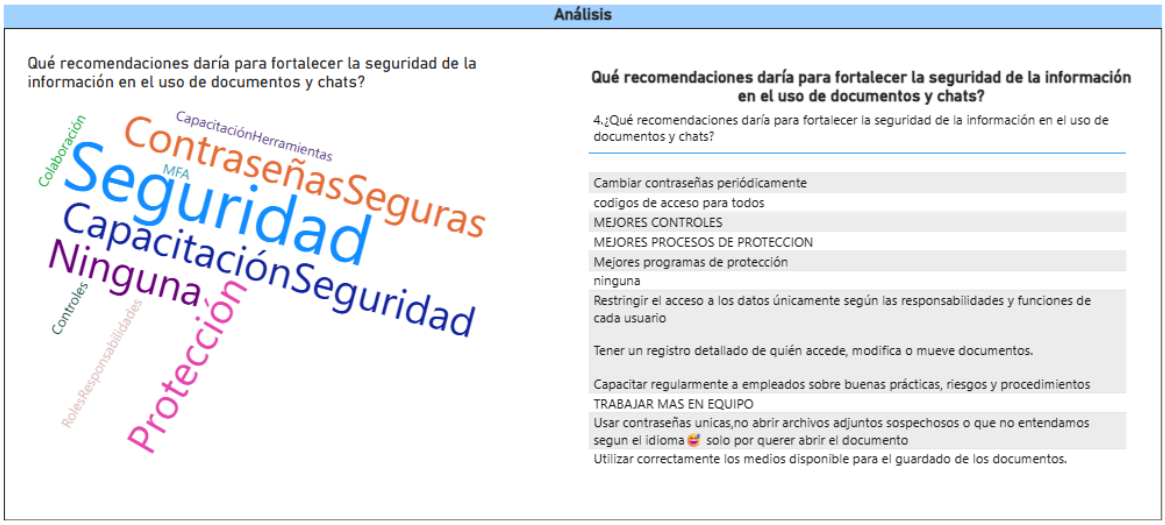


Nota: Elaborada por los autores

Las respuestas evidencian una visión organizacional consistente orientada hacia una gestión documental completamente digital, centralizada y accesible, donde la información pueda consultarse de forma rápida, ordenada y segura. Los colaboradores expresan la necesidad

de contar con una plataforma única que integre documentos, CRM y demás sistemas, evitando la dispersión actual y facilitando la búsqueda eficiente. Además, se destaca como prioridad la protección de la información, el control de accesos y la actualización continua, lo cual coincide con los principios de integridad, disponibilidad, confiabilidad y seguridad establecidos por ISO 15489, ISO 30301 e ISO/IEC 27001. En conjunto, estas percepciones reflejan una clara oportunidad de modernización y fortalecimiento del ecosistema documental mediante soluciones digitales que aumenten la eficiencia operativa y la gobernanza de la información.

Figura 33: Recomendaciones de Seguridad



Nota: Elaborada por los autores

Las respuestas muestran que los colaboradores reconocen la importancia de fortalecer la seguridad de la información mediante controles básicos pero críticos, como el uso de contraseñas seguras, cambios periódicos, restricciones de acceso por roles y mejores procesos de protección. También se evidencia la necesidad de capacitación continua en buenas prácticas, riesgos y uso adecuado de documentos y canales digitales. Sin embargo, destaca que algunos colaboradores indican “ninguna”, lo cual refleja brechas en conciencia y cultura de seguridad que deben ser atendidas. En conjunto, estos hallazgos confirman oportunidades para mejorar la gobernanza, protección y uso responsable de la información, en coherencia con los controles de ISO/IEC 27001 (A.5, A.7, A.8, A.9 y A.12), con los principios de integridad y protección documental de ISO 15489 y con las funciones de Proteger, Detectar e Identificar del Marco NIST.

4.4.3 ANÁLISIS DE MATRIZ FODA

Con base en el Objetivo 1, orientado a evaluar la situación actual de la gestión documental y su nivel de alineación con las normas ISO 15489, ISO 30301, ISO/IEC 27001 y el Marco

NIST, se realizó un análisis integral de los procesos, herramientas, seguridad de la información y percepción de los colaboradores. A partir de esta evaluación se construyó la siguiente matriz FODA, la cual resume de manera estratégica las fortalezas, oportunidades, debilidades y amenazas que influyen directamente en la arquitectura documental vigente.

Figura 34: Matriz FODA

Nota: Elaborada por los autores

Las fortalezas como el uso de herramientas digitales, la apertura del personal a la digitalización, la estructura organizativa flexible y la conciencia sobre seguridad se relacionan con los pilares de Información y Tecnología, demostrando que ya existen prácticas y actitudes favorables para adoptar los principios de organización, disponibilidad y acceso definidos por ISO 15489 e ISO 30301. Además, la conciencia sobre seguridad refuerza la alineación con ISO 27001 y la función Proteger del NIST.

Las debilidades, que incluyen la falta de roles definidos, la ausencia de un proceso formal de gestión documental, la baja seguridad en herramientas digitales, el desconocimiento parcial de las normas y la falta de indicadores o planes de acción, evidencian brechas en los cuatro pilares: desorden de la información, falta de estandarización de procesos, herramientas no optimizadas y una infraestructura insuficiente. Estas debilidades coinciden directamente con los requisitos incumplidos de ISO 15489 (ciclo de vida documental), ISO 30301 (gobernanza y responsabilidades), ISO 27001 (controles de seguridad) y NIST (Identificar, Proteger y Responder).

Las oportunidades identificadas como la posibilidad de implementar un SGD basado en

ISO/NIST, la disponibilidad de herramientas integrables, el fortalecimiento de la capacitación, y la mejora de la accesibilidad y seguridad complementan las brechas detectadas y muestran que el mercado ofrece soluciones alineadas tanto a los estándares internacionales como a los pilares de Aplicaciones y Negocio, permitiendo cerrar los vacíos detectadas en procesos, controles y herramientas.

Finalmente, las amenazas entre ellas ataques de ciberseguridad, pérdida de información sensible, falta de continuidad operativa, competencia tecnológica y ausencia de respaldo documental exponen riesgos que impactan los pilares de Tecnología e Información, y reflejan directamente los dominios críticos de ISO 27001 (control de accesos, continuidad, protección de activos) y del NIST (Detectar, Responder, Recuperar). Estas amenazas evidencian el nivel de urgencia para fortalecer la arquitectura documental.

4.4.4 HALLAZGOS DE OBJETIVO 3

1. Nivel de Arquitectura

La siguiente tabla detalla el nivel de madurez percibido de la correduría con base a su arquitectura actual:

Tabla 44: Nivel de Madurez Gestión de Documentos

Pilar	Madurez	Justificación
Información	Bajo	Existe una digitalización inicial y accesibilidad básica, pero no hay controles, trazabilidad, clasificación o roles definidos.
Negocio	Bajo	Procesos no estandarizados, no existe un control sobre los flujos de trabajo, no existen indicadores de monitoreo y dependen de criterios individuales.
Aplicaciones	Bajo	Existe herramientas digitales como ser Gmail y Google Drive, pero no están utilizándose de forma eficiente o con las medidas de seguridad adecuadas y la información vive en silos.
Tecnología	Bajo	La infraestructura es limitada, sin controles formales de seguridad, continuidad y monitoreo.

Nota: Elaborada por los autores

2.Pilar de la Información

- La información está digitalizada parcialmente, pero sin orden, clasificación ni controles formales, generando dispersión y pérdida de trazabilidad.
- Existen riesgos recurrentes de pérdida de datos, manipulación, accesos no autorizados y falta de actualización, señalados tanto por directivos como por colaboradores.
- No hay una estructura definida para proteger datos sensibles o PII, incumpliendo los principios de integridad, autenticidad y disponibilidad establecidos por las ISO 15489,

ISO 30301 e ISO 27001.

- Información es accesible pero no existen controles sobre ella.

3.Pilar de Negocios

- Los procesos documentales no están estandarizados, no se encuentran formalmente documentados ni alineados a los procesos operativos de la correduría.
- Se evidencia una alta dependencia del criterio individual, lo que incrementa errores y retrabajos.
- La organización carece de roles, responsabilidades y protocolos de acción, incumpliendo ISO 30301 y el dominio Identificar/Responder del NIST.

4.Pilar de Aplicaciones

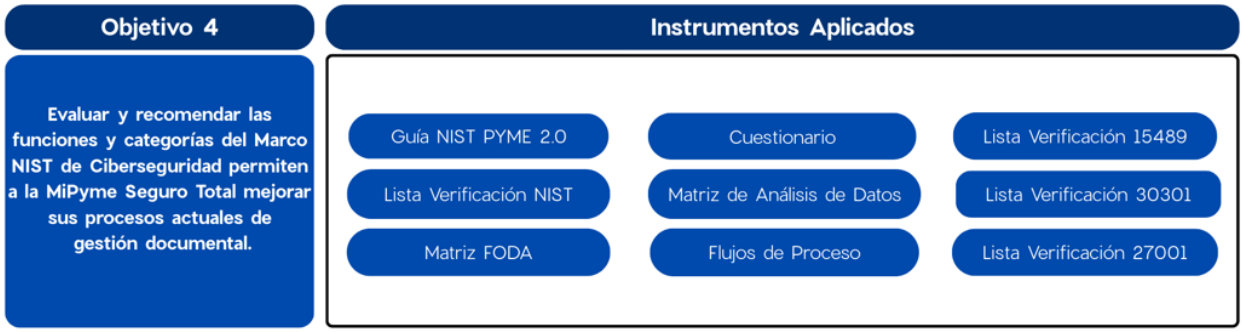
- Las herramientas actuales (sistema de gestión de pólizas, Google Drive) no están integradas, generando silos de información y duplicidad de esfuerzos.
- Los usuarios expresan la necesidad de un sistema más automatizado y una base de datos consolidada con recordatorios y alertas.
- No existen funciones de auditoría, monitoreo ni seguridad en las aplicaciones, generando brechas con ISO 27001 y NIST.

5.Pilar de Tecnología

- La infraestructura es básica y carece de controles de seguridad, monitoreo, continuidad operativa y gestión de incidentes.
- Se identifican riesgos graves: pérdida de información, exposición de documentos y accesos no autorizados.
- Aunque existe intención de avanzar hacia un 90% de digitalización, la tecnología actual no sostiene ese nivel de madurez.

4.5 ANÁLISIS DE CATEGORÍAS NIST PARA EL MEJORAMIENTO DE LOS PROCESOS DOCUMENTALES

Figura 35: Instrumentos Aplicados al Objetivo 4



Nota: Elaborado por los autores

Con el propósito de cumplir con el objetivo 4, orientado a evaluar la y recomendar funciones y categorías del marco NIST de ciberseguridad que permitan a la compañía aseguradora Seguros Total mejorar sus procesos actuales de gestión documental.

Este análisis permite identificar brechas relacionadas con la gestión de la información, seguridad cibernética y la respuesta ante incidentes, con el fin de proponer mejoras que fortalecen los procesos actuales de gestión documental y protejan la información de la organización.

Con la necesidad de cumplir el objetivo, se utilizaron instrumentos cuantitativos y cualitativos, incluyendo cuestionarios, lista de verificación normativa (ISO 15489, 30301 y 27001) y una matriz de control basada en funciones del marco de ciberseguridad NIST: Identificar, Proteger, Detectar, Responder y Recuperar.

4.5.1 METODOLOGÍA DE DESARROLLO

Con la necesidad de cumplir con el objetivo se aplicó un enfoque metodológico con tres componentes:

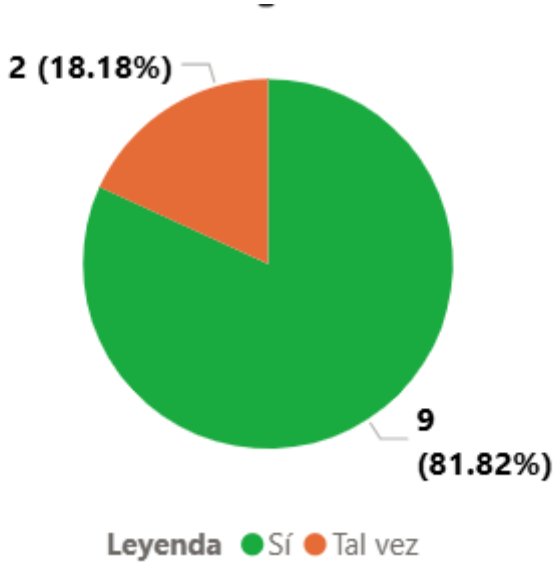
1. Evaluación de conocimiento y percepción donde se aplicó un cuestionario al personal para medir comprensión de ciberseguridad, riesgos, manejo de documentos y buenas practicas
2. Evaluación Normativa donde se realizaron listas estructuradas para validar el cumplimiento de requisitos de gestión documental y seguridad
3. Evaluación técnica por funciones NIST donde la aplicación de matrices orientadas a la verificación de funciones Identificar, Proteger, Detectar, Responder y recuperar.

4.5.2 EVALUACIÓN POR FUNCIONES DEL MARCO NIST DE CIBERSEGURIDAD

4.5.2.1 FUNCIÓN: IDENTIFICAR

La función identificar evaluara las capacidades de la organización para reconocer sus activos documentales, riesgos, roles y flujos de trabajo claros.

Gráfico 42: ¿Conoce usted o ha escuchado sobre la ciberseguridad?

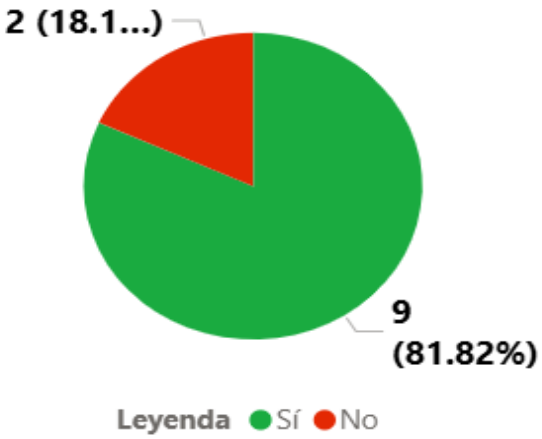


Nota: Elaborado por autores

El gráfico presenta la distribución de las respuestas relacionadas con el conocimiento general sobre ciberseguridad. Se muestra que el 81.82% de los colaboradores selecciono la opción “Sí” indicando que ha escuchado sobre ciberseguridad o conoce mínimamente el término. Por su parte, el 18.18%. Elegio la categoría “Tal vez” lo que refleja conocimiento parcial del tema.

Esto nos indica que gran parte de los colaboradores muestran un conocimiento básico mínimamente sobre el concepto de ciberseguridad, esto permite ejercer cualquier tipo de acciones orientadas a la aplicación de metodologías de ciberseguridad sin necesidad de aplicar capacitaciones sumamente básicas.

Gráfico 43: ¿Conoce los riesgos más comunes de ciberseguridad (virus, programa maligno, robo de datos)?

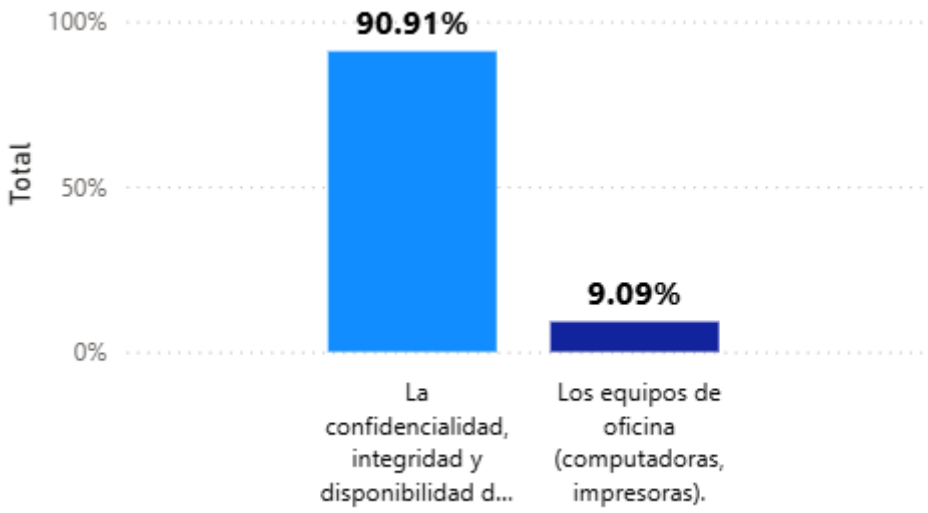


Nota: Elaborado por autores

El 81.82% de los encuestados afirmó haber escuchado sobre la ciberseguridad y conocer los riesgos más comunes como virus, programa maligno y robo de datos. Sin embargo, el 18.18% restante indicó no tener claridad sobre el tema, lo cual revela que, aunque hay conocimiento general, no existe una capacitación institucional o estandarización de conceptos.

Los resultados del cuestionario evidencian que, aunque existe una conciencia general sobre los conceptos de ciberseguridad, todavía no se traducen en prácticas formales o estructurales dentro de la organización.

Gráfico 44: La gestión documental en una empresa consiste en:



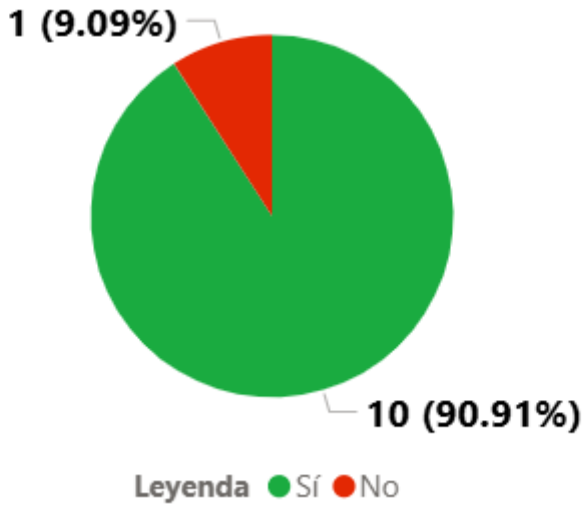
Nota: Elaborado por autores

El gráfico presenta la distribución de respuestas relacionadas con la comprensión que tienen los colaboradores sobre que implica la gestión documental dentro de una empresa. Se

observa un 90.91% selecciono la “Confidencialidad, integridad y disponibilidad de la información” mientras el 9.09% eligió “Los equipos de oficina (computadora, impresoras).

La mayora del personal comprende el concepto de gestión documental relacionado con la protección de información mediante principios básicos como confidencialidad, integridad y disponibilidad. Sin embargo, un pequeño grupo continúa asociando la gestión documental únicamente con equipos físicos como computadoras e impresoras, lo que indica la presencia de una brecha conceptual. Aunque el porcentaje es reducido refleja la necesidad de capacitación formal, donde se aclare que es la gestión documental adecuada y la determina.

Gráfico 45: ¿Conoce que la gestión documental incluye organizar, proteger y dar acceso a la información?



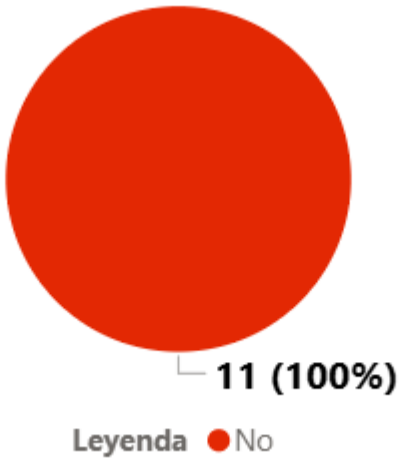
Nota: Elaborada por autores

En cuanto el manejo documental, el 90.91% del personal reconoce que la gestión documental implica organizar, proteger y otorgar acceso seguro a la información y un 100% afirma comprender que la seguridad de la información no se limita a los documentos en papel, lo cual refleja una visión moderna y alineada a la transformación digital.

Los resultados muestran que el 90.01% de los colaboradores reconocen que la gestión documental implica organizar, proteger y garantizar el acceso adecuado a la información. Esto evidencia una comprensión solida de los principios fundamentales del ciclo de vida documental establecidos por las normas ISO 15489 e ISO 30301.

El bajo porcentaje que respondieron negativamente indica que aún existe una mínima brecha de formación en concepto documentales, que podría generar practicas inconsistentes si no se gestiona adecuadamente. Aunque la cantidad no es alarmante indica que hay una necesidad de implementar programas de capacitación formales.

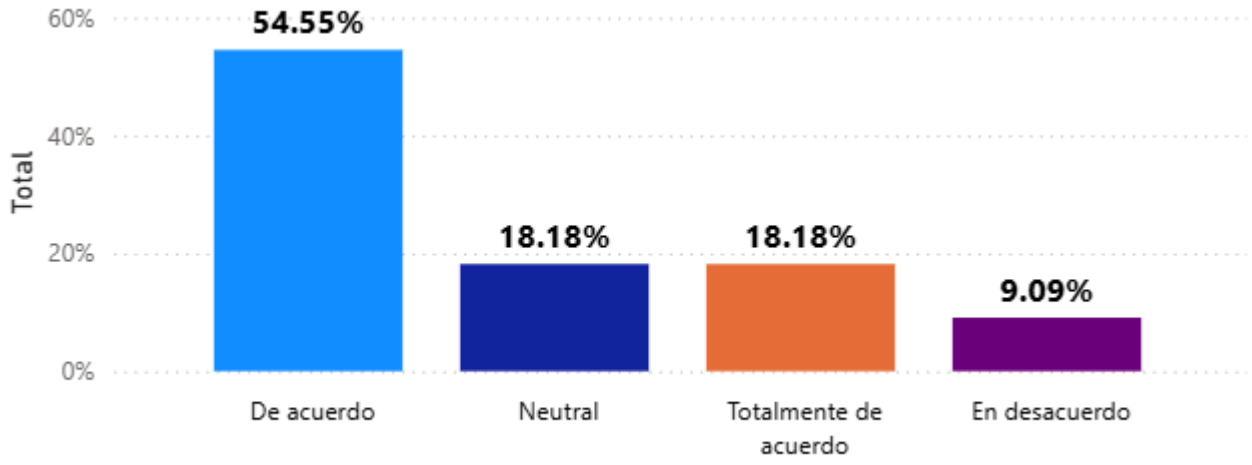
Gráfico 46: ¿Cree que la seguridad de la información protege únicamente los documentos en papel?



Nota: Elaborado por autores

En cuanto a la seguridad de la información, el 100% de los colaboradores consideran que no solo protegen los documentos físicos sino, los digitales de igual manera, lo cual refleja una visión moderna y alineada a la transformación digital.

Gráfico 47: ¿Conoce que la gestión documental incluye organizar, proteger y dar acceso a la información?



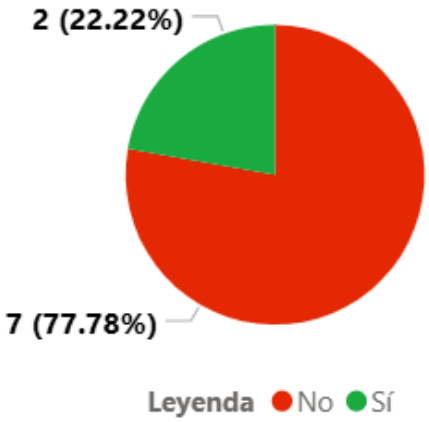
Nota: Elaborado por autores

El gráfico presenta la distribución de las respuestas relacionadas con el conocimiento del personal sobre si la gestión documental incluye organizar, proteger y dar acceso a la información. Se observa que el 54.55% selecciono la opción “De acuerdo” mientras que un 18.18% manifestó postura “Neutral” y otro 18.18% elegio la categoría “Totalmente de acuerdo”. Finalmente, el 9.09% indica estar “En desacuerdo”.

El gráfico muestra que la mayoría del personal reconoce que la gestión documental implica organizar, proteger y facilitar el acceso a la información. El 54.55 colaboradores manifestaron estar de acuerdo y dos, lo que refleja una comprensión positiva sobre el propósito de la gestión documental. Sin embargo, la presencia de respuestas neutras y en desacuerdo evidencia que aún existen brechas en el entendimiento integral del proceso, especialmente en lo relacionado con la protección de la información y su trazabilidad digital.

4.5.2.2 FUNCIÓN: PROTEGER

Gráfico 48: ¿Sabe que existe una norma llamada ISO 27001 que ayuda a proteger la información de las empresas?



Nota: Elaborado por autores

El 77.78% de los encuestados desconocía de la norma ISO 27001, lo que evidencia una falta de conocimiento sobre los estándares internacionales que regulan la gestión de seguridad de la información, mientras que el 22.22% indican que conocen sobre la norma ISO 27001.

Los resultados del cuestionario reflejan que, si bien existe una conciencia individual sobre la importancia de la protección de la información, las medidas formales a nivel a nivel institucional aún no se encuentran estandarizadas ni documentadas.

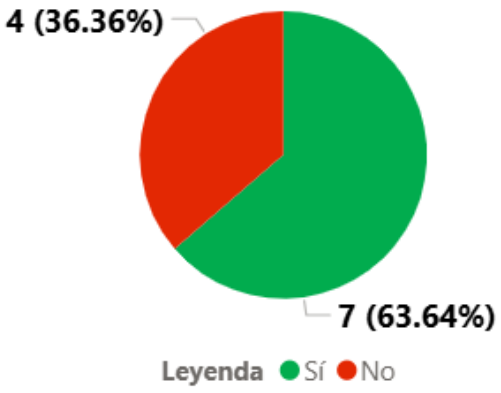
Gráfico 49: ¿Conoce la importancia de crear y usar contraseñas seguras?

Nota: Elaborado por autores

El gráfico presenta la distribución de las respuestas relacionadas con el conocimiento que tienen los colaboradores sobre la importancia de crear y utilizar contraseñas seguras. Se observa un 90.91% selecciono “Si” mientras que el 9.09% respondieron “No”.

Los resultados reflejan que el 90.91% del personal reconoce la importancia de crear y utilizar contraseñas seguras, lo cual constituye una base positiva para la adopción de medidas más avanzadas de seguridad de la información. Sin embargo, el hecho que exista un 9.09% que desconozca este principio, evidencia una brecha de formación que podría presentar un riesgo para la organización, especialmente considerando que las contraseñas constituyen la primera línea de defensa contra accesos no autorizados.

Gráfico 50: ¿Sabe cómo navegar de forma segura en internet (evitar descargas peligrosas, no compartir información sensible, etc.)?

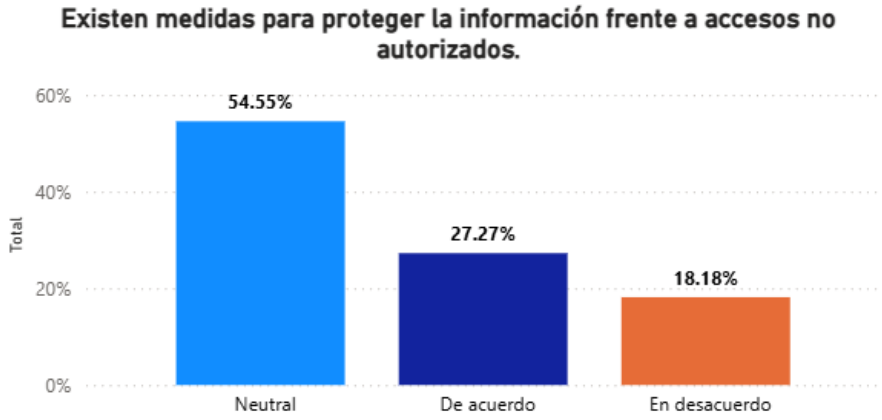


Nota: Elaborado por autores

El gráfico presenta la distribución de las respuestas relacionadas con el conocimiento

de los colaboradores sobre la navegación segura en internet, incluyendo prácticas como evitar descargas sospechosas o no compartir información sensible. Se observa que el 63.64% selecciono la opción “Si”, mientras que el 36.36% respondieron “No”. Los resultados muestran que, aunque la mayoría de los colaboradores afirmas conocer prácticas de navegación seguras, existe un porcentaje significativo que reconoce no tener claridad sobre estas medidas. Esta brecha es importante, pues la navegación segura constituye uno de los pilares de la función Proteger del marco NIST.

Gráfico 51: Existen medidas para proteger la información frente a accesos no autorizados.

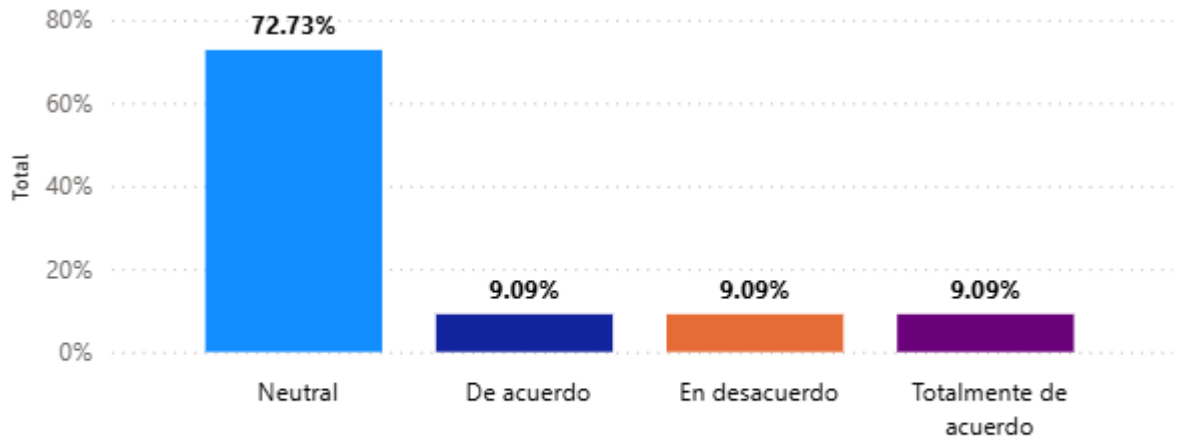


Nota: Elaborado por autores

El gráfico presenta la distribución de las respuestas sobre la percepción del personal respecto a la existencia de medidas para proteger la información frente a accesos no autorizados. Se observa que el 54.55% selecciono la opción “Neutral”, mientras que el 27.27% indico esta “De acuerdo”. Por su parte el 18.189% eligió la categoría “En desacuerdo”.

Los resultados evidencian que la mayoría del personal mantiene una percepción neutral respecto a la existencia de medidas concretas de protección frente a accesos no autorizados, mientras que solo una parte menor afirma conocer controles activos en este ámbito. Esto refleja una falta de claridad institucional sobre los mecanismos de seguridad implementados y su aplicación práctica, lo que sugiere que, aunque pueden existir controles básicos (como contraseñas o accesos restringidos), no están formalmente comunicados ni documentados dentro de la organización.

Gráfico 52: Confío en que la información almacenada está protegida frente a pérdidas o accesos indebidos.



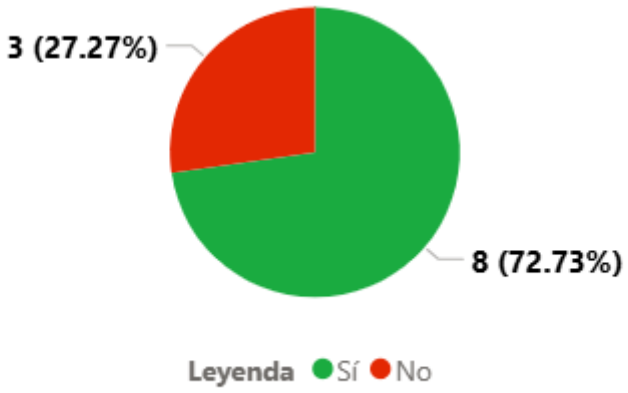
Nota: Elaborado por autores

El gráfico presenta la distribución de respuestas sobre la percepción del personal respecto a la existencia de medidas para proteger la información frente a accesos no autorizados. Se observa que el 54.55% selecciono la opción “Neutral”, mientras que el 27.27% indico estar de acuerdo. Por su parte el 18.18% eligió la categoría “En desacuerdo”.

En este caso, la mayoría de los encuestados manifestó una posición neutral, lo que indica incertidumbre sobre la efectividad de los mecanismos de resguardo de la información almacenada. Solo una minoría expresó confianza en la seguridad actual, lo que evidencia una percepción débil de protección y respaldo ante incidentes. Este hallazgo señala la necesidad de fortalecer los controles técnicos y las políticas de respaldo para garantizar la integridad y disponibilidad de los datos, aspectos clave de la función Proteger del Marco NIST.

4.5.2.3 FUNCIÓN: DETECTAR

Gráfico 53: ¿Sabe identificar un correo electrónico sospechoso o fraudulento (phishing)?

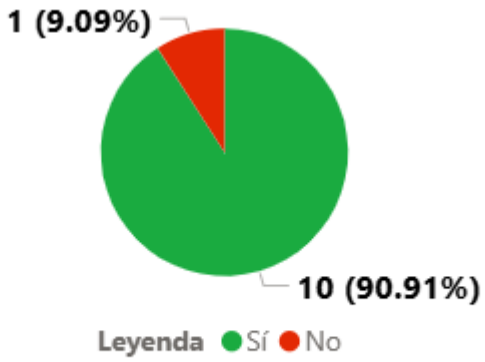


Nota: Elaborado por autores

El 72.73% de los colaboradores afirmó saber identificar un correo malicioso mientras el resto (27.27%) desconoce plenamente como identificar este tipo de amenazas recurrentes, aunque la mayoría reconoce los ataques comunes, el hecho de que no existan procesos institucionales para reportar o registrar dichos eventos limitan la efectividad de esta capacidad.

Los resultados obtenidos en el cuestionario revelan que Seguro Total posee un nivel bajo de madurez en detección, caracterizado por la ausencia de mecanismos formales de monitoreo, auditoría o alerta ante posibles amenazas.

Gráfico 54: ¿Conoce la importancia de crear y usar contraseñas seguras?

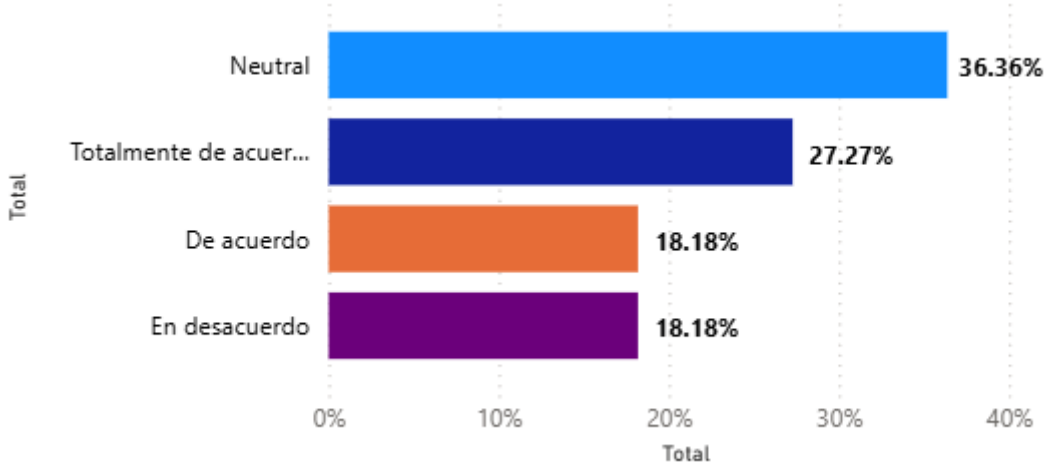


Nota: Elaborado por autores

El gráfico presenta la distribución de las respuestas en base a la importancia de crear contraseñas seguras. Se observa que el 90.91% de los colaboradores tiene conocimiento sobre la importancia, mientras que el 9.09% desconoce del tema.

Los resultados obtenidos reflejan un alto nivel de conocimiento entre los colaboradores sobre la importancia de crear y utilizar contraseñas seguras, con más del 90% respondieron afirmativamente. Este hallazgo demuestra una conciencia positiva en cuanto a prácticas básicas de ciberseguridad. lo que constituye un punto fuerte en base a los lineamientos del marco de ciberseguridad NIST donde está orientada a prevenir accesos no autorizados mediante el reconocimiento temprano de vulnerabilidades humanas.

Gráfico 55: El sistema tiene funciones útiles como búsqueda rápida, control de versiones y permisos de acceso.



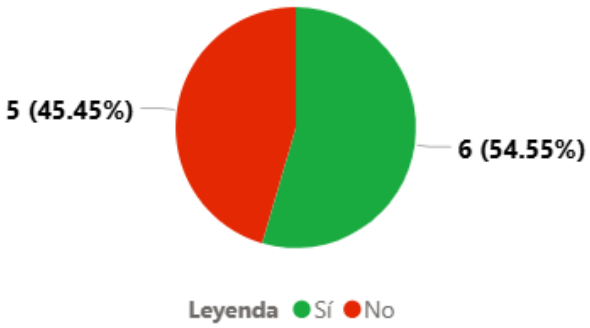
Nota: Elaborado por autores

El gráfico presenta la distribución de las respuestas relacionadas con la percepción sobre el sistema utilizado y las funciones que ofrece. Se observa que el 36.36% selecciono la opción "Neutral", mientras que el 27.27% indico estar "toralmente de acuerdo". Por su parte, el 18.18% eligió la categoría "De acuerdo" y el 18.18% selecciono "En desacuerdo".

En cuanto al sistema utilizado actualmente, los resultados son moderadamente positivos pero dispersos, aunque varios usuarios reconocen que la herramienta cuenta con funciones útiles para la gestión documental, una mayoría se mantiene en posición neutral, lo que sugiere que estas funciones no son plenamente conocidas o aprovechadas por todos los empleados. Esto evidencia una falta de capacitación o estandarización en el uso de la funcionalidad del sistema.

4.5.2.4 FUNCIÓN: RESPONDER

Gráfico 56: ¿Sabe qué hacer o a quién reportar en caso de un incidente de ciberseguridad?

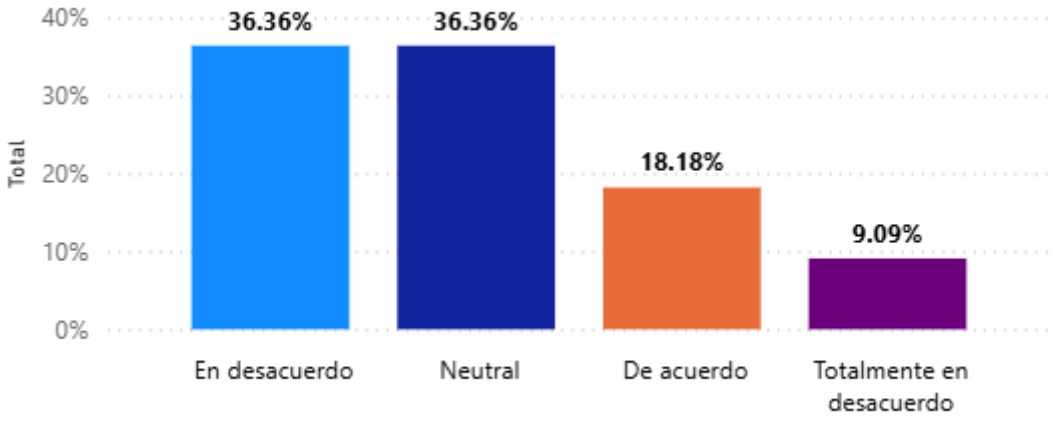


Nota: Elaborado por autores

El gráfico presenta la distribución de las respuestas relacionadas con el concomimiento del personal sobre que hacer o a quien reportar en caso de incidente de ciberseguridad. Se observa que el 54.55% selecciono la opción “Si”, indicando que saben cómo proceder ante un incidente, mientras que el 45.45% respondieron “No”. Los resultados de la encuesta muestran que Seguro Total no dispone actualmente de protocolos ni responsables específicos para la respuesta ante incidentes, operando de forma reactiva e improvisada cuando surgen problemas.

Como se muestra en el gráfico, existe una división casi equitativa en el conocimiento del personal sobre los pasos a seguir ante un incidente de ciberseguridad. poco más de la mitad de los encuestados (54.55%) afirma saber a quién reportar un evento de este tipo, mientras el resto desconoce saber el procedimiento. Este resultado refleja que, aunque existe cierta conciencia individual sobre la importancia de reportar un incidente, la organización carece de un protocolo formal y definido de respuesta.

Gráfico 57: Hay procedimientos para actuar en caso de incidentes relacionados con los documentos.



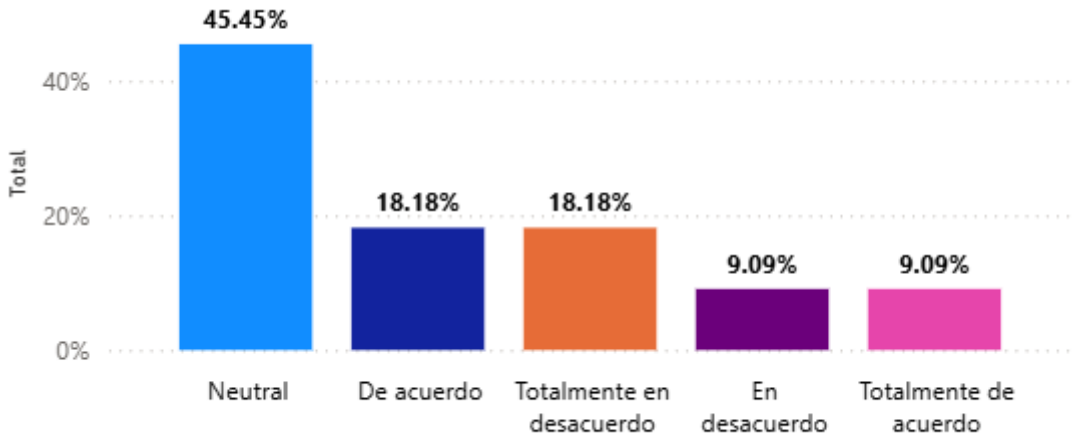
Nota: Elaborado por autores

El gráfico presenta la distribución de las respuestas relacionadas con la existencia de procedimientos para actuar en caso de incidentes relacionados con los documentos. Se observa que el 36.36% de los colaboradores selecciono la opción “En desacuerdo”, mientras que un porcentaje igual del 36.36% se ubicó en la categoría “Neutral”. Así mismo, el 18.18% indico estar “De acuerdo” y el 9.09% restante selecciono “Totalmente en desacuerdo”.

Los resultados muestran que la mayoría de los colaboradores no percibe la existencia de procedimientos claros para actuar en caso de incidentes vinculados con la gestión

documental. La combinación de respuestas “En desacuerdo” y “Neutral” indican una ausencia de lineamientos institucionales que orienten al personal sobre cómo Responder ante pérdidas, errores o accesos no autorizados.

Gráfico 58: Cuando surge un problema con la plataforma, recibimos apoyo oportuno.



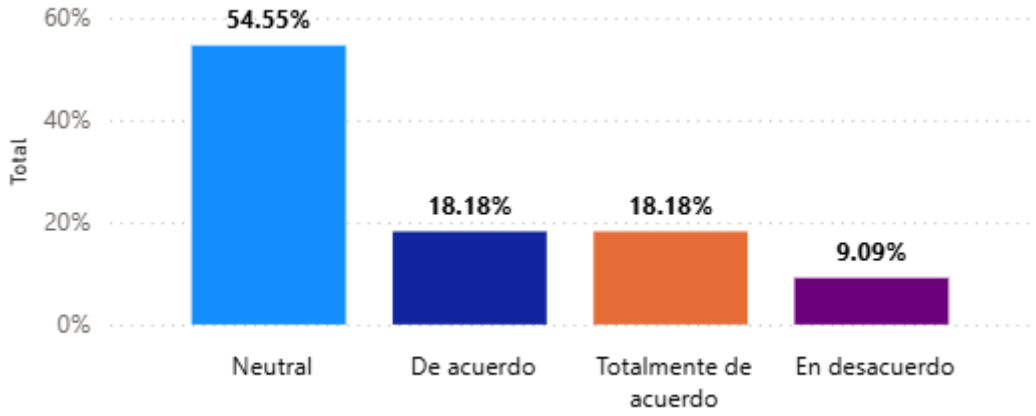
Nota: Elaborado por autores

En este caso, la mayoría de los participantes mantiene una posición “Neutral” con un 45.45%, “Totalmente en desacuerdo” (18.18%) y un 9.09% “En desacuerdo” respecto al apoyo recibido cuando surge un problema con la plataforma

Mientras que un grupo menor afirma haber recibido asistencia oportuna obteniendo un total de 27.27% correspondiente al 18.18% con una posición como “De acuerdo” y el 9.09% “Totalmente de acuerdo”. Esto sugiere que los mecanismos de soporte no son consistentes y no están claramente establecidos. lo que podría generar demoras o dependencias de soluciones improvisadas.

4.5.2.5 FUNCIÓN RECUPERAR

Gráfico 59: La forma en que manejamos documentos ayuda a mantener la continuidad del trabajo en caso de problemas.



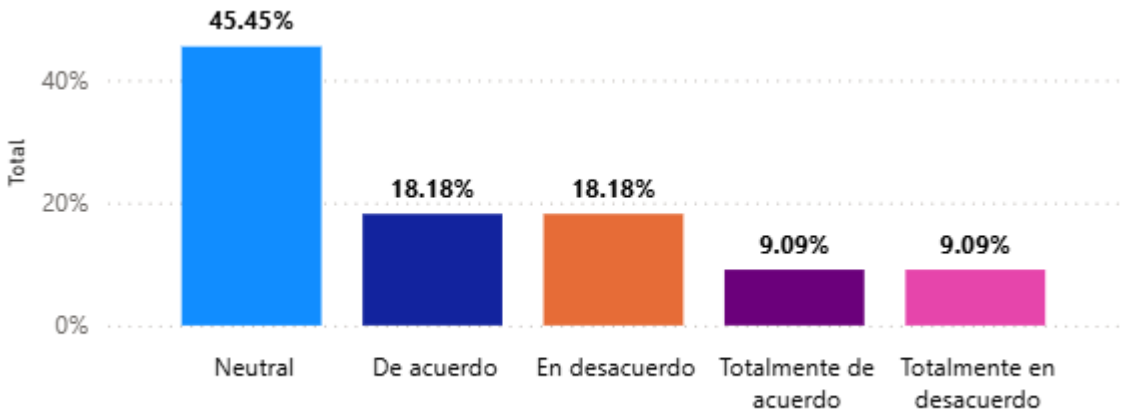
Nota: Elaborado por autores

El 81.82% de los encuestados mantiene una posición desfavorable respecto a la forma en que se manejan los documentos realmente ayuda a mantener la continuidad del negocio y el trabajo en caso de problemas, podemos verlo mediante las respuestas “Neutral” (54.55%), “Totalmente de acuerdo” (18.18%) y el 9.09% en “En descuerdo”. A nivel contrario vemos un porcentaje muy bajo favorable con base a la continuidad de las labores diarias equivalente al 36.36%, con base a las respuestas del 18.18% como ·De acuerdo” y el 18.18% “En desacuerdo”.

Esto demuestra que no existen procedimientos definidos ni respaldos automatizados lo cual genera vulnerabilidad ante incidentes como fallas técnicas, perdidas de acceso o eliminación de archivos.

Los resultados del cuestionario evidencian que la organización no cuenta con mecanismos formales de respaldo ni de recuperación de datos, y que la continuidad del trabajo depende de los conocimientos individuales y del uso cotidiano de herramientas digitales básicas como Google Drive.

Gráfico 60: La empresa tiene planes para recuperar la información y continuar operando si ocurre una pérdida.

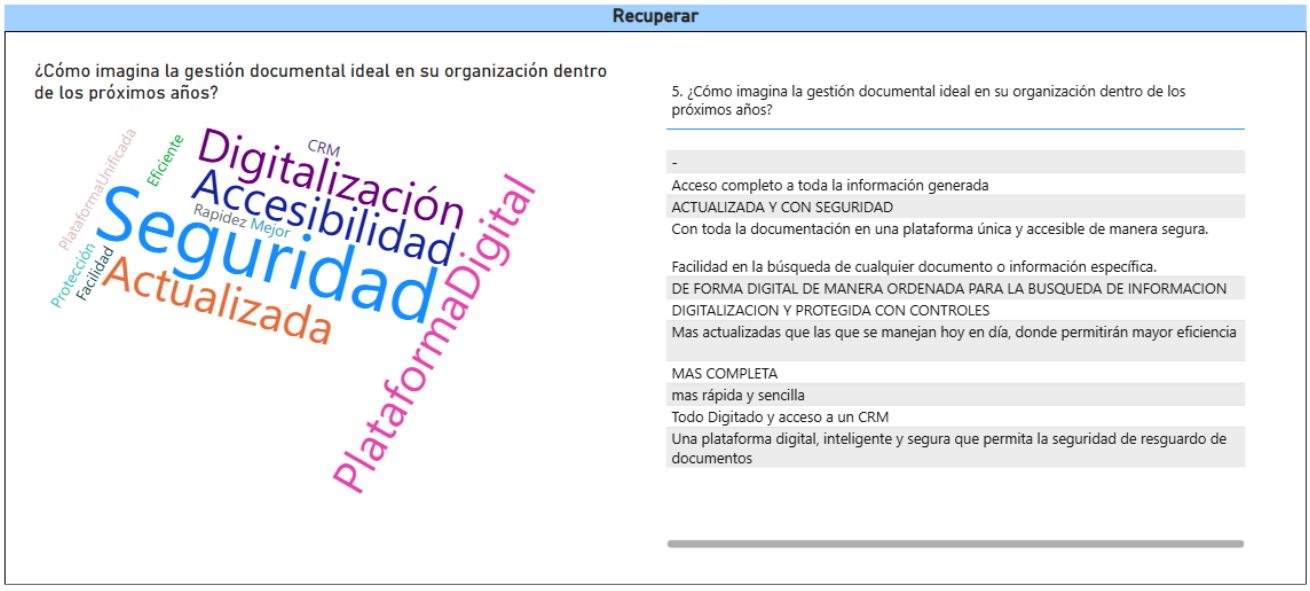


Nota: Elaborado por autores

Los resultados indican que la mayoría del personal coincide que no existen planes de recuperación de la información frente a perdidas en donde se obtuvo el 45.45% como "Neutral",18.18 "En desacuerdo" y "9.09% como "Totalmente en desacuerdo" dando un total del 72.72%. Mientras que solo el 27.27% considera que existen planes de recuperación al obtener el 18.18% como "De acuerdo" y un 9.09% como "En desacuerdo".

Esto refleja que la organización no cuenta con un plan de respaldo o contingencia claramente definido, lo que la deja expuesta ante incidentes que puedan comprometer la disponibilidad de datos críticos.

Figura 36: Gestión documental Ideal



Nota: Elaborado por autores

Los resultados cualitativos demuestran una perspectiva interesante. Los colaboradores mantienen términos como “Seguridad”, “Digitalización”, “accesibilidad”, “plataforma digital” y “actualizada”, dichos términos son recurrentes lo cual indica que los colaboradores reconocen la necesidad de evolucionar hacia un sistema documental inteligente, seguro y automatizado.

4.5.3 ANÁLISIS RESULTADOS DE LISTA DE VERIFICACIÓN DE NORMAS ISO

El análisis de las listas de verificaciones como ISO 15489, ISO 30301 e ISO 27001 permitieron evaluar la madurez documental y de seguridad de la información en la empresa seguro total, con el fin de identificar como las funciones del marco NIST de ciberseguridad pueden aplicarse para mejorar sus procesos actuales de gestión documental.

Tabla 45: Lista verificación ISO 15489

N.º	Elemento por verificar	Cumple (Sí/No/En Proceso)	Comentarios / Evidencias
1	La organización tiene una política de gestión documental aprobada por la dirección.	No	No existe dentro de la organización una política definida o aprobada con respaldo sobre la gestión documental.
2	Se identifican los requisitos legales, regulatorios y normativos aplicables.	No	No existen en Honduras regulaciones sobre el almacenamiento, seguridad y distribución sobre documentos digitales o físicos.
3	Existen responsables designados para la gestión documental en todas las áreas.	En proceso	Existen personas asignadas que reciben, solicitan documentos físicos y electrónicos, los cuales también digitalizan documentos. Pero no se encuentran definidas en las funciones o responsabilidades de sus puestos.
4	Los documentos creados son completos, auténticos y fiables.	En proceso	El 100% de los documentos creados no son completos o no están actualizados al no existir procesos definidos.
5	Los procedimientos para la captura y registro de documentos están implementados.	En proceso	Existe un proceso, sin embargo, no está estructurado o está diagramado para su consulta o revisión.
6	Los documentos tienen metadatos asignados (autor, fecha, asunto, clasificación).	No	Inexistente, actualmente no se lleva esta información complementaria de los documentos digitales. Los

N.º	Elemento por verificar	Cumple (Sí/No/En Proceso)	Comentarios / Evidencias
			documentos físicos solamente se reconocen dónde está almacenados debido a que el archivo tiene una calcomanía con el tipo de seguro y letra que indica que apellidos están almacenados en ese archivero.
7	Existe un esquema de clasificación documental aprobado y actualizado.	En Proceso	Como se menciona en el punto anterior existe un esquema de clasificación para documentación física pero el mismo puede ser más eficiente. La documentación digital se almacena en las carpetas de Google Drive de cada colaborador y la mayoría de los registros de la documentación sólo vive en el correo de Gmail.
8	Se aplican reglas de acceso y confidencialidad a los documentos.	En proceso	Solo existen los controles de acceso realizados mediante las credenciales de Google.
9	Los documentos son recuperables de manera eficiente por usuarios autorizados.	En proceso	Lo pueden recuperar solo si existe en el correo o fue almacenado en el Drive, pero no existen roles definidos de acceso y control.
10	Los documentos están protegidos contra pérdida, acceso no autorizado o destrucción.	En proceso	El acceso de los documentos físicos puede ser realizado por cualquier colaborador, los archiveros no tienen llave para cerrar. Los documentos están parcialmente protegidos con las credenciales de Google.
11	Se mantienen copias de seguridad y planes de contingencia para documentos críticos.	En proceso	Solo aquellos documentos que han sido almacenados en el Google Drive tienen copias de seguridad, no existe como tal un plan de contingencia ante brechas de seguridad y recuperación de la documentación.
12	Almacenamiento físico y digital cumple condiciones de seguridad y conservación.	No	Se cumplen funciones muy básicas de seguridad y conservación como se menciona en el punto 10.
13	Existe un calendario de conservación y disposición	No	Inexistente actualmente en la organización.

N.º	Elemento por verificar	Cumple (Sí/No/En Proceso)	Comentarios / Evidencias
	documental.		
14	Se aplican procesos documentados para eliminación o transferencia a archivo histórico.	En proceso	En caso de baja de un colaborador se envía una copia de seguridad a la gerente de operaciones para acceder al correo y Drive para recuperar información y documentación necesaria.
15	Se realizan auditorías o revisiones periódicas del sistema de gestión documental.	No	Inexistente actualmente en la organización.
16	Política y procedimientos de gestión documental se revisan y actualizan regularmente.	No	Inexistente actualmente en la organización.
17	El personal recibe capacitación en gestión de documentos.	No	No se realiza capacitación en términos de la gestión de documentos.
18	Se utilizan indicadores o métricas de eficacia en la gestión documental.	No	No existen indicadores actualmente de seguimiento de la eficacia de la gestión documental.
19	Se fomenta la mejora continua en la gestión documental.	En proceso	La junta directiva busca mejorar la gestión documental pero no se ha concretado una revisión.

Nota: Elaborada por los autores

Tabla 46: Lista verificación ISO 30301

N.º	Elemento por verificar	Cumple (Sí/No/En Proceso)	Comentarios / Evidencias
1	Se ha definido el contexto interno y externo de la organización en relación con los documentos.	En proceso	Se conoce el contexto interno y externo de la empresa y regulaciones, pero están asociadas más a la operatividad de la empresa frente a la CNBS.
2	Se han identificado las partes interesadas y sus requisitos respecto a los documentos.	Sí	Se ha identificado, pero no se ha puesto en marcha un proyecto para mejorar la gestión documental.
3	Está definido el alcance del Sistema de Gestión de Documentos (SGD).	No	El alcance del sistema de gestión documental actual no se encuentra definido o documentado.

N.º	Elemento por verificar	Cumple (Sí/No/En Proceso)	Comentarios / Evidencias
4	Existe una política de gestión documental comunicada en toda la organización.	En proceso	Existe una política de gestión básica de solicitud, revisión y almacenamiento de documentación.
5	La alta dirección demuestra liderazgo y compromiso con el SGD.	Sí	Pudimos ver en las entrevistas y las pláticas con los líderes que están comprometidos a mejorar la gestión documental dentro de la organización.
6	Roles, responsabilidades y autoridades para el SGD están claramente definidos.	No	No existe actualmente una clara definición de rol y responsabilidades asociadas al SGD.
7	Se han identificado riesgos y oportunidades relacionados con la gestión documental.	Sí	Si se han identificado desde antes de la investigación puntos por mejorar y la investigación actual lo está complementando.
8	Existen objetivos medibles para la gestión documental y planes para lograrlos.	No	No existen objetivos establecidos asociados a la gestión de documentación por lo cual no se pueden medir o tomar acciones de corrección.
9	Se asignan recursos suficientes (humanos, tecnológicos, financieros).	Sí	La empresa ha asignado los recursos necesarios para mejorar la gestión documental y otras áreas para mejorar su competitividad.
10	El personal tiene competencia y recibe formación en gestión documental.	En proceso	El personal tiene experiencia en la gestión documental, pero necesita capacitaciones extras para ser más eficientes.
11	Existe concientización sobre la importancia de los documentos.	Sí	La documentación al ser una parte integral de la correduría concientiza a los internos y expresa la importancia de su gestión.
12	Se definen y mantienen los canales de comunicación interna y externa sobre gestión documental.	En proceso	Existen canales parciales de comunicación, pero no una definición formal.
13	Se mantiene la documentación necesaria para el SGD (‘información documentada’).	En proceso	Si existe actualmente la documentación necesaria para el SGD, pero se debe revisar igualmente que esté actualizada.
14	Los procesos de gestión documental están planificados y controlados.	En proceso	Se encuentran parcialmente controlados, sin un proceso de revisión o verificación. Sí se

N.º	Elemento por verificar	Cumple (Sí/No/En Proceso)	Comentarios / Evidencias
			encuentran planificados en cómo deben realizarse en el día a día.
15	Se determinan los documentos que deben crearse, conservarse y cómo hacerlo.	Sí	Si existe un control de cuáles documentos deben crearse, conservarse y cómo hacerlo.
16	Se implementan controles y sistemas para la gestión documental de forma efectiva.	En proceso	Se revisa de forma anual o cuando son las renovaciones de las pólizas que la información esté actualizada.
17	Se monitorean y miden los procesos del SGD.	No	Actualmente no se realiza.
18	Se realizan auditorías internas al SGD.	No	Actualmente no se realiza.
19	La alta dirección revisa regularmente el sistema de gestión documental.	No	Actualmente no se realiza.
20	Se gestionan no conformidades y acciones correctivas para el SGD.	No	Actualmente no se realiza.
21	Se promueve la mejora continua del SGD.	En proceso	Si se promueve a lo interno mejorar la gestión documental.

Nota: Elaborada por los autores

Tabla 47: Lista verificación ISO 27001

N.º	Control adaptado	Aplicado (Sí/No)	Observaciones
1	La empresa cuenta con políticas internas de confidencialidad y resguardo de datos de clientes asegurados.	No	No existen actualmente políticas internas que los colaboradores firmen con respaldo legal para temas de confidencialidad y resguardo de la información.
2	Se han definido roles de seguridad de la información, incluyendo al responsable ante la CNBS.	No	No existe un rol como tal de la seguridad de la información.
3	Existe un inventario actualizado de sistemas críticos: plataforma de emisión de pólizas, CRM, bases de datos de clientes.	No	No se lleva un inventario de sistemas críticos. Internamente la correduría solo depende de Gmail, Google Drive, Microsoft Word, Microsoft Excel, PowerPoint y Adobe Acrobat.
4	El acceso a sistemas de pólizas y bases de datos está restringido por roles y	No	MFA no se utiliza.

	autenticación multifactorial.		
5	Se gestionan vulnerabilidades en aplicaciones de clientes (web y móviles) y se validan con pruebas periódicas de seguridad.	No	No se realizan pruebas de vulnerabilidad y tampoco pruebas periódicas de seguridad.
6	Los datos personales y financieros de los asegurados se encuentran cifrados en reposo y en tránsito.	Parcial	Se utilizan los protocolos de seguridad inherentes de Google.
7	Se realizan pruebas de penetración enfocadas en portales de clientes y sistemas de pago electrónico.	No	No se realizan este tipo de pruebas.
8	Se cuenta con un registro de incidentes relacionados con fraude digital, fuga de datos o caídas de sistemas.	No	No se lleva un control o seguimiento de incidentes.
9	La organización revisa periódicamente los controles de seguridad conforme a ISO 27001, Ley de Protección de Datos y normativa CNBS.	No	Al no ser requisitos legales en Honduras aún no se emplean los controles de seguridad mencionados.

Nota: Elaborada por los autores

Los resultados evidencian que la organización se encuentra en una etapa inicial de madurez, con procesos no estandarizados y carencia de políticas internas completas, lo que limita grandemente la correcta identificación, protección y trazabilidad de la información.

En términos generales, los hallazgos revelan que la organización opera con procesos empíricos y descentralizados, sin políticas formales de documentación ni controles estructurados de seguridad. Esto se traduce con una madurez cibernética inicial, donde predominan acciones reactivas frentes a los riesgos en lugar de estrategias preventivas alineadas con estándares internacionales.

La evaluación permite identificar las funciones “Identificar”, “Proteger” presentan nivel medio-bajo de avance, mientras que “Detectar”, “Responder” y “Recuperar” muestran carencias significativas, en base a eso se detallaran los principales hallazgos y su relación con el marco NIST.

4.5.3.1 ANÁLISIS DE LAS NORMAS ISO

- **ISO 15489**

Con la aplicación de la lista de verificación, se permitió analizar de mejor manera la existencia de las políticas, procedimientos y estructuras asociadas al control de documentos. Los resultados muestran que la corredura Seguros Total carece de un sistema para crear, clasificar, almacenamientos y disposición de los documentos. Lo que genera problemáticas internas entre ellas la pérdida de trazabilidad o una clara dependencia a procesos manuales.

Se identificó que los archivos no poseen metadatos normalizados y aunque se mantiene

inventarios de algunos documentos, esto impide una correcta identificación de los activos de información. Este vacío afecta directamente la función “Identificar” la cual necesita un conocimiento claro de los sistemas, datos y procesos que deben protegerse. Asimismo, la falta de controles de validación sobre los documentos limita la función “Detectar”, ya que no se cuenta con mecanismos que permitan verificar alteraciones o inconsistencia.

- **ISO 30301**

La evaluación basada en dicha norma mostró algunos avances en materia de liderazgo y compromiso institucional, pero sin evidencia de un sistema documentado, roles definidos ni objetivos medibles vinculados a la gestión de información.

Aunque se reconoce la importancia de la documentación para la organización y sus operaciones, no se han establecido procedimientos formales para la planificación, monitoreo y evaluación del desempeño documental. ni mecanismos de auditoría o mejora continua. Estas falencias guardan una relación concreta y directa con las funciones “Proteger”, “Responder” y “Recuperar” ya que la falta de controles operativos formales y planes de contingencia limita la capacidad de la organización para proteger sus activos de información y Responder ante incidentes, tales como, pérdida, corrupción o acceso no autorizado.

- **ISO 27001**

La lista de verificación basada en esta norma permitió examinar los controles de seguridad, gestión de riesgos, confidencialidad y disponibilidad de la información. Los resultados evidencian la ausencia de una política institucional de seguridad de la información, así como, la falta de inventarios de activos, controles de accesos formales y auditorías de seguridad. La empresa depende de las medidas predeterminadas del ecosistema Google Workspace, sin que existan políticas propias de cifrado, autenticación o monitoreo de incidentes, dichas carencias impactan directamente en las funciones Proteger, Detectar, Responder, Recuperar del marco NIST.

4.5.4 ANÁLISIS RESULTADOS DE LISTA DE VERIFICACIÓN DEL MARCO NIST

Tabla 48: Lista de verificación NIST

Función NIST	Categorías / Controles evaluados	Descripción de la práctica esperada	Nivel de cumplimiento	Evidencia observada
Identificar **(Identificar)**	1. Inventario de activos documentales	Se mantiene un inventario actualizado de documentos, sistemas y usuarios con acceso.	No cumple	No existen inventarios formales; la información se gestiona manualmente.
	2. Clasificación y metadatos	Los documentos se clasifican según tipo y nivel de confidencialidad.	En proceso	Carpeta general por área, sin clasificación estructurada.
	3. Roles y responsabilidades	Se han definido roles de custodia y propiedad de la información.	No cumple	No hay responsables formales ni jerarquía documental.
	4. Evaluación de riesgos	Se realiza evaluación de riesgos sobre información y procesos digitales.	No cumple	No hay matriz de riesgos documental ni tecnológica.
Proteger (Proteger)	1. Control de acceso	Los permisos de acceso se definen según rol o nivel jerárquico.	En proceso	Usuarios gestionan accesos sin control institucional.
	2. Cifrado y seguridad de datos	Los datos están cifrados en tránsito y reposo.	En proceso	Cifrado automático de Google Workspace.
	3. Capacitación en seguridad	El personal recibe formación en manejo seguro de información.	No cumple	No hay capacitaciones ni guías de buenas prácticas.
	4. Políticas y procedimientos	Existen políticas formales de seguridad y gestión documental.	No cumple	No hay políticas documentadas ni difundidas.

	5. Respaldo de información	Se realizan respaldos periódicos de documentos críticos.	No cumple	No se realizan copias ni hay plan de respaldo.
Detectar (Detectar)	1. Monitoreo de accesos	Se lleva registro de accesos y modificaciones en documentos.	No cumple	No existen bitácoras ni auditorías.
	2. Alertas y notificaciones	El sistema genera alertas ante cambios o intentos no autorizados.	No cumple	Drive no posee alertas activas.
	3. Auditorías internas	Se ejecutan auditorías periódicas de control documental.	No cumple	No se han realizado auditorías de control o seguridad.
Responder (Responder)	1. Procedimientos ante incidentes	Existen protocolos de actuación ante pérdida o corrupción documental.	No cumple	No hay protocolos definidos.
	2. Comunicación interna	Se establecen canales de notificación y gestión de incidentes.	No cumple	La comunicación es informal y reactiva.
	3. Registro de incidentes	Se documentan y analizan los incidentes ocurridos.	No cumple	No hay registro de eventos o incidentes.
Recuperar (Recuperar)	1. Plan de continuidad y recuperación	Se cuenta con planes de respaldo y restauración de datos.	No cumple	No existen procedimientos de recuperación.
	2. Validación de respaldos	Se realizan pruebas de recuperación de datos.	No cumple	No hay pruebas o simulacros.
	3. Actualización de planes	Los planes se revisan y actualizan regularmente.	No cumple	No existen revisiones periódicas.

Nota: Elaborado por autores

Tabla 49: Resumen general de madurez en base al marco NIST

Función NIST	Nivel general de cumplimiento	Evaluación cualitativa
Identificar	Bajo	No existen inventarios ni roles definidos; gestión manual.
Proteger	Medio bajo	Cifrado básico, sin políticas ni capacitación.
Detectar	Bajo	Sin monitoreo ni alertas activas.
Responder	Bajo	No hay protocolos ni registros de incidentes.
Recuperar	Bajo	No existen respaldos ni planes de continuidad.

Fuente: Elaborado por autores.

Los resultados de la matriz reflejan que seguro total mantiene un nivel inicial de madurez cibernética, caracterizado por la ausencia de políticas institucionales, controles formales y procedimientos ante emergencias. A pesar de contar con tecnologías como Google drive que es funcional, el uso actual es limitado a nivel de gobernanza documental y de seguridad careciendo de una estructura preventiva o reactiva.

La función Identificar evidencia la principal debilidad: la empresa no tiene visibilidad ni control de sus activos documentales, lo que impide gestionar riesgos o priorizar información crítica.

En Proteger, aunque se aprovechan funciones automáticas como el cifrado de Google, no existen controles administrativos, respaldo ni capacitación del personal, lo que limita la protección efectiva.

Las funciones “Detectar”, “Responder” y “Recuperar” presentan un nivel muy bajo, evidenciando la ausencia total de monitoreo, protocolos de respuesta y planes de recuperación, lo cual deja a la empresa expuesta ante eventos de pérdida o alteración de información.

Basado en ese diagnóstico, se debe priorizar la iniciación o aplicación del Marco NIST mediante las funciones de identificar y proteger, esto para llegar a un nivel de madurez necesario.

4.5.5 ANÁLISIS RESULTADOS DE NIST FRAMEWORK: GUÍA DE INICIO RÁPIDO PARA PEQUEÑAS EMPRESAS

Tabla 50: Función Gobernar (Contexto Organizativo)

Establecimiento del contexto organizativo	
Nuestra misión empresarial:	Somos una Correduría de seguros que nace para brindar tranquilidad a nuestros clientes con asesoría en servicios y productos de Seguros que promueven el crecimiento y resguardo de su patrimonio ante posibles riesgos, con el personal comprometido altamente calificado y motivado.
¿Qué riesgos de seguridad cibernética pueden impedirnos lograr esta misión?	Pérdida o alteraciones de información de clientes por accesos no autorizados, filtraciones de datos, falta de copias de seguridad o respaldos, uso de herramientas sin seguridad adecuada.

Nota: Elaborado por autores

Tabla 51: Requisitos de Seguridad Cibernética

Documentación de los requisitos de seguridad cibernética	
Enumere sus requisitos legales:	● Ley de protección de datos personales ● Reglamento del CNBS
Enumere sus requisitos normativos:	● ISO: 27001 ● ISO:30301 ● ISO: 15489 ● Marco NIST de Ciberseguridad
Enumere sus requisitos contractuales:	● Contratos con aseguradoras. ● Acuerdo de licencias para Google Workspace

Nota: Elaborado por autores

Actualmente se mantiene una misión empresarial firme, basada directamente en la protección del patrimonio de los clientes, enfatizando en la seguridad de estos y de la información que el cliente confía, basado en ello, podemos encontrar múltiples riesgos que comprometería la misión como la pérdida de información, filtración de datos o hasta el mal desarrollo de la documentación.

Con ello se planea brindar una mejora considerable enumerando requisitos normativos como normas ISO o marco NIST.

Tabla 52: Control de Sistemas

Software/ hardware/ sistema/ servicio	**Uso oficial del activo**	**Administrador o propietario del activo:**	**Identifique los datos sensibles a los que tiene acceso el activo:**	**¿Se requiere autenticación de múltiples factores para acceder a este activo?**	**Riesgo para la empresa si perdemos el acceso a este activo**
Google Drive	Almacenamiento, verificación de información, respaldos	Gerente General, administrador de información	Contratos, pólizas, información por colaborador, información contable	No	Alto: se pierde información sensible de cada capa que compone la empresa
Correo corporativo	Comunicación interna y externa, envío de documentación y digitalización	Gerente general, administrador y área de atención	Datos personales y de contacto de clientes	No	Alto: se filtran datos y pérdida de información sensible
Computadoras por usuario	Procesamiento, almacenamiento temporal y digitalización de documentos	colaboradores	Datos personales	No	Alto: vulnerabilidad ante pérdida de información personal

Sistema de pólizas	Registro manual, almacena datos por póliza	Colaboradores (área de venta y atención)	Datos por póliza, información de clientes	No	Alto: pérdida de información o modificación no autorizada

Nota: Elaborado por autores

Basado en la matriz encontramos hardware y software que está a la disposición de la correduría, entre las cuales podemos ver el impacto que genera su uso, así como, el impacto que generaría al perder el activo. Esto podría influir mucho en el desarrollo óptimo de la empresa, de igual manera mermaría la confianza del cliente hacia la MiPyme.

Tabla 53: Controles de Seguridad asociado a cuentas

Cuentas	**MFA habilitado (sí/no)**
Cuenta(s) bancaria(s)	Sí
Cuenta(s) contable(s) y fiscal (es	Sí
Cuenta(s) comercial (es	Sí
Cuentas de Google, Microsoft y/o ID de Apple	No
Cuenta(s) de correo electrónico Gestor(es) de	No
Cuentas de sitios web	No

Nota: Elaborado por autores

Basado en la matriz anterior, se puede observar que únicamente las cuentas bancarias y comerciales disponen de esta medida de seguridad, lo que demuestra una protección prioritaria hacia los activos financieros, sin embargo, el resto de las cuentas institucionales, como contables, fiscales, correos o gestores de documentos carecen de MFA.

Tabla 54: Matriz de responsables de la correduría

Contacto	Nombre	Teléfono	Responsabilidad
Responsable de la empresa:	Karla Lima	+(504) 9992-3044	Responsable principal del cumplimiento de la organización.
Soporte Técnico:	Erick	+(504) 9510-3879	Responsable de dar mantenimiento al hardware y software.
Administrador de Correo:	Christian Padilla	+(504) 9915-6014	Responsable de G-Suite.
Administrador de dominio y página web:	Ingenio Digital-Rubén	+(504) 9570-2083	Responsable del mantenimiento de la página web, dominio corporativo y campañas de marketing.
Administrador de Sistema de Póliza	Dynamic Solutions	+(504) 2221-3125	Responsable como SaaS del mantenimiento y extensión de funcionalidades.
Policía	Policía	911	Emergencias físicas y digitales.
Legal:	Carlos Flores	+ (504) 9760-7729	Efectos legales de contratos, pólizas o seguimientos.
Bancos:	Diferentes Bancos	Número de soporte al cliente	Gestión de cuentas monetarias.
Seguros:	Diferentes Compañías	Contacto números oficiales de compañías aseguradoras	Control de alta, actualización o baja de pólizas.

Nota: Elaborado por autores

Basado en la matriz anterior, se evidencia una estructura de respuesta parcialmente organizada, con funciones distribuidas entre personal interno (administración, soporte técnico y gestión de correos) y proveedores como Dynamic soluciones.

Sí bien existe una red de contactos operativos definida, no se cuenta con un protocolo

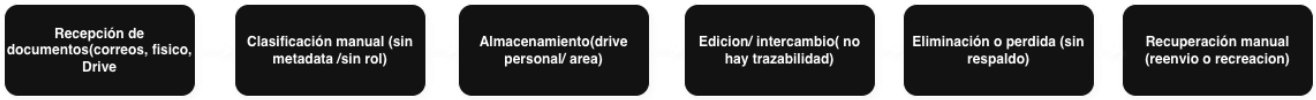
formal de actuación ni con un plan de respuesta documentado. La comunicación ante incidentes depende de la disponibilidad individual y de la experiencia técnica de cada responsable, sin mecanismos de escalamientos o tiempos de respuesta establecidos limitando la eficacia de la coordinación ante incidentes críticos como pérdida de acceso, falla de software o ataques a los sistemas de información.

4.5.6 ANÁLISIS RESULTADOS DEL FLUJO DE PROCESOS

Considerando la actualidad de la correduría seguros total, el flujo de procesos orientado a las funciones NIST puede demostrar con claridad los factores que afectan el óptimo funcionamiento de la empresa, actual el flujo se tiene características como:

- No existe sistema de gestión documental centralizado
- Dependencia manual en múltiples factores
- Falta de control de seguridad y trazabilidad

Figura 37: Flujo actual de procesos



Nota: Elaborado por autores.

- Identificar: No hay inventario ni clasificación.
- Proteger: No hay políticas ni controles de acceso.
- Detectar: No existen registros ni alertas.
- Responder: No hay protocolos de respuesta ante errores.
- Recuperar: No existen respaldos ni restauración sistemática.

4.5.7 HALLAZGOS DE OBJETIVO 4

Con base a los instrumentos aplicados se sintetizan los principales hallazgos con dimensiones clave para la gestión documental y la seguridad de la información de la correduría Seguros total.

a. Hallazgo sobre gobernanza y estructura organizacional

   El estudio muestra que Seguro Total carece de un sistema formal para la gestión documental. No hay políticas internas, ni procedimientos establecidos, ni personas asignadas para manejar el ciclo de vida de los documentos. A pesar de que gran parte del equipo tiene un entendimiento básico sobre ciberseguridad, esa conciencia no se

refleja en prácticas estandarizadas ni en métodos de monitoreo. La falta de funciones, indicadores y controles infringe los principios de la ISO 30301 y la función Gobernar del NIST CSF, lo que posiciona a la empresa en un estado preliminar de madurez en gestión documental.

b. Hallazgo sobre cumplimiento normativo

Las listas de verificación realizadas revelan un bajo nivel de adherencia a los requisitos de gestión de documentos y seguridad definidos por los estándares internacionales. Se han encontrado incumplimientos constantes en áreas como la trazabilidad, manejo de versiones, políticas de retención, auditorías y clasificación, que son fundamentales en las normas ISO 30301 e ISO 15489. Además, la ausencia de controles de acceso, autenticación de múltiples factores, inventario de activos y procedimientos de vigilancia evidencia el incumplimiento en los ámbitos de seguridad de la ISO 27001, así como las funciones de Identificar, Proteger, Detectar, Responder y Recuperar del NIST CSF. En cada uno de estos marcos, las categorías mayormente presentes son “En proceso” o “No cumple”.

c. Hallazgos sobre necesidades operativas de seguro total

El análisis indica que la organización necesita un sistema de documentos que pueda unir trazabilidad, pruebas documentales que puedan ser verificadas, clasificación ordenada, control seguro de accesos, retención automática y apoyo a procesos esenciales como renovaciones y reclamaciones. La evaluación del desempeño real señala la necesidad inmediata de:

- Único repositorio institucional
- Flujos documentos estandarizados
- Disminución de la dependencia del juicio particular del trabajador
- Herramientas que no necesiten soporte interno de TI
- Coordinación entre procesos, software y estructura tecnológica.

La falta de estos componentes impacta negativamente en la eficiencia operativa, aumenta los reprocesos y restringe la capacidad de proporcionar un servicio constante al cliente.

d. Hallazgo de riesgo

El entorno actual presenta riesgos críticos derivados del uso de herramientas informales,

ausencia de mecanismos de trazabilidad y falta de controles de seguridad.

4.6 OPORTUNIDADES DE MEJORA PARA LA CORREDURÍA SEGURO TOTAL

El presente objetivo tiene como finalidad identificar y proponer oportunidades de mejora en los procesos de gestión documental de Seguro Total, tomando como referencia los requisitos de la ISO 30301:2019, las guías funcionales de la ISO/TS 161752:2020, los controles de seguridad de la ISO/IEC 27001, y los lineamientos de gobernanza establecidos en la función Gobernar del Marco NIST CSF 2.0.

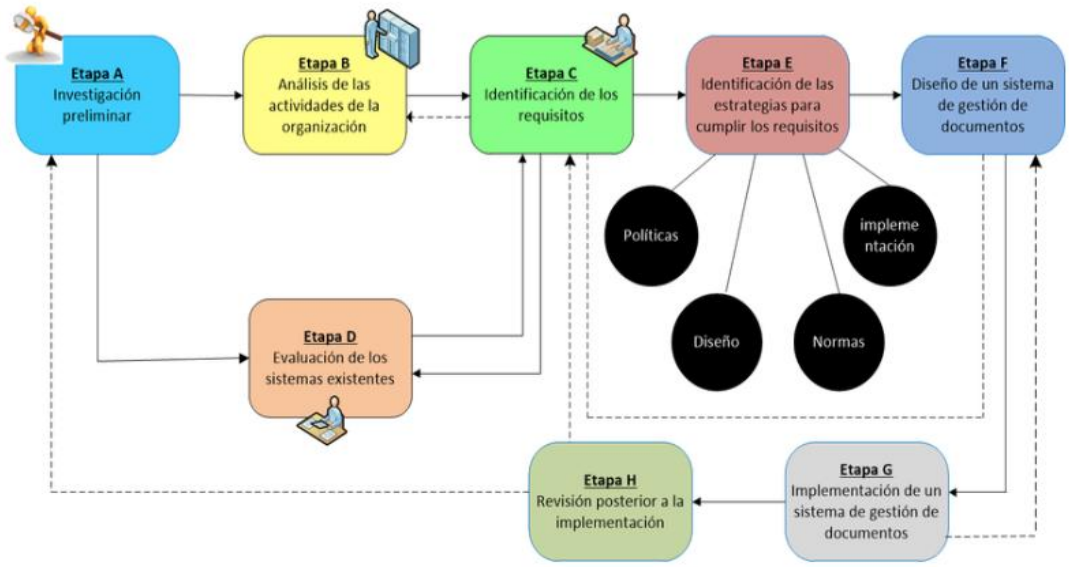
Para llevar a cabo este análisis se aplicó la metodología DIRKS (AS ISO 15489), abarcando únicamente las etapas A–D, enfocadas en evaluación, diagnóstico y detección de mejoras. La implementación y diseño del sistema documental (Etapas F–H) se desarrollará posteriormente en el Capítulo VI.

4.6.1 ANÁLISIS RESULTADOS DE OBJETIVO 5

Figura 38: Instrumentos aplicados al Objetivo 5

Nota: Elaborado por los autores

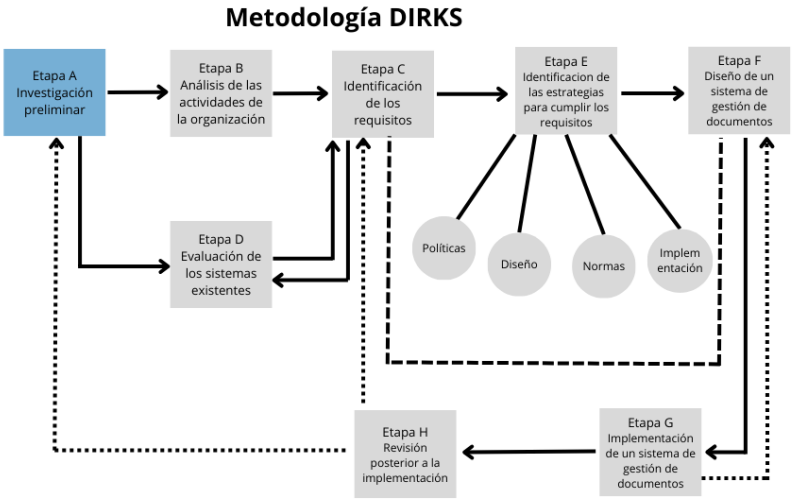
Figura 39: Proceso Metodología DIRKS



Nota: Información obtenida de Cárdenas Giler, Wilches Medina, Peñate Santana & Lozada Núñez, 2018).

4.6.2 ETAPA A – INVESTIGACIÓN PRELIMINAR Y DIAGNÓSTICO DE LA GOBERNANZA ACTUAL

Figura 40: Etapa A metodología DIRKS



Nota: Elaborada por los autores

En esta etapa se recopiló información general sobre la estructura organizativa, los documentos generados, los sistemas utilizados y las prácticas actuales de manejo de información y gestión de documentos. Las principales oportunidades de mejora identificadas son las siguientes:

4.6.2.1ANALISIS DEL CONTEXTO EMPRESARIAL:

Durante esta etapa la cual está relacionada al objetivo uno de la investigación se recopilo información a través del diferentes instrumentos temáticos y metodológicos, observación y notas de campo en la oficina principal de Tegucigalpa. Este ejercicio permitió identificar de forma general que, aunque la organización reconoce la importancia de la digitalización y la accesibilidad de esta para mejorar la toma de decisiones, esto no se ha traducido en un sistema formal de gestión de la documentación.

La estructura interna de la correduría evidencia una fuerte dependencia hacia el conocimiento de cada individuo, practicas informales de gestión de documentación, criterios no unificados de búsqueda de información, incorrecto almacenamiento de documentos tanto físicos como digitales. Lo cual evidencia un grado de madurez inicial o bajo frente a la ISO 15489 en términos de gestión documental, sin acompañamiento de gobernanza, controles o estándares formales dentro de la correduría.

Con base a esto encontramos las siguientes oportunidades de mejora:

1.Fortalecimiento del marco de gestión documental y gobernanza (ISO 15489, ISO 30301 y Gobernar NIST)

Se han identificado oportunidades para consolidar un modelo de gobernanza de la documentación con mayor estructuración durante todo el ciclo de vida documental centrándonos en la base de la ISO 15489, enfocándose en la definición de roles y responsabilidades, alineación con los objetivos estratégicos de la correduría, escalabilidad, facilidad de uso, accesibilidad de la información y definición de criterios de éxito y de monitoreo.

Esta oportunidad da respuesta y se conecta con la gobernanza que se necesita sobre la documentación por la ISO 30301, y el componente de Gobernar del NIST haciendo énfasis en el liderazgo, dirección estratégica y control de la arquitectura empresarial.

2.Mejorar la coordinación de las actividades operativos con las actividades documentales asociado a la ISO 30301

Mejora la comunicación interdepartamental entre los colaborades beneficiándose de un mecanismo más claro de coordinación, lo que permitirá mejor la transferencia de conocimiento y eficiencia de las actividades documentales diarias, esto con base la Norma ISO 15489 en donde todo el ciclo de vida de la gestión documental debe realizarse de forma estructurada en toda la organización. Considerando que la gestión documental sea más eficiente y se alinee con la estrategia interna para como base para utilizar la Norma ISO 30301.

3.Mejorar el control, autenticidad, veracidad y trazabilidad de los documentos

Se han identificado oportunidades relacionadas en la forma actual de cómo se organizan, describen y clasifican los documentos. Como base de la ISO 15489 todo documento debe ser confiable y tener sus metadatos corresponde rientes los cuales faciliten su almacenamiento e identificación dentro de la organización.

4.Mejorar los controles de Seguridad (ISO 27001, NIST Gobernar, ISO 15489)

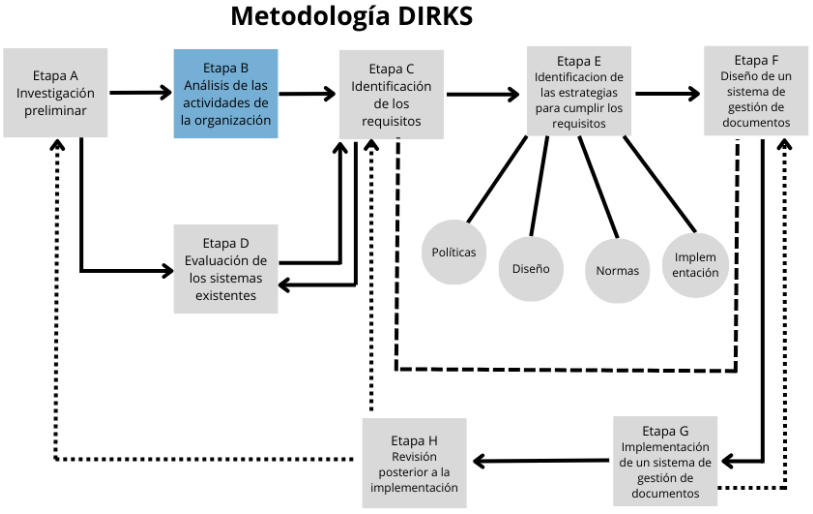
Con base al bajo nivel de seguridad en las aplicaciones utilizadas por la correduría se ha identifica la oportunidad de mejorar todos los protocoles de acceso tanto a las plataformas digitales utilizadas por la correduría como el acceso a documentos físicos.

5.Asegurar la disponibilidad y continuidad de la gestión documental

Como principio clave de la ISO 15489 se identificado la oportunidad de mejorar la disponibilidad de los documentos dentro de la correduría, en donde se deben fortalecer mecanismo que garanticen la continuidad del negocio, acceso y recuperación de los documentos ante incidentes, entrelazándose con los requisitos de continuidad de la ISO 27001.

4.6.3 ETAPA B – ANÁLISIS DE LAS ACTIVIDADES Y EVALUACIÓN DE RESPONSABILIDADES DOCUMENTALES

Figura 41: Etapa B metodología DIRKS



Nota: Elaborada por los autores

Esta etapa permitió centrarse en identificar y analizar cualquier actividad que realice la organización que generen, reciben, o requiera acceso a documentación, así como determinar roles actuales y potenciales involucrados en la gestión documental. El objetivo es comprender en como circula la información en la organización, cual es la función de esta en los flujos

operativos y su alineamiento con los principios normativos internacionales de gestión documental y seguridad de la información.

4.6.3.1 RELACIÓN ENTRE LAS ACTIVIDADES DEL NEGOCIO Y LA GENERACIÓN DOCUMENTAL

Los resultados en los hallazgos del objetivo 1 muestran que todos los procesos operativos de seguro total dependen de la documentación como insumo clave en el negocio. Cada fase que se realiza en el flujo operativo como cotización, suscripción, emisión o cualquier servicio como gestión de reclamos y renovación implica la creación y manejo de información clave como documento nacional de identificación, diagnósticos y dictámenes médicos, contratos, pólizas, anexos o cualquier comprobante que implique ajustar a la gestión de documentación. Sin embargo, esta documentación no se gestiona de manera íntegra o uniforme, ya que podría variar entre cada colaborador porque cada uno de ellos aplica su propio criterio de gestión de archivos, clasificación y comunicación lo cual podría fragmentar el ciclo de vida del documento y dificulta su trazabilidad.

4.6.3.2 FLUJOS DOCUMENTALES INFORMALES Y VARIABILIDAD OPERATIVA

El análisis realizado evidencia que las actividades documentales se desarrollan en un ambiente informal, caracterizado por la ausencia de procedimientos institucionales, falta de lineamientos operativos y la inexistencia de mecanismos de control que regulen el flujo, validación y preservación de documentos.

En la práctica la gestión se lleva a cabo mediante métodos y herramientas no estandarizadas, entre lo que podemos observar:

- Uso simultaneo de múltiples plataformas no integradas

  Considerando el constante uso de herramientas diversas, esto puede ocasionar problemas operativos y de versiones que pueden crear fragmentación documental, inconsistencia y perdidas de trazabilidad, ya que no existe un repositorio institucional único ni un mecanismo obligatorio de registro. Entre las herramientas más comunicas usadas como plataforma encontramos: WhatsApp, correos electrónicos personales, correo corporativo, Google Drive, etc. Aquí los documentos se intercambian y almacenan de manera paralela y sin un control especifico.

- Ausencia de puntos de control formales

  Actualmente no se han definido etapas o hitos en los procesos para validar la completitud de la documentación ni verificar la autenticidad de la información, así

como, confirmar la vigencia de esta. Esta falta de un punto de control formal genera expedientes incompletos, obsoletos o inconsistentes afectando la exactitud del proceso como también, la eficiencia operativa y la calidad de la gestión documental.

- Gestión de versiones no adecuada

  La ausencia de control de versiones que es uno de los requisitos primordiales de ISO 30301 e ISO 15489 provoca múltiples consecuencias que generan inconformidad y mala gestión operativa. Algunas como la existencia de múltiples archivos con el mismo nombre, versiones no oficiales, imposibilidad de identificación de documento final y diferencias entre cada colaborador. Esto afecta procesos críticos como renovaciones y reclamos, donde la veracidad y actualización del documento tiene implicaciones legales y contractuales.

- Falta de evidencia del ciclo de revisión y aprobación

  El análisis muestra la falta de mecanismos que permiten saber quién realizo uno revisión del documento, cuando, donde y que tipo de modificación hizo. Esta falta de trazabilidad interna es sumamente problemática ya que impide reconstruir el historial documental, comprometiendo la confiabilidad del expediente y limitando la capacidad de auditoría.

- Almacenamiento según el criterio del colaborador

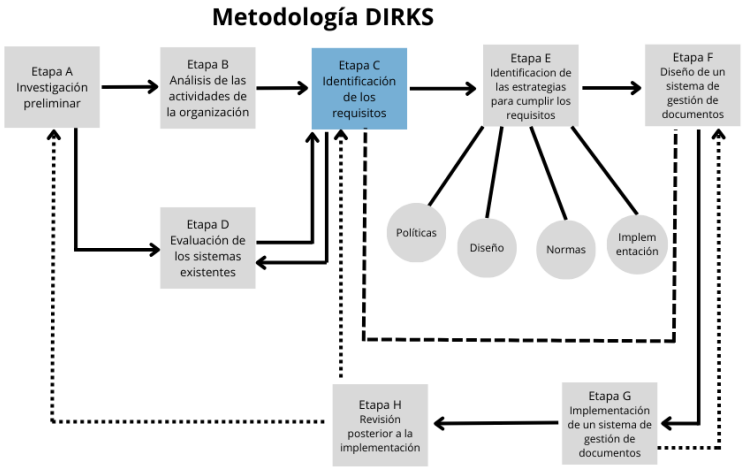
  No existe patrón o estructura especifica de nombrado, clasificación, orden y almacenamiento para un documento. Lo que genera problemáticas constantes como carpetas duplicadas, inconsistencia estructural, documentos ubicados en carpetas erróneas, falta de visibilidad institucional sobre la documentación esencia lo que genera un sin fin de problemas que ocasionan lentitud, problemas de búsqueda, dificultad operativa y el no cumplimiento de requisitos básicos para l ISO 15489 e ISO 27001.

Considerando estos factores podemos tener múltiples consecuencias operativas ya identificadas como ser:

- Riesgo elevado de pérdida o alteración de documentación
- Inconsistencia en la información utilizada para la toma de decisiones
- Incremento de reprocesos y tiempos operativos
- Exposición a incumplimientos regulatorios
- Dificultad para Responder auditorías internas o externas

4.6.4 ETAPA C – IDENTIFICACIÓN DE LOS REQUISITOS NORMATIVOS Y DE GOBERNANZA (ISO 30301, ISO 15489, ISO 27001 Y NIST GOBERNAR)

Figura 42: Etapa C metodología DIRKS



Nota: Elaborada por los autores

La Etapa C de la metodología DIRKS se centra en evaluar los requisitos base por los cuales debe estructurarse un sistema de gestión documental de una organización. En este punto es necesario evaluar todos aquellos criterios legales, institucionales, operativos y normativos que influyen directamente en el ciclo de vida de los documentos y en la forma en que estos deben ser creados, gestionados, protegidos y conservados. En este caso se utilizan como referencia los principios y lineamientos establecidos en la ISO 15489, que constituye la base para determinar qué atributos debe cumplir un documento para ser auténtico, confiable, íntegro y utilizable.

Asimismo, se incorporan los requisitos de gobernanza, desempeño y evidencia exigidos por la ISO 30301, y los controles de seguridad definidos por la ISO 27001**.** Estos marcos normativos se complementan con la función Gobernar del NIST Marco de Ciberseguridad 2.0.

1.Requisitos institucionales

Existe una oportunidad para estructurar de manera más concreta los requisitos que definen la creación, clasificación, acceso, uso, retención y disposición de los documentos con base a las necesidades de la correduría tanto actuales, como su futuro crecimiento. La información disponible muestra que estos criterios se aplican de forma intuitiva o bajo prácticas heredadas, lo que difiere del enfoque sistemático requerido por la ISO 15489 y la ISO 30301.

Con base al marco NIST se destacan las oportunidades de mejorar de definir los roles y privilegios la información que administra; esta etapa evidencia la oportunidad de fortalecer ese marco.

2.Requisitos de autenticidad, integridad y confiabilidad

Los requisitos para la autenticidad, integridad y trazabilidad del documento no están completamente establecidos ni expresados formalmente. Esto abre la oportunidad de fortalecer los lineamientos que garantizan que los documentos mantengan su valor único y su integridad a lo largo del tiempo, conforme lo exige la ISO 15489.

3.Requisitos de seguridad y protección

Los mecanismos actuales de seguridad se apoyan en configuraciones predeterminadas de herramientas tecnológicas, sin integrar de manera formal los requisitos de seguridad de la ISO 27001.Esto presenta la oportunidad de definir requisitos más robustos relacionados con:

- Control de accesos,
- Multifactor de autenticación a cuentas institucionales
- Protección de documentos físicos y digitales,
- Gestión de incidentes,
- Continuidad y respaldo.

Tanto ISO 27001 como el Marco NIST subrayan que los requisitos de seguridad deben estar definidos antes del diseño de los procesos, lo cual se evidencia como una oportunidad de mejora en esta etapa.

3.Requisitos de definición de Roles y Privilegios documentales

Se identifica una oportunidad para especificar los requisitos relacionados con las responsabilidades de quienes crean, gestionan, almacenan y disponen los documentos. Actualmente, estas responsabilidades no están delimitadas en los procesos o descripciones de los roles de la correduría, lo que dificulta la trazabilidad y la rendición de cuentas.

Según ISO 15489, estos requisitos deben estar definidos desde la fase de identificación, y la ISO 30301 complementa esta necesidad mediante su estructura de gobernanza y asignación de responsabilidades.

4.Requisitos para continuidad, disponibilidad y recuperación

La organización presenta la oportunidad de definir los requisitos de la disponibilidad de la información, considerando situaciones de incidentes, pérdida de datos o indisponibilidad de

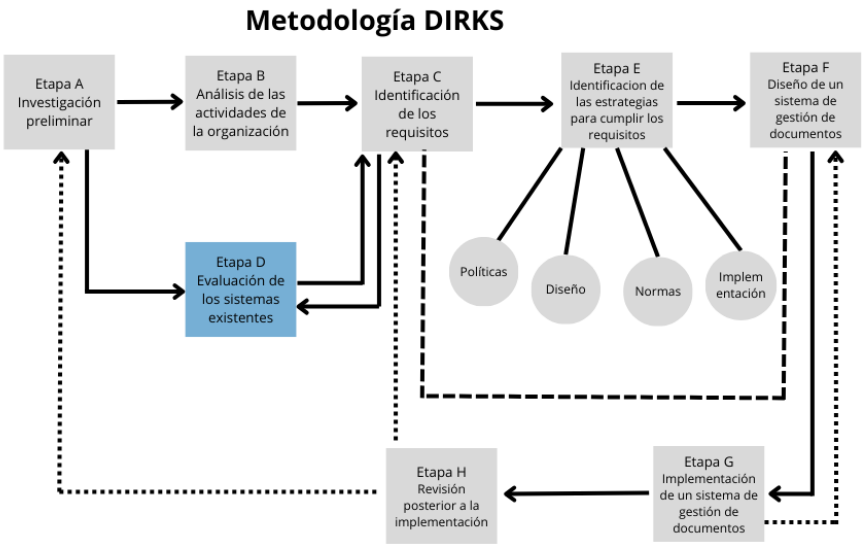
los medios usados. La ISO 15489 establece que la información debe estar disponible cuando se necesite, mientras que la ISO 27001 exige la existencia de requisitos explícitos para continuidad y recuperación, lo cual aún puede fortalecerse.

5.Requisitos para el monitoreo, seguimiento y mejora continua

Se presenta una oportunidad para definir requisitos vinculados a la evaluación del desempeño, indicadores y mecanismos de seguimiento. La ISO 30301 demanda un enfoque de gestión basado en resultados y evidencia, mientras que NIST enfatiza la necesidad de estructuras que permitan revisar y ajustar los requisitos de forma continua. En el contexto actual, estos procesos aún no se encuentran definidos y representan un punto de mejora clave.

4.6.5 ETAPA D – EVALUACIÓN DE LOS SISTEMAS EXISTENTES Y BRECHAS DE GOBERNANZA DOCUMENTAL

Figura 43: Etapa D metodología DIRKS



Nota: Elaborada por los autores

La Etapa D de la metodología DIRKS se centra en evaluar de manera crítica los sistemas, herramientas y prácticas tecnológicas actualmente utilizadas en Seguro Total para la gestión de documentos, con el propósito de determinar su capacidad para cumplir con los requisitos

funcionales, normativos y de gobernanza establecidos por estándares internacionales como ISO 30301, ISO 15489, ISO 27001 y el Marco NIST CSF 2.0.

Este análisis presenta un punto clave en el diagnostico, ya que permite identificar brechas que deben ser abordadas para fortalecer el sistema documental y avanzar hacia una arquitectura más segura, estandarizada y resiliente. Los resultados evidencian que la organización funciona mediante un sistema fragmentado, informal y sin lineamientos institucionales, lo que dificulta el cumplimiento exigido por las ISO antes mencionadas.

a. Fragmentación del sistema y ausencia de un repositorio único

Se ha destacado, entre varios puntos cruciales, la fragmentación informativa entre plataformas, careciendo de un eje central para la documentación oficial. Actualmente, los datos de los usuarios se hallan diseminados en Google Drive, tanto en correos electrónicos personales como laborales, conversaciones de WhatsApp, archivos guardados localmente y documentos físicos almacenados sin orden. Esta dispersión entorpece el rastreo documental, dificulta encontrar datos esenciales, eleva el riesgo de duplicidades y causa discordancias entre las distintas copias existentes. Esta situación constituye un incumplimiento de los pilares de autenticidad, integridad y accesibilidad de la norma ISO 15489, y contraviene el control operativo exigido por la norma ISO 30301, que demanda depósitos seguros y regulados.

b. Capacidades y limitaciones del uso actual de Google Drive

Aunque Google Drive es la herramienta digital más empleada en la organización, su configuración actual no posee la estructura necesaria para operar como un Sistema de Gestión Documental (SGD) que cumpla con los estándares internacionales. Este recurso funciona simplemente como un lugar de almacenamiento sin reglas institucionales para la clasificación, sin un sistema de metadatos, sin control de versiones adecuado y sin mecanismos para la preservación de documentos. La falta de un modelo de carpetas consistente y la ausencia de normativas en la denominación y organización de documentos aumentan el riesgo de cometer errores, perder información o utilizar datos incorrectos. Además, Drive no lleva un registro de los ciclos de revisión, aprobación o auditoría, lo que va en contra de los requerimientos funcionales dictados por la ISO/TS 161752 y complica la obtención de pruebas verificables durante auditorías o reclamaciones.

c. Dependencia de canales informales como medios documentales

La evaluación mostró una alta dependencia de medios informales como

WhatsApp, que se emplea con frecuencia para obtener documentos personales, diagnósticos médicos, imágenes de daños, detalles de pólizas y comunicaciones delicadas entre el cliente, el corredor y las aseguradoras. Este comportamiento da lugar a copias incontroladas en dispositivos personales, pone en riesgo información confidencial y elimina la posibilidad de asegurar trazabilidad, secreto y veracidad. La transferencia de documentos a través de mensajería instantánea infringe los principios de seguridad establecidos en la ISO 27001, especialmente en las áreas que regulan el control de accesos, la gestión segura de los datos y la salvaguarda de la información personal. Además, esta práctica se aparta de las directrices del NIST CSF, ya que no cuenta con procesos formales para identificar, Responder o rastrear incidentes relacionados con documentos.

d. Riesgos operativos, regulatorios y organizacionales

La falta de coordinación y supervisión en los sistemas de documentos provoca riesgos considerables que impactan tanto en la gestión diaria como en el cumplimiento de normativas. La pérdida de archivos, la presencia de expedientes incompletos, el riesgo de trabajar con versiones antiguas y las dificultades para recuperar evidencia afectan de manera directa procesos esenciales como renovaciones, reclamaciones y soporte ante compañías de seguros. Desde una perspectiva regulatoria, la exposición de información personal sensible en canales no supervisados pone a la entidad en una situación vulnerable frente a posibles incidentes de seguridad o exigencias legales. Asimismo, la incapacidad de presentar evidencia documental fidedigna perjudica la credibilidad de la institución y pone en riesgo la confianza de clientes y aseguradoras.

CAPÍTULO V. CONCLUSIONES Y RECOMENDACIONES

Con base a los resultados obtenidos en el capítulo IV mediante la aplicación de los diferentes instrumentos tanto metodológicos y temáticos aplicados a los colaboradores de la correduría Seguro Total, podemos establecer la existencia de la oportunidad de mejorar la gestión actual de los documentos tanto físicos como digitales dentro de la empresa, haciendo un hincapié en el uso de las Normas ISO y el marco NIST de Ciberseguridad como referencia.

5.1 CONCLUSIONES

1. El análisis FODA permitió identificar que la empresa Seguro Total cuenta con una base digital funcional apoyada en herramientas que ofrece Google Workspace (Gmail y Drive), las cuales facilitan la colaboración y el acceso remoto a la información. Sin embargo, dicha estructura carece de control formal, trazabilidad y mecanismos de respaldo, lo que limita su alineación con buenas prácticas internacionales.

   Dicho esto, la organización presenta una estructura flexible y personal comprometido, lo que favorece a la adopción de nuevas tecnologías. Sin embargo, la falta de roles definidos y procesos estandarizados en la gestión documental impiden aprovechar plenamente dichas fortalezas.

   Las principales debilidades se centran en la ausencia de políticas, indicadores de control, capacitación y procesos de seguimiento, mientras que las oportunidades se orientan a la adopción de un sistema de gestión documental certificado. Desde la perspectiva estratégica, el entorno digital ofrece amplias oportunidades para modernizar los procesos internos mediante la adopción de marcos y normas internacionales, lo cual permitiría establecer una gobernanza de la información más segura, eficiente y alineada con los requerimientos regulatorios del sector asegurador hondureño. No obstante, la organización cuenta con fortalezas clave, como la apertura al cambio, el uso cotidiano de herramientas digitales colaborativas y el liderazgo comprometido con la mejora tecnológica, factores que constituyen una base sólida para implementar un sistema documental certificado y sostenible.
   Finalmente, se determina que Seguro Total tiene la capacidad de evolucionar hacia un modelo de gobernanza documental integral, pero requiere establecer una estrategia formal de gestión basada en normas internacionales, integrando procesos de control, seguridad, respaldo y mejora continua que garanticen la integridad, accesibilidad y disponibilidad de la información institucional.

2. El análisis permitió identificar que, aunque Google Drive facilite la colaboración y el acceso a la información, su nivel de madurez tecnológica y cumplimiento normativo es limitado para las exigencias de una gestión documental formal bajo los estándares de ISO 30301:2019, ISO 27001 y el marco de ciberseguridad de la NIST. Los resultados obtenidos mediante los instrumentos y el dashboard reflejan una alta percepción de facilidad de uso y accesibilidad, pero una considerable baja de confianza de seguridad, trazabilidad y control de auditoría, factores esenciales para asegurar la integridad de la información.

   Así mismo, la matriz comparativa y ponderada confirmó que plataformas como M-Files y DocuWare ofrecen mayor robustez funcional, cumplimiento normativo, integrado automatización de flujos, gestión basada en metadatos, cifrado avanzado y auditoría en tiempo real, características que permiten una alineación efectiva con los requisitos de seguridad y gobernanza de datos.

   La empresa Seguro Total se encuentra en una etapa inicial de madurez documental: cuenta con infraestructura digital básica, pero requiere evolucionar hacia una solución que incorpore control, trazabilidad, cumplimiento y resiliencia para garantizar la continuidad del negocio y la protección de la información crítica.

3. Con base a los pilares integrales de una arquitectura empresarial podemos ver un nivel bajo de la correduría, el cual se ha caracterizado o muestra presencia de avance importantes en la digitalización, pero al mismo tiempo se caracteriza por brechas en temas de organización, protección y trazabilidad de la información. Esta falta de estructuras formales, silos de información, falta de colaboración y ausencia de roles definidos afectan directamente a Seguro Total en materia de integridad, autenticidad y disponibilidad las cuales son exigidas por las Normas ISO 15489 e ISO 30301.Asimismo, los riesgos claves identificados como ser la perdida de la información, accesos no autorizados, y falta de actualización nos recalcan la urgencia de fortalecer los mecanismos de control y gobernanza documental.

   El análisis realizado de los procesos, herramientas y percepciones de los colaboradores de Seguro Total nos confirma que la organización depende de prácticas y procesos no estandarizados, lo que es una gran amenaza ya que se están más propensos a errores, inconsistencias y retrasos en actividades críticas del negocio como ser renovaciones, seguimiento de clientes y cumplimiento normativa. La falta también de la integración entre sistemas, falta de políticas de seguridad y la baja automatización limitan a la eficiencia operativa y evidencian que la arquitectura tecnológica actual no es la adecuada para soportar un sistema de gestión documental más robusto. Estas condiciones actuales son un contraste directo frente a los requisitos de seguridad y continuidad de la ISO 27001 y las funciones del

marco NIST, haciendo un énfasis en las funciones de Proteger, Detectar y Responder en donde existen capacidades muy limitadas actualmente.

Finalmente, aunque mediante las respuestas de los directivos se puede ver una visión clara hacia la modernización, lo que se traduce en la transformación digital y un alto deseo de avanzar en la digitalización de los documentos en un umbral del 90%-100% en los próximos años, la infraestructura, procesos y controles actuales requieren de una reestructuración profunda. La implementación de una arquitectura documental eficiente alineadas a las normas ISO le permitirá a Seguro Total consolidar toda la información, reducir riesgos, fortalecer la seguridad y optimizar la operación. Este análisis realizado en el objetivo tres reafirma la necesidad de diseñar una propuesta y directrices que integre la gobernanza, tecnología, procesos y seguridad, buscando la construcción de un sistema resiliente, accesible, sostenible y escalable para la correduría.

4. La empresa Seguros Total presenta un nivel inicial de madurez en materia de seguridad y gestión documental, evidenciando por la ausencia de políticas formales, roles claramente definidos y procedimientos estructurados que garanticen una administración segura y trazable. Los resultados de los instrumentos aplicados confirman que las actividades relacionadas con la gestión documental se desarrollan mayormente de forma manual y descentralizada, sin mecanismos de respaldo o control que aseguren la integridad y disponibilidad de los datos. Esta situación incrementa la vulnerabilidad institucional ante incidentes de pérdida, manipulación o acceso no autorizado.

   Con base en la aplicación del Marco NIST de Ciberseguridad, se identificaron niveles bajos de cumplimiento en las funciones identificar, Detectar, Responder y recuperar. Esto refleja carencias en la identificación de activos, la detección oportuna de incidentes y la preparación para Responder o recuperar la operatividad ante eventos adversos. A diferencia, la función proteger presentó un nivel medio bajo de madurez, sustentando principalmente en las funcionalidades que brinda los servicios de Google donde se muestran controles básicos de seguridad como permisos para accesos o cifrado de tránsito, aunque, aun así, no se cuenta con una configuración institucional formalizada ni respaldo estratégico.

   Los resultados derivados de las listas de verificación de las Normas ISO 15489, 27001 y la 30301 ratifican que las debilidades en la gestión documental y la seguridad de la información están estrechamente interconectadas, ya que falta de políticas, procesos técnicos, capacitación del personal y métricas de seguimiento impiden alcanzar la madurez requerida y deseada. En este contexto, la adopción gradual del Marco NIST de

ciberseguridad representa una estrategia técnica y organizacional viable para la realidad operativa de una MiPyme como la correduría Seguros Total. Su implementación permitirá establecer un sistema integral de gestión documental y seguridad de la información, fortaleciendo la identificación de activos críticos, protección de datos, el monitoreo de eventos y la capacidad de respuesta, así como, la recuperación de incidentes.

5. Mediante la aplicación de la metodología DIRKS en sus etapas A–D, complementada con el análisis desarrollado en los Objetivos 1, 2, 3 y 4, fue posible comprender con mayor claridad el nivel de madurez documental actual de la correduría Seguro Total. Este proceso permitió identificar un conjunto de oportunidades de mejora que resultan fundamentales para fortalecer el ciclo de vida documental y avanzar hacia un modelo más estructurado y eficiente.

   Los resultados evidencian que la correduría presenta un nivel de madurez bajo en relación con los lineamientos establecidos por las normas ISO 15489, ISO 30301 e ISO 27001, así como con las funciones del Marco NIST CSF 2.0. En este contexto, las oportunidades de mejora identificadas se vuelven esenciales para establecer políticas, directrices y normas que sirvan como base para el diseño de un sistema de gestión documental alineado con la metodología DIRKS.

   De forma general, las oportunidades detectadas resaltan la necesidad de avanzar hacia una gestión documental más estructurada, segura y alineada con los estándares internacionales previamente mencionados. Entre los aspectos más relevantes destacan la definición de roles y responsabilidades, el establecimiento de requisitos institucionales y de seguridad, la identificación y definición de estructuras de almacenamiento, así como el fortalecimiento de la colaboración y comunicación entre los equipos. Estos elementos contribuirán a mejorar la eficiencia operativa, la transferencia de conocimiento, la accesibilidad de la información y la capacidad de respuesta ante incidentes o auditorías externas.

   Asimismo, se identificó que la correduría posee una base de conocimiento y reconoce la importancia de la gestión documental para su crecimiento organizacional. Esto facilita la adopción de un nuevo sistema de gestión documental y la implementación de estructuras y lineamientos que permitan una adopción más sostenible y eficiente, generando una ventaja competitiva mediante la optimización de procesos, la reducción de errores y la mejora de la experiencia tanto de colaboradores como de clientes. Las oportunidades detectadas constituyen un insumo esencial para orientar el diseño de la solución propuesta en el Capítulo VI, asegurando que respondan tanto a la realidad operativa de la correduría como a las buenas prácticas internacionales en gobernanza de la información, seguridad y continuidad del negocio.

5.2 RECOMENDACIONES

a) Objetivo 1

- Desarrollar y aprobar una política institucional alineada con la ISO 15489, que define responsabilidad, procedimientos de creación, clasificación, almacenamiento y disposición de información.
- Delimitar formalmente el alcance del sistema de gestión documental, asignando roles y autoridades responsables de su administración. Este paso debe incluir la elaboración de un manual operativo y la definición de indicadores de desempeño.
- Configurar medidas de protección multifactor, cifrado de datos, respaldo periódico y monitoreo de accesos. Además, debe elaborarse un inventario de activos críticos.
- Capacitar al personal en gestión documental y ciberseguridad desarrollando un programa de formación continua enfocándose en el uso adecuado de herramientas digitales, buenas prácticas de seguridad de la información, clasificación de documentos y cumplimiento normativo. Esto fomentará una cultura organizacional basada en la prevención y responsabilidad.
- Adoptar un enfoque de mejora continua realizando auditorías periódicas de cumplimiento respecto a Normas internacionales con el fin de evaluar el desempeño del sistema, identificando brechas y aplicando acciones de corrección oportuna.
- Considerar plataformas que integren automatizaciones de flujos, control de versiones, metadatos y trazabilidad con posibilidades claras de integración con servicios de Google para reducir procesos manuales y aumentar el cumplimiento normativo.

b) Objetivo 2

- Adoptar herramientas de gestión documental certificada, tomando como referencia las arquitecturas de M-Files o DocuWare, que permiten integrar controles de seguridad, automatización de flujos y clasificación por metadatos y registro de auditoría.
- Configurar una política interna de gestión documental y ciberseguridad alineada con las normas ISO 15489, ISO 30301 e ISO 27001, estableciendo responsabilidades, procedimientos de respaldo y control de acceso por niveles de confidencialidad.
- Implementar sesiones de capacitación para el personal, orientadas a mejorar el uso de las funciones avanzadas de las herramientas (búsqueda, control de versiones, permisos, firma digital), reduciendo la dependencia de procesos manuales.
- Diseñar un plan de transición de tecnología actual hacia la nueva de forma gradual que permita migrar de Google Drive hacia un sistema documental más completo,

priorizando interoperabilidad, trazabilidad y seguridad de la información.

- Integrar los lineamientos del marco NIST de ciberseguridad (identificar, Proteger, Detectar, Responder y Recuperar) dentro del sistema propuesto, asegurando una respuesta resiliente ante incidentes y pérdida de datos.
- Se recomienda que Seguro Total evalúe la implementación de un modelo híbrido de gestión documental, que combine las funcionalidades colaborativas y de bajo costo de Google Drive con las capacidades avanzadas de control, trazabilidad y cumplimiento normativo de sistemas especializados como M-Files o DocuWare.

c) Objetivo 3

- Realizar un análisis financiero sobre las posibilidades monetarias existentes que se implemente un nuevo SGD o se mejore la gestión del SGD actual.
- Documentar y estandarizar el flujo completo de gestión documental buscando abarcar puntos como ser la captura, control, acceso, actualización y eliminación de documentos.
- Implementar un esquema o modelo de clasificación de documentos en el cual se incluyan metadatos mínimos obligatorios como ser la fecha de vigencia, código del documento, código del asegurado y aseguradora.
- Mejorar los controles de acceso a la información mediante la implementación de roles y privilegios, uso de autenticación doble, realizar auditoras de revisión, respaldos de la información y cifrado de esta.
- Establecer como objetivo prioritario un ecosistema de aplicaciones que se integren entre sí y así lograr tener un mejor control de los asegurados, facilitar los procesos de renovación, tener datos confiables y mayor eficiencia operativa.
- Establecer un plan de capacitación continua para los colaborades con relación al uso del SGD actual y mejores prácticas de seguridad para prevenir incidentes.

d) Objetivo 4

- Formalizar el inventario de activos documentales y tecnológicos, identificando tipos de información, sus propietarios, niveles de criticidad y ubicaciones. Esta acción permitirá consolidar la función identificar del Marco NIST, facilitar trazabilidad documental y establecer controles de protección adecuados según el activo.
- Incorporar mecanismos de control de acceso, autenticación multifactor y cifrado de datos, mejorando significativamente la seguridad tanto en el uso de la herramienta Google como la eventual incorporación de tecnologías más robustos como ser M-Files o DocuWare, con ellas permitirá operar bajo una estructura jerárquica de permisos,

visibilidad operativa y auditoría de continua.

- Desarrollar un plan formal ante incidentes que defina las responsabilidades, protocolos, tiempos de ejecución y registro de eventos que garantice una reacción oportuna y coordinada ante fallas, brechas o accesos indebidos.
- Establecer procesos automáticos de respaldo y recuperación de información, tanto en entornos cloud como on premise, asegurando que existen validaciones de restauración programadas que respaldan la continuidad operativa del negocio frente a fallas técnicas o ciberataques.
- Capacitar de forma continua al personal en temas de ciberseguridad, gestión documental y protección de datos personales, las responsabilidades y la mejora continua, conforme a las buenas prácticas que pretenden las Normas ISO 27001 y la ley de protección de datos personales.
- Adoptar gradualmente el Marco NIST de Ciberseguridad como guía de gobernanza, priorizando las funciones identificar y proteger en una primera fase y extendiendo posteriormente la aplicación hacia las funciones Detectar, Responder y recuperar consiguiendo una madurez progresiva.

e) Objetivo 5

- Establecer un marco de gobernanza documental, en el cual se definan roles, responsabilidades y autores sobre la información, buscando cumplir con los estándares de las normas ISO, como ser la autenticidad, trazabilidad, fiabilidad de los comentaos y alinearse a la función de Gobernar del NIST.
- Estandarizar los procesos de creación, almacenamiento/clasificación, acceso, uso, versionamiento y eliminación de documentos, en donde se incorporen lineamientos formales que garanticen la autenticidad, integridad, confiabilidad y disponibilidad conforme a los principios base de la norma ISO 15489.
- Fortalecer las políticas de seguridad de la información, mediante la implementación de controles como ser la autenticación multifactor, gestión de acceso mediante privilegios, monitoreo de incidentes o brechas de seguridad y procedimientos de respaldo y recuperación de la información base a los requerimientos de la norma ISO 27001.
- Consolidar mediante el uso correcto de un SGD, en donde se reduzcan los silos de información, para mejorar la eficiencia operativa, comunicación entre áreas, búsqueda de información y mantener la información actualizada.
- Invertir en desarrollar programas de capacitación continua y en la cultura organizacional

en gestión documental y la seguridad de la información, en donde se busque garantizar que los colaboradores y directivos tengan las competencias necesarias para gestionar el SGD y asegurar la continuidad del negocio.

CAPÍTULO VI. APLICABILIDAD

6.1 PROPUESTA DE ESTRATEGIA DE FORTALECIMIENTO DE LA GESTIÓN DOCUMENTAL Y LA PROTECCIÓN DE LA INFORMACIÓN EN LA EMPRESA SEGURO TOTAL.

El presente capítulo detalla la propuesta de una estrategia de fortalecimiento de la gestión documental y la protección de la información basado en las capacidades y necesidades actuales de la Correduría Seguros total, dejando un mapa de ruta de una futura implementación del sistema brindando información sólida y puntual de la aplicabilidad de dicha mejora. Esta propuesta se basa en la metodología DIRKS.

6.2 JUSTIFICACIÓN DE LA PROPUESTA

El estudio llevado a cabo en los objetivos del uno al cuatro hizo posible reconocer varios descubrimientos que muestran la urgencia de implementar un plan global para mejorar la gestión de documentos y salvaguardar la información en la correduría Seguros Total. Aunque estos descubrimientos tratan aspectos diferentes, todos concluyen: la organización no posee un modelo desarrollado, confiable y uniforme para manejar su información sensible.

En el objetivo 1, el diagnóstico de la problemática actual nos muestra una fuerte dependencia de procesos manuales y documentos físicos, así como la ausencia de controles formales, trazabilidad y criterios homogéneos para el manejo de la información. Esta situación incrementa el riesgo de pérdida, duplicidad, acceso no autorizado y dificulta la toma de decisiones adecuada afectando directamente a la eficiencia operativa de la correduría. De igual manera, el objetivo evidencio que, aunque existe una oferta variada de herramientas de gestión documental, no todas responden adecuadamente a las necesidades específicas de la correduría. El análisis de estas soluciones permitió identificar brechas entre las capacidades ofrecidas por las plataformas y las practicas actuales de la organización, resaltando la importancia de seleccionar una herramienta que apoye procesos estandarizados y seguros.

El objetivo 3 verificar la arquitectura sobre la cual se sustenta la gestión documental, identificando un nivel de madurez considerablemente bajo en pilares como información, negocios y las aplicaciones actuales. La falta de procesos es evidente, así como la utilización limitada y poco controlada de herramientas digitales como correo y almacenamiento en la nube, así como la carencia de roles y responsabilidades claramente establecidos, confirman que la

organización no cuenta con una arquitectura alineada con buenas prácticas de gestión documental.

En su defecto, el objetivo 4 basado en el enfoque del marco NIST de ciberseguridad, permitió identificar brechas muy relevantes en funciones clave asociadas a la protección de la información, tales como la identificación de activos de información, implementación de medidas de protección, detección de incidentes y capacidades de respuesta y recuperación. Estas brechas evidencian que la organización se encuentra expuesta a riesgos operativos y alcanzan dimensiones normativas y reputacionales, especialmente considerando la sensibilidad de los datos que gestiona.

Finalmente, el objetivo 5 identifica oportunidades de mejora que servirían como guía para el fortalecimiento progresivo del sistema en el capítulo 6, sin embargo, debido a su carácter prospectivo, dichas oportunidades no constituyen hallazgos significativos y por ello no forma una parte fundamental para la justificación.

En resumen, los resultados de estos cuatro objetivos sustentan la urgencia de desarrollar, en el Capítulo 6, un plan de fortalecimiento que combine procesos estandarizados, tecnologías pertinentes y medidas de seguridad que se ajusten a normas como ISO 15489-1:2016 e ISO/IEC 27001:2022, además de los lineamientos del marco NIST. La meta del plan es disminuir los peligros relacionados con la gestión de la información, aumentar la trazabilidad y la supervisión de documentos y fomentar un sistema de gestión más eficaz, seguro y que cumpla con la legislación actual en Honduras.

6.3 ALCANCE

La estrategia que se pretende realizar se enfoca en el diseño conceptual y metodológico de un sistema digital de gestión documental para la empresa Seguro Total, orientado a fortalecer la gobernanza de la información y los datos con base a las siguientes etapas de la metodología DIRKS.

Las Etapas G y H que comprende la implementación y revisión posterior del sistema documental no entran dentro del desarrollo de la propuesta, debido a que la misma solo comprende el diseño y estrategias para que la correduría pueda implementar posteriormente un SGD

En este alcance del estudio se busca comprender la identificación de los procesos críticos de la gestión documental, el análisis de riesgo asociados al manejo de la información actual y una mejora asociada a los lineamientos estratégicos para mejorar la eficiencia,

trazabilidad y seguridad de los documentos tanto físicos como digitales. Considerando los procesos y las necesidades, se recurre a la integración de los marcos normativos internacionales como la ISO 15489, ISO 30301, 27001 y el marco de ciberseguridad NIST adaptados a las necesidades de las MiPymes Seguro Total.

6.3.1 OBJETIVOS DE LA PROPUESTA

6.3.1.1 OBJETIVO GENERAL

Diseñar una estrategia que permita fortalecer la gobernanza documental y la protección de los datos en la MiPymes Seguro Total, integrando las normas ISO 15489, ISO 30301, ISO 27001 y el Marco NIST, para garantizar la eficiencia operativa, el cumplimiento normativo y la resiliencia organizacional.

6.3.1.2 OBJETIVOS ESPECÍFICOS

1. Elaborar la Etapa E de la metodología DIRKS basado en la ISO 30301:2019 e integrado con controles de seguridad de la ISO 27001:2022 y las funciones del Marco NIST de Ciberseguridad.
2. Elaborar la Etapa F de la metodología DIRKS basado en la ISO 30301:2019 e integrado con controles de seguridad de la ISO 27001:2022 y las funciones del Marco NIST de Ciberseguridad.
3. Ejemplificar indicadores clave de desempeño (KPIs) que permitan evaluar y monitorear la eficiencia, trazabilidad y seguridad de la gestión documental dentro de la organización.
4. Definir políticas y estrategias que fortalezcan la protección de la información, la gobernanza documental y la continuidad del negocio en la MiPyme Seguro Total.

6.4 RELACIÓN DE HALLAZGOS Y PROPUESTAS DE ESTRATEGIAS

La relación de hallazgos es clave para la formulación de la estrategia de gestión documental y protección de datos para la corredura Seguros Total. Los resultados obtenidos mediante los instrumentos aplicados evidencian brechas significativas en materia operativa, tecnológica, normativa y de seguridad. Estas brechas se transforman en oportunidades de mejora, que orientan la construcción de un modelo documental sólido, estandarizado y alineado con la misión de la empresa.

6.4.1 DEL DIAGNÓSTICO A LA PROPUESTA: APORTES DEL OBJETIVO 1 AL MODELO PLANTEADO

Hallazgos clave:

Considerando el bajo nivel de aplicación práctica de estándares internacionales como Normas ISO, ausencia de roles, gestión documental empírica, falta de coordinación, controles insuficientes, carencia de políticas, limitada continuidad, nula capacitación formal.

6.4.1.1 ESTRATEGIA DE MITIGACIÓN Y MEJORA

- Crear y aprobar la política institucional de gestión documental y seguridad de la información alineada a ISO 15489, ISO 27001 e ISO 30301
- Definición de roles y responsabilidades integrándolos en base a los permisos dinámicos que ofrece M-Files.
- Unificar la gestión documental en un repositorio institucional basado en M-Files, eliminando la dispersión actual en carpetas sin control
- Implementar flujos de trabajo estandarizados, para creación, revisión, aprobación, archivo y retención.
- Establecer controles de acceso, verificación multifactor y clasificación mediante niveles de confidencialidad, fortaleciendo la seguridad documental y cibernética.
- Implementación de un plan de continuidad del negocio y su documentación con respaldos, restauración y control de versionamiento.

6.4.2 DEL DIAGNÓSTICO A LA PROPUESTA: APORTES DEL OBJETIVO 2 AL MODELO PLANTEADO

Hallazgo clave:

Alta aceptación del uso de Google Drive, pero limitaciones en auditoría y trazabilidad, control de versiones y seguridad, así como, problemas con digitalizaciones y dificultades de acceso.

6.4.2.1 ESTRATEGIA DE MITIGACIÓN Y MEJORA

- Adoptar un modelo híbrido M-Files y Google Workspace, donde M-files sea el eje y sistema principal y Drive una herramienta colaborativa
- Configurar metadatos obligatorios para mejorar clasificación, recuperación y controles normativos
- Habilitación de mecanicismo de auditoría que permite M-Files que garanticen una trazabilidad completa
- Diseño de plantillas personalizadas y normalizadas para aquellos trámites que requieran donde vaya ligada directamente a metadatos y mejor control operativo

- Optimizar el proceso de digitalización integrando OCR y flujo directos hacia M-Files
- Implementación de sistemas de búsqueda basada en metadatos, reduciendo la dificultad de acceso a documentos

6.4.3 DEL DIAGNÓSTICO A LA PROPUESTA: APORTES DEL OBJETIVO 3 AL MODELO PLANTEADO

Hallazgo Clave:

Bajo nivel de madurez en los pilares de arquitectura con procesos no estandarizados, información dispersa sin controles, herramientas no integradas y una infraestructura limitada que impide trazabilidad, seguridad y continuidad operativa.

6.4.3.1 ESTRATEGIA DE MITIGACIÓN Y MEJORA

- Implementar un modelo arquitectónico hibrido donde M-files actúe como repositorio oficial y núcleo de gobernanza documental
- Estandarizar procesos documentales mediante flujos automatizados en M-files, reduciendo la dependencia del criterio individual y garantizando consistencia operativa en toda la correduría.
- Integrar M-Files con las aplicaciones existente para consolidar información actualmente dispersa, mejorar la eficiencia y asegurar una única fuente de verdad
- Configurar metadatos obligatorios para todos los documentos lo que permite clasificación automática, búsquedas inteligentes, trazabilidad y alineación con los pilares de información y negocio
- Fortalecer la infraestructura tecnológica integrando mecanismos de respaldo, recuperación, continuidad operativa y monitoreo apoyándose en capacidades de M-files

6.4.4 DEL DIAGNÓSTICO A LA PROPUESTA: APORTES DEL OBJETIVO 4 AL MODELO PLANTEADO

Hallazgo Clave:

Mínimo nivel de madurez en funciones Identificar, Detectar, Responder y Recuperar. Inexistencia de inventario, de evaluaciones de riesgos, uso empírico de Google Workspace, ausencia de validación multifactor, falta de monitoreo y registro, desconocimiento de protocolos para respaldo y recuperación de información.

6.4.4.1 ESTRATEGIA DE MITIGACIÓN Y MEJORA

Tabla 55: Oportunidades de mejora conforme al Marco NIST

Función NIST	Oportunidad de mejora Identificada	Descripción de problemáticas resolver
Identificar	• Crear un inventario de activos documentales y tecnológicos • Clasificar documentos por niveles de sensibilidad y metadatos • Definir roles y responsabilidades documentales	• Actualmente no existe un registro formal de información, documentos ni dispositivos. Esto impide conocer criticidad de documentos y procesos, propietarios y el riesgo • Falta de clasificación limita controles de acceso, trazabilidad y cumplimiento de ISO 15489 e ISO 27001 • No hay responsables para crear, actualizar o custodiar información.
Proteger	• Implementación de validación multifactor para cada cuenta organizacional • Configuración de permisos por roles • Capacitación de personal sobre seguridad de información y buenas prácticas • Aplicar políticas de retención y control de versiones	• El acceso Google Workspace, correo y plataformas se hace solo por contraseñas, generando riesgo de intrusión • Las carpetas se comparten sin criterios normativos, lo que expone documentos sensibles • No existen líneas de versiones ni ciclos de vida de un documento
Detectar	• Activar auditoría automatizada y registro de eventos • Establecer alertas tempranas ante anomalías o intentos de acceso indebido • Implementar revisiones periódicas de logs y actividad documental	• No hay monitoreo de accesos ni de modificaciones o cualquier actividad • La empresa no cuenta con herramientas de detección de actividades sospechosas o irregularidades • No existen mecanismos de supervisión
Responder	• Crear un procedimiento formal de respuesta a incidentes	• El personal desconoce a quien reporta o qué hacer ante un incidente • No existen rutas de comunicación internas ante una emergencia documental o de acceso indebido

Función NIST	Oportunidad de mejora Identificada	Descripción de problemáticas resolver
	• Definir canales de comunicación y responsable de atención • Implementar un flujo automatizado de reporte de incidentes que proporciona M-Files	• El proceso es totalmente manual y reactivo
Recuperar	• Establecer un plan de recuperación documental • Realizar respaldos automatizados y pruebas de recuperación • Mantener historial de versiones y evidencia de recuperación y respaldos	• No se cuenta con protocolos para restaurar información ante pérdida o incidente • La empresa depende del comportamiento de Google Drive y no realizan respaldo automatizados

Nota: Elaborado por autores

6.5 DESCRIPCIÓN Y DESARROLLO A DETALLE DE LA PROPUESTA

El desarrollo de esta propuesta se basa en las etapas E y F de la metodología DIRKS como se describe anteriormente en el Alcance y objetivos específicos de la propuesta, en este caso por cada Etapa se mostrarán sus puntos estratégicos para cumplir con los descrito por la metodología.

6.5.1 DESARROLLO DE LA ETAPA E IDENTIFICACIÓN DE LAS ESTRATEGIAS PARA CUMPLIR CON LOS REQUISITOS

La metodología DIRKS ofrece un enfoque sistemático para diseñar, implementar y evaluar sistemas de gestión documental alineados a estándares internacionales como ISO 15489 e ISO 30301.

La etapa E consiste en la identificación de estrategias organizacionales, normativas, tecnológicas y operativas necesarias para cumplir los requisitos documentales detectados en el diagnóstico previo (Objetivo 1-4). Esta etapa funciona como un puente entre los hallazgos encontrados previamente y la propuesta final del sistema, integrando controles de seguridad, políticas de retención, diseños de flujos, requisitos regulatorios y criterios de mejora continua.

6.5.1.1 POLÍTICAS

La formulación de políticas institucionales constituye el pilar fundamental para el diseño del sistema de gestión documental: Estas políticas establecen el marco normativo interno

que guiara a la creación, organización, protección, uso y disposición de los documentos, asegurando que las prácticas operativas se alineen con los estándares internacionales mencionado y que responden a las debilidades identificadas durante el diagnostico.

Las políticas definen los principios rectores de la gobernanza documental, garantizando que toda la información generada por la organización sea gestionada bajo criterios de autenticidad, integridad, confiabilidad, disponibilidad y trazabilidad, conforme a lo estipulado en ISO 15489. Estos principios aseguran que los documentos mantengan su valor probatorio y su relevancia para soportar decisiones operativas, administrativas y legales. Se establecen los lineamientos para el control de acceso, autenticación y privacidad, fundamentados en los requisitos de seguridad de la información descritos por ISO 27001 y por la función "Proteger" del marco NIST de ciberseguridad. Esto incluye políticas como:

- Autenticación en múltiples factores
- Perfiles y roles diferenciados según nivel de confidencialidad
- Restricciones de permisos para edición, descarga y eliminación de documentos.
- Criterios para el uso seguro de dispositivos personales y corporativos

Un componente critico de esta fase es la definición de políticas de retención y disposición documental, alineadas con los lineamientos de la ISO 30301, que instruyen sobre los periodos de conversación, la clasificación por tipos documentales y los procedimientos para transferencia de archivos o eliminación segura. Estas políticas permiten estandarizar el ciclo de vida de los documentos evitando acumulaciones innecesarias, perdidas de información duplicidades, problemas que actualmente afectan de manera recurrente a Seguro total.

Del mismo modo, se formalizan los roles y responsabilidades asociados a la creación, almacenamiento, auditoria y custodia de la información, Subsanando una de las debilidades más evidentes identificadas: La ausencia de responsables formales de la gestión documental y de la seguridad de la información, bajo nueva política se proponen responsabilidades concretas para:

- Propietarios de procesos
- Administradores del repositorio documental
- Responsables de seguridad de la información
- Usuarios finales y su deber de cumplimiento
- Personal encargado de digitalización, control de versiones y auditorias

Estas políticas responden de forma directa y estructuradas a los hallazgos diagnosticados. La falta de controles de acceso, inexistencia de trazabilidad documental en Google Drive, ausencia de procedimientos formales y el uso empírico de herramientas tecnológicos. Al concretarse un marco normativo adecuado y sólido, la correduría seguros total establecería las bases para un sistema documental seguro y estandarizado.

6.5.1.2 NORMAS

Con base a los requisitos identificados en las etapas previas de la metodología DRIKS, es necesarios establecer un conjunto de elementos normativos y organizaciones dentro de la correduría que funcionen como fundamento del futuro SGD. Estos componentes permitirán garantizar la uniformidad, control, seguridad y monitoreo del ciclo completo de vida de los documentos e información, asegurando cumplir con los lineamientos establecidos por las normas internacionales ISO y el Marco NIST de Ciberseguridad. A continuación, se presentan aquellos elementos base que serán definidos para asegurar el funcionamiento eficiente y sostenible del sistema.

1. Lineamientos para nombramiento y metadatos de los documentos
2. Estructura institucional de carpetas
3. Controles mínimos establecidos por las Normas ISO 15489,30301,27001
4. Definición de roles y responsabilidades documentales

6.5.1.3 MODELO DE ADOPCIÓN

La estrategia propuesta para la correduría Seguros Total se centra en la construcción de un sistema digital de gestión documental bajo un enfoque híbrido combinando Google Workspace bajo el entorno colaborativo y M-Files como plataforma principal que trata de controlar la metadata, trazabilidad y seguridad. Esta combinación permite a la MiPyme elevar su madurez documental sin abandonar sus herramientas actuales, optimizando costos y facilitando la transición tecnológica.

La propuesta se fundamenta en cuatro ejes:

1. **Principios de gestión documental (ISO 15489)**
    a. Autenticidad y confiabilidad del documento
    b. Trazabilidad durante todo su ciclo de vida
    c. Clasificación y metadatos estructurados
    d. Disponibilidad y accesibilidad controlada

2. **Principios de gobernanza documental (ISO 30301)**
    a. Roles claros
    b. Procesos definidos y medibles
    c. Infraestructura documental estandarizada
    d. Reglas de retención y disposición
3. **Principios de seguridad de la información (ISO 27001)**
    a. Control de accesos por rol
    b. Cifrado en reposos y tránsito
    c. Gestión de incidentes
    d. Copias de respaldo y recuperación
4. **Funciones del Marco NIST**
    a. Identificar: Inventario documental, riesgos, criticidad
    b. Proteger: Verificación multifactor, permisos, cifrados y automatización de procesos de protección
    c. Detectar: Auditorías, logs, alertas de cambios
    d. Responder: Flujos de aprobación, escalamiento y registro de respuesta ante incidentes
    e. Recuperar: Respaldos y recuperación de versiones automatizados

6.6.1 DESARROLLO DE LA ETAPA F IDENTIFICACIÓN DE LAS ESTRATEGIAS PARA CUMPLIR CON LOS REQUISITOS

6.6.1.1 ARQUITECTURA CONCEPTUAL DEL SISTEMA PROPUESTO

La arquitectura conceptual describe la organización lógica de los componentes y cómo estos interactúan entre sí para gestionar el ciclo de la vida completo de los documentos. En el centro del modelo se encuentra un repositorio documental gobernado por metadatos, administrado en base a las funciones de M-Files. Dicho repositorio será la fuente de verdad institucional; todos los documentos que ingresan pasarán por procesos de clasificación, validación, versionamiento y trazabilidad

Considerando esto, alrededor del repositorio operan distintos módulos funcionales:

- Capa de captura de información donde se incluyen las fuentes de recepción de documento como correo electrónico, digitalización mediante escáner y carga manual al aplicativo (M-Files y Drive)
- Capa de procesamiento que incorpora el OCR, identificación automática del tipo de documento, vinculación con plantillas y validaciones.

- Capa de clasificación donde el sistema asigna metadatos obligatorios según las reglas definidas por el negocio (tipo de documento, confidencialidad, cliente, numero de póliza, área)
- Capa de operación, donde los usuarios realizarán consultas y aprobarán documentos participando en flujos mediante los roles ya predefinidos
- Capa de gobernanza donde se gestionan las auditorías, roles, permisos y políticas de seguridad documental y de información

6.6.1.2 ARQUITECTURA TECNOLÓGICA HÍBRIDA (M-FILES Y GOOGLE WORKSPACE)

La estrategia se basa en aprovechar las fortalezas existentes que ofrece los servicios de Google a la organización y complementarlas con las ventajas competitivas que ofrece M-Files brindando robustez en áreas donde Google Drive resulta ciertamente limitado:

- Trazabilidad
- Auditoría
- Retención
- Controles de seguridad
- Metadatos estructurados y automatizaciones

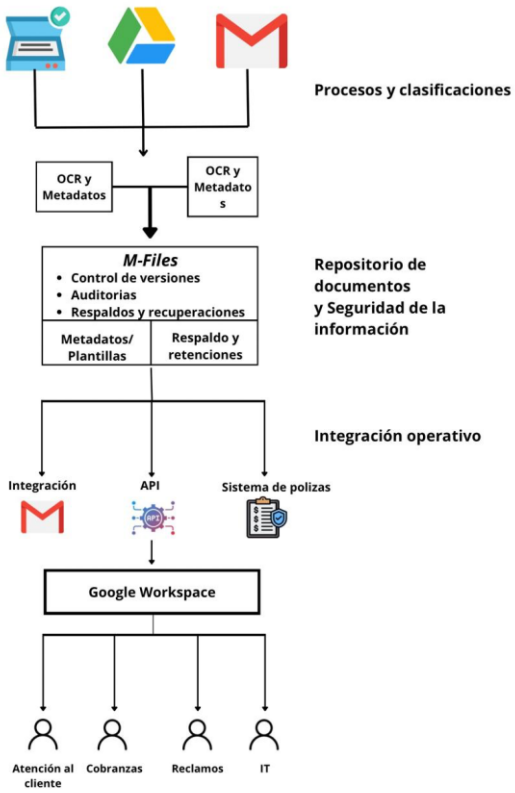
Google Workspace se mantiene como la herramienta principal de comunicación y manejo básico y cotidiano de archivos dado que su bajo costo y lo familiarizado que está con el personal lo hace sumamente indispensable.

M-Files por su parte se integra como:

- Repositorio documental oficial y primario
- El sistema de metadatos y clasificación optimizado
- Motor principal de automatizaciones
- Plataforma de auditoría y seguridad de la información

Con la integración de ambos servicios no solo lograremos un mejor flujo de trabajo, sino una estructura más robusta y adecuada, alineada a las normas ISO y el marco NIST de ciberseguridad permitiendo una interoperabilidad amplia donde se podrán guardar documentos de Gmail hacia M-Files, edición de documentos con controles de versiones, respaldos sincronizados con copias en Drive y automatizaciones de flujos de aprobación y protección de archivos.

Figura 44: Arquitectura Empresarial Propuesta Seguro Total

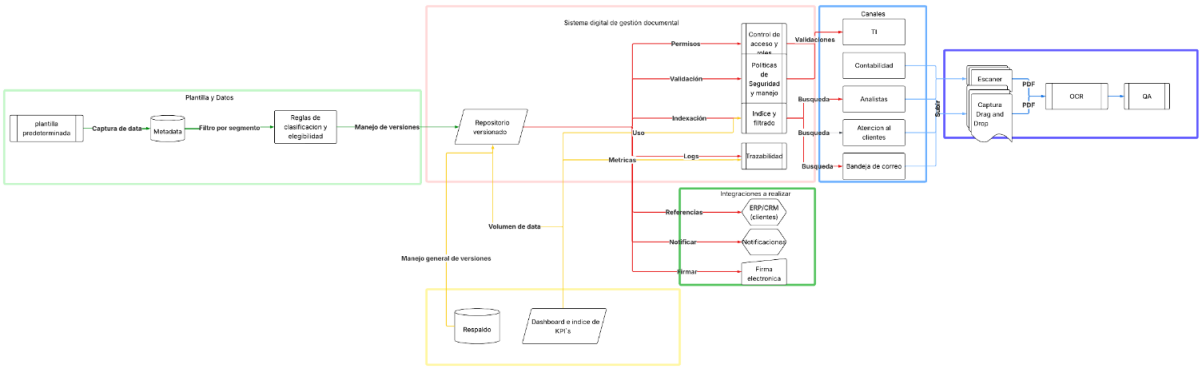


Nota: Elaborada por los autores

La arquitectura propuesta consolida en un solo ecosistema todas las funciones esenciales del ciclo de vida documental. Los documentos ingresan desde diversas fuentes operativas y son sometidos a un tratamiento inicial que incluye reconocimiento óptico de caracteres, asignación automática de metadatos, este preprocesamiento garantiza estandarizados, integridad y calidad antes de que los documentos pasen al repositorio central que proporciona M-Files.

Dentro de M-Files el sistema actúa como un núcleo de gobernanza documental, proporcionando capacidades avanzadas de control de versiones, auditoria continua, aplicación de política de retenciones y mecanismos automatizados, con ello constituye la capa forma que asegura cumplimiento normativo, trazabilidad completa y protección frente a alteraciones o perdidas de información. La arquitectura incorpora además una capa de integración mediante API, que permite la conexión directa con Google Workspace y sistema de pólizas utilizado actualmente por la correduría, esto facilitara gradualmente a las áreas funcionales que accedan a información desde sus propios entornos de trabajo, manteniendo al mismo tiempo controles estrictos de permisos, roles y registro de actividad. En líneas generales, este diseño establecerá un flujo documental optimo y seguro, plenamente alineado con los principios de las normas ISO y el marco NIST y garantizando una operación más eficiente, coherente y resiliente.

Figura 45: Arquitectura Tecnológica del Sistema Digital de Gestión Documental



Nota: Elaborada por los auto

Conforme a la figura anterior de arquitectura propuesta para el sistema de gestión documental constituye un eje central de la estrategia de modernización documental y de seguridad de la información para la empresa Seguro Total. Su diseño responde directamente a las necesidades identificadas en los hallazgos previos, así como los requisitos establecidos mediante la necesidad de aplicar las Normas ISO 15489, ISO 27001 e ISO 30301 así como, el marco de ciberseguridad NIST, con la inclusión de estos marcos se garantiza una solución integral que no solo automatizan procesos, sino que formaliza la gobernanza documental de acuerdo con estándares internacionales.

La arquitectura se sostendrá mediante 5 capas:

1. **Capa de captura y digitalización**

La primera sección corresponde a los mecanismos mediante los cuales la información ingresa al sistema y aquí se ubican factores como:

- Digitalización vía escáner
- Carga manual de archivos
- Importación desde correos electrónicos
- Carpetas sincronizadas

Con ello se soluciona problemáticas actuales como inconsistencias en la calidad de los documentos, pérdida de información por digitalizaciones mal realizadas o duplicadas y falta de control de trazabilidad del ciclo del documento. Con la incorporación de un OCR automatiza la identificación del contenido y posibilitar procesos avanzados de clasificación, lo que reduce la carga operativa sobre el usuario y disminuye errores humanos. En base a la alineación con la norma ISO 15489 esta capa asegura la calidad de la documentación y su ingreso a la plataforma con índices mínimos de calidad, integridad y autenticidad.

2. Capa de clasificación de metadatos y reglas de negocio

Esta es la pieza clave del modelo, donde su fortaleza radica en el uso de M-Files como motor de gobernanza documental. A diferencia del sistema actual, donde los documentos se clasifican manualmente y sin criterios uniformes, esta capa permite:

- Asignación automática de metadatos obligatorios
- Aplicación de reglas de negocio
- Asignación de plantillas documentales
- Activación de flujo
- Validación de completitud

El uso de metadatos es un requisito fundamental para cumplir con ISO 30301 ya que permite estructurar el sistema de gestión documental y con ISO 15489 que exige controles sobre seguridad, autenticidad, confiabilidad e integridad.

3. Capa de repositorio y control de versiones

El repositorio documental gobernado es el corazón del sistema digital de gestión documental donde se garantizarán factores como almacenamiento estructurado, controles de versiones automatizados, auditoría completa por cada acción, permiso basado en roles y usuarios o cifrado en reposo.

En comparación con el estado actual esta capa transforma radicalmente el control institucional sobre la información. Este repositorio será compatible:

- Función Proteger
- Función Detectar
- Función Recuperar
- ISO 27001
- ISO 15489

4. Capa de integración operativa

La arquitectura considera la integración del sistema digital de gestión documental con las herramientas operativas de la MiPyme permitiendo factores como la conexión con módulos ERP, flujos de intercambio de información con demás sistemas del negocio, aprobación de documentos desde bandejas de correo, firma electrónica y más. Esta capa garantiza que la gestión documental sea un proceso propio de la organización siendo parte fundamental de la misma.

Con dicha integración posibilitará la automatización de trámites como:

- Aprobación de póliza

- Respaldo de contratos
- Vinculación de reclamos por póliza
- Expedientes digitales por cliente

5. Capa de seguridad, auditoría y continuidad

Es la capa más crítica en términos de cumplimiento normativo y resiliencia operativa ya que incluye factores como autenticación multifactor, políticas de retención, monitoreo y logs, verificación por acciones indebidas o anomalías, así como, respaldo automático y recuperación ante incidentes.

Con esta capa se solucionan hallazgos críticos identificados en el Objetivo 4 del capítulo IV específicamente en:

- Ausencia de controles de acceso
- Falta de trazabilidad
- Inexistencia de procesos de recuperación de información
- Deficiencias de seguridad informática

Alineadas con las ISO 27001 y el marco de ciberseguridad de NIST brindará una mejora sustentable y considerable a las necesidades que tiene la correduría Seguros Total.

6.6.1.3 MODELO DE PROCESOS TO-BE

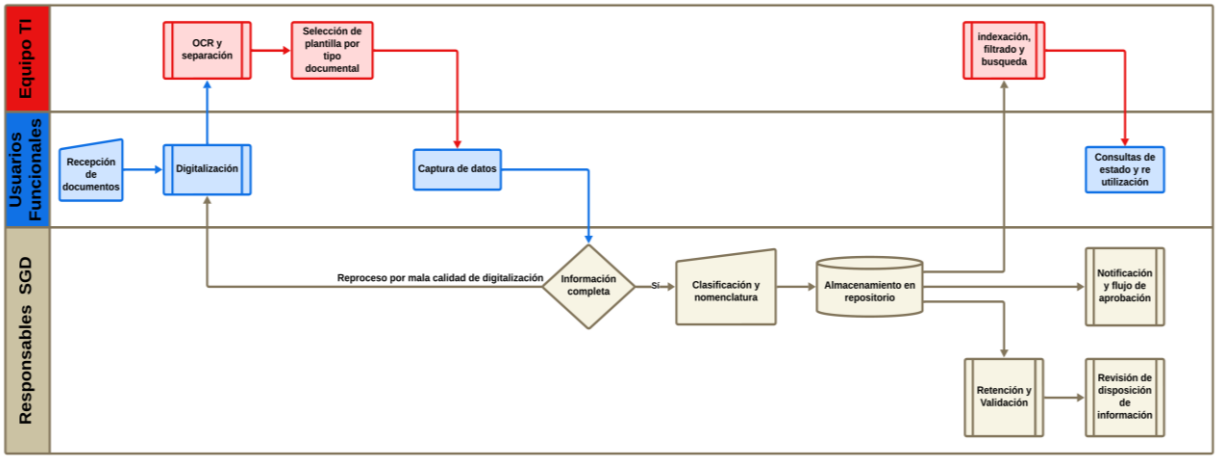
El proceso TO-BE representará la forma idealizada y optimizada en la que la empresa gestiona sus documentos una vez que se implemente el sistema digital de gestión documental. A diferencia del modelo actual, los procesos se estructuran para eliminar reprocesos donde se garantiza la calidad, asegura trazabilidad y cumplimiento de los requisitos normativos.

El modelo de procesos se basa en factores como:

- Recepción y digitalización donde todos los documentos ingresan mediante un punto único de captura. Los documentos digitales se cargan mediante la bandeja de entrada, Drive o Gmail
- Procesamiento OCR donde el documento pasa por el OCR y se identifican tipo, estructura, clasificación y contenido relevante
- La aplicación de plantillas y metadatos donde el sistema asigna automáticamente metadatos obligatorios, lo que permite orden, búsqueda y trazabilidad
- Controles de calidad donde el documento se mide mediante una serie de validación obligatorias que garanticen profundamente la calidad y legibilidad, de lo contrario, el documento se devuelve automáticamente al usuario

- La clasificación y almacenamiento donde el documento se ingresa al repositorio versionado, lo que garantiza integridad y control
- Indexación y recuperación donde los usuarios pueden encontrar documentos por contenido, metadatos, cliente, póliza y fecha
- Flujos de aprobación donde los documentos eran calificados mediante parámetros o factores para verificar la calidad y que puedan enviarse a los responsables
- Retención según políticas basadas en la Norma ISO 15489 y 30301, el sistema determina que documentos conservar, transferir o eliminar.

Figura 46: Modelo de procesos TO-BE



Nota: Elaborado por autores

El flujo representa la transición hacia un ciclo de vida documental completamente estructurado, automatizado y conforme a los estándares internacionales de gestión y seguridad de la información. Cada etapa del proceso está diseñada para asegurar la integridad, autenticidad, disponibilidad y trazabilidad del documento desde su origen hasta su disposición final alineándose con los requisitos de la ISO 15489, ISO 30301 y la ISO 27001.

El proceso inicia con un punto único de entrada que centraliza la recepción de documentos físicos y digitales donde serán sometidos a OCR y preparados para su clasificación. A diferencia del modelo actual donde eliminara procesos y garantizara uniformidad desde la primera etapa.

El sistema incorpora una fase de validación y control de calidad que verifica automáticamente la legibilidad del documento, la coherencia de los metadatos y el cumplimiento de las plantillas definidas; Solo los documentos que cumplen con los criterios

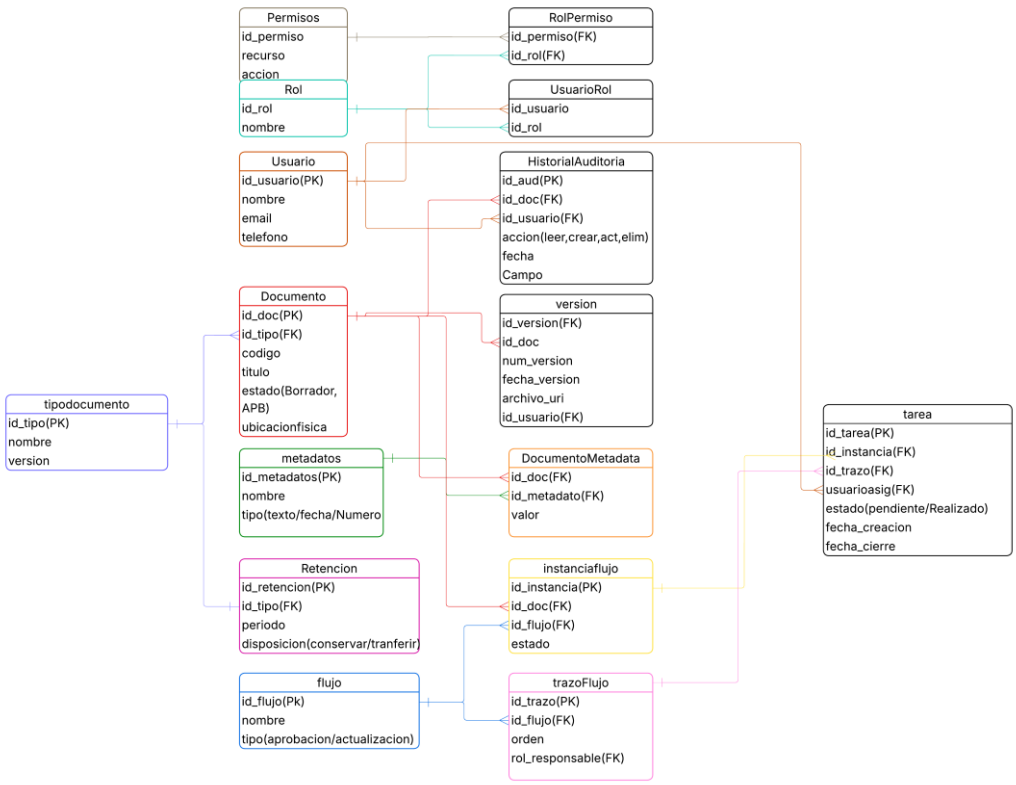
avanzan. Posteriormente mediante clasificación inteligente, el sistema asigna metadatos, nivel de acceso, ubicación y ciclo de retención. Este proceso incluye también flujos de aprobación automatizados, que registran actividad, notifican a los responsables y evitan retrasos operativos. Finalmente, el ciclo culmina con la aplicación de políticas de retención y disposición que determinan la conservación, transferencia o eliminación segura del documento.

6.6.1.4 MODELO LOGICO DE INFORMACIÓN

El esquema de entidad-relación (ER) muestra de forma organizada los elementos clave del sistema digital propuesto para la gestión de documentos y la manera en que se conectan para asegurar un manejo completo del ciclo de vida de los archivos. Cada entidad dentro de este modelo tiene un papel particular en el entorno de gestión de documentos, mientras que las conexiones entre ellas garantizan la trazabilidad, seguridad, autenticidad y cumplimiento de normativas, de acuerdo con las directrices de la ISO 15489, ISO 30301 e ISO/IEC 27001.

De manera general, el diagrama de ER permite observar cómo se administran los documentos a través del uso de metadatos, controles de acceso, registros de auditoría, versiones y políticas de retención, estableciendo una base robusta que apoya la gestión digital de la información.

Figura 47: Modelo Entidad-Relación



Nota:

Elaborado por autores

En este modelo, el Documento es el elemento central del sistema, ya que todos los procesos, usuarios y controles giran en torno a él. Cada documento tiene que ir acompañado de información adicional, una versión actual, un propietario, un registro de auditoría y un flujo de trabajo que marque su movimiento dentro del sistema. Esta organización previene la existencia de documentos sin un contexto claro, mejora la capacidad de seguimiento y facilita la gestión eficiente de su ciclo de vida.

La entidad de Metadatos desempeña un papel clave en la gestión de documentos. A través de ella se definen aspectos tales como categoría, tipo, proceso, fecha, nivel de confidencialidad y área responsable. Estos componentes permiten clasificar, localizar y auditar los documentos de manera coherente, asegurando que se mantenga la estandarización y se cumplan con los requisitos organizativos y de control que establecen las normas ISO.

La entidad Versión garantiza que los documentos sean auténticos y se mantengan intactos, ya que anota cada cambio efectuado, señalando el autor, la fecha y la razón. Este sistema permite mostrar cómo ha cambiado el documento, evitar modificaciones no autorizadas y recuperar versiones anteriores, aspectos fundamentales para las auditorías tanto internas como externas.

La parte de seguridad del sistema está compuesta por las entidades Usuario, Rol y Permiso, que regulan quién tiene la autorización para ver, modificar, aprobar, eliminar o auditar un documento. Este enfoque de permisos detallado sigue el principio de mínimo privilegio, tal como lo sugieren ISO 27001 y el marco NIST, lo que reduce los riesgos de accesos no autorizados y mejora la protección de la información.

La entidad Auditoría anota de manera automática todas las actividades llevadas a cabo sobre los documentos, formándose así un elemento clave para asegurar la transparencia y la trazabilidad normativa. Estos registros son cruciales para evidenciar el cumplimiento, investigar acontecimientos y fundamentar las decisiones institucionales.

El sistema también incluye la entidad Flujo, que simboliza los procedimientos de revisión y aprobación requeridos para cada documento. Este elemento automatiza tareas, establece quienes son los encargados y asegura que el documento pase por fases formales y comprobables, mejorando la eficiencia y estandarización de los procesos operativos. Por último, la entidad Retención establece los plazos y requisitos para la conservación, transferencia al archivo histórico o eliminación de los documentos. Su inclusión permite llevar a cabo un ciclo de vida documental integral y conforme a las obligaciones legales y reglamentarias actuales.

6.6.1.5 GESTIÓN DE RIESGOS

La implementación de un sistema digital de gestión documental y de seguridad de la información implica la aparición de nuevos riesgos tecnológicos, organizacionales y normativos que deben ser gestionados de manera oportuna y preventiva. En el caso del desarrollo de una estrategia que fortalezca la gestión documental y la seguridad de la información presentará principales riesgos identificados que se agrupan en categorías como ser:

1. **Riesgos Operativos:**

La adopción del modelo híbrido puede generar riesgos operativos derivados de la modificación de actividades diarias y la restructuración de flujos de proceso y trabajo, entre los cuales encontramos:

a) Migración de documentos sin control ni estructura definida, lo que genera pérdida temporal de archivos, duplicidad o inconsistencia en versiones
b) Redefinición de roles y responsabilidades, que pueden generar incertidumbre o confusión operativa durante la transición
c) Cambios constantes en flujos de trabajo donde ciertos procesos manuales deberán transformarse en flujos automatizados dentro de M-Files, lo que requiere adaptación gradual por parte del personal
d) Dependencia temporal de ambos sistemas durante la transición lo que generará carga laboral adicional al personal

Con ellos será importante mitigar riesgos, donde se planea que con la utilización de M-Files como herramienta principal, ya que permitirá aplicar automatizaciones que reducen errores operativos comunes tales como:

- Clasificación y catalogación mediante metadatos obligatorios
- Control de versiones y registro de auditorías
- Políticas automáticas de retención
- Asignación de roles y permisos
- Integración completa y segura con Google Drive y Gmail

Con la inclusión de M-Files como propuesta principal no solo garantizamos la mejora y mitigación de múltiples errores que puedan detener la operatividad del negocio sino, mejoramos gradualmente el flujo de trabajo que se realiza en la MiPymes de correduría Seguros Total.

2. **Riesgos tecnológicos:**

Los riesgos tecnológicos van relacionados estrechamente con fallas de infraestructura,

interoperabilidad entre sistemas y aseguramiento de la disponibilidad de la información, entre los cuales encontramos:

a. Interoperabilidad incompleta entre Google Workspace y M-Files, lo que genera inconsistencia en la sincronización de documentos

b. Dependencia de la conectividad a internet, tanto para una consulta o solicitud como la actualización de archivos

c. Errores técnicos durante la migración de documentos, incluyendo archivos corruptos o incompatibles

d. Falta de copias de respaldo automatizadas durante el periodo de transición, lo que aumenta la posibilidad de pérdida de información

e. Dependencia creciente en servicios de nube, que ante cualquier interrupción temporal podría afectar el acceso a documentos críticos para la operación del negocio

En contraste a los riesgos, M-Files incorpora controles tecnológicos que fortalecen la operación y la disponibilidad del sistema como:

- Conectores certificados para Google Drive y Gmail
- Repositorios redundantes y política de respaldo automático
- Restauración inmediata de versiones anteriores
- Cifrado en tránsito y reposo
- Arquitectura escalable

Con la inclusión de M-Files se mejora la estabilidad del entorno híbrido y los riesgos técnicos asociados a una posible implementación.

3. Riesgos en seguridad de la información:

La información manejada por la correduría Seguros Total es sumamente delicada y sensible, por lo que pueden surgir múltiples riesgos como ser:

a. Ausencia de autenticación multifactor en cuentas institucionales

b. Permisos heredados o mal configurados en Google Drive

c. Falta de clasificación por niveles de confidencialidad

d. Riesgo de phishing e ingeniería social detectados en encuestas

e. Ausencia de monitoreo, auditoría o registro formal de incidentes

Con ello, M-Files actuará como una capa robusta que brindará seguridad documental que controla, audita y restringe el acceso a la información, entre sus capacidades se encuentra:

- Modelo de acceso basado en roles y permisos dinámicos
- Autenticación multifactor integrado
- clasificación automática por niveles de seguridad

- Auditoría completa de actividades y rastreo de acción por usuario
- Alerta y controles de acceso y actividades inusuales

Con la inclusión de M-Files como propuesta principal no solo garantizamos la reducción significativa de las vulnerabilidades sino promovemos la seguridad documental total en el flujo operativo.

4. Riesgos de cambio organizacional:

La introducción de un nuevo sistema documental supone un cambio cultural y funcional dentro de la correduría Seguros Total, se identifican riesgos como:

a. Resistencia del personal ante nuevas herramientas y procesos
b. Curva de aprendizaje para el uso de M-Files
c. Falta de adherencia a los nuevos procedimientos
d. Hábitos no estandarizados derivados de los procesos manuales

Considerando estos factores delicados, M-Files brinda unas series de ventajas que permiten combinar la tecnología con la gestión del cambio en las que encontramos:

- Interfaz intuitiva y fácil de aprender
- Flujos automatizados que disminuyen considerablemente carga operativa
- Plantillas preconfiguradas
- Capacitación continua
- Paneles de seguimiento y monitoreo

Con la inclusión de M-Files no solo tendremos una capa de seguridad de información considerable, sino que permitirá que el personal se adapte a la herramienta de manera gradual, segura y efectiva.

6.7 RELACIÓN DEL MODELO CON LAS FUNCIONES DEL MARCO NIST

En la evaluación inicial de Seguro Total, los resultados de los cuestionarios, listas de verificación, análisis de procesos y flujos de documentos mostraron un nivel fundamental o elemental de desarrollo en todas las funciones del NIST, marcado por la falta de políticas, la ausencia de controles sistemáticos, la inexistencia de trazabilidad y una capacidad limitada para Detectar, Responder o recuperarse de incidentes. Estas deficiencias representan riesgos importantes para la continuidad de las operaciones, la integridad de los documentos y la seguridad de la información.

El modelo propuesto para un sistema digital de gestión documental busca reforzar de manera integral las cinco funciones del marco NIST. Cada elemento del diseño se vincula

directamente a los hallazgos del diagnóstico, conectando capacidades operativas y de gobernanza que aumentan la resiliencia de la organización.

Tabla 56: Relación con marco NIST

Función NIST	Aplicación del modelo propuesto	Contribución al cierre de brechas identificadas
Identificar	• Implementación de un modelo estructurado de metadatos que permite identificar el tipo, propósito, nivel de confidencialidad y responsable de cada documento. • Definición formal de roles documentales y propietarios de información, con responsabilidades asociadas. • Repositorio centralizado que actúa como inventario vivo de activos documentales. • Modelo ER que establece relaciones entre documentos, usuarios, procesos y flujos, facilitando la comprensión del ecosistema informacional.	• La empresa carecía de inventario documental y de claridad sobre la propiedad de la información. • Existían procesos fragmentados y dependientes del criterio individual. • No había mecanismos estandarizados para clasificar o comprender el ciclo de vida de la información.
Proteger	• Implementación de controles de acceso basados en roles, aplicando el principio de mínimo privilegio. • Incorporación de autenticación multifactor (MFA) y cifrado de datos en tránsito y reposo. • Uso de plantillas normalizadas y validaciones de calidad obligatorias antes del ingreso al repositorio. • Gestión automatizada de versiones, permisos y retención, alineada con ISO 27001.	• Google Drive se utilizaba sin configuración de seguridad avanzada ni MFA. • No existían controles formales de acceso, visibilidad ni manejo de versiones. • La información estaba expuesta a cambios no autorizados y pérdida de integridad.
Detectar	• Registro continuo de actividades mediante la entidad Auditoría, que documenta accesos, modificaciones, aprobaciones y eliminaciones. • Paneles de actividad y monitoreo de comportamiento del usuario en tiempo real. • Alertas automáticas para Detectar	• La empresa no contaba con mecanismos formales de monitoreo. • No existían registros históricos que permitieran identificar incidentes

	anomalías en flujos, patrones inusuales o incumplimientos de políticas.	o analizar eventos sospechosos. • La capacidad de detección dependía exclusivamente de observaciones manuales y criterios empíricos.
Responder	• Activación de flujos automatizados de revisión y aprobación, que permiten documentar acciones, generar evidencia y coordinar la respuesta. • Capacidad de revertir versiones previas ante incidentes o modificaciones indebidas. • Definición de roles responsables para la gestión de incidentes documentales y escalamiento interno.	• No existía un protocolo institucional para Responder ante incidentes documentales o de seguridad. • El personal dependía de su propio criterio para corregir errores o pérdidas. • No había evidencia documental para sustentar investigaciones posteriores.
Recuperar	• Implementación de versiones históricas recuperables y restauración de documentos comprometidos. • Respaldos automáticos en la nube y redundancia operativa entre M-Files y Google Workspace. • Políticas formales de retención y disposición documental que aseguran continuidad y disponibilidad.	• No existían planes formales de continuidad ni mecanismos de recuperación documental. • El 54–63% del personal dudaba de la capacidad de la empresa para recuperar información tras un incidente. • Se identificó una dependencia riesgosa de Google Drive sin políticas de respaldo.

Nota: Elaborado por autores

6.8 RELACIÓN DEL MODELO CON LAS NORMAS ISO 15489, ISO 30301 E ISO 27001

El sistema digital de gestión documental propuesto se fundamenta en los lineamientos

establecidos por las normas ISO 15489, ISO 30301 e ISO 27001, las cuales definen los requisitos esenciales para asegurar una gestión eficiente, segura y trazable de los documentos y de la información. Estas normas proporcionan el marco conceptual y operativo que garantiza que el diseño planteado no solo optimiza los procesos internos, sino que también fortalece la gobernanza, la seguridad y la continuidad operativa en la organización.

El modelo integra elementos clave como metadatos estructurados, roles documentales, repositorio centralizado, controles de acceso, auditorias y políticas de retención. Cada componente contribuye directamente al cumplimiento de las normas mencionadas, subsanando las debilidades detectadas en el diagnóstico inicial.

Tabla 57: Modelo propuesto versus Normas ISO

Norma ISO	Principios o requisitos clave	Cómo el modelo propuesto los cumple	Brecha identificada que se soluciona
ISO 15489 Gestión de documentos	• Autenticidad, integridad, confiabilidad y disponibilidad documental. • Ciclo de vida del documento. • Clasificación, metadatos y trazabilidad. • Gestión de riesgos documentales.	• Implementación de un repositorio central versionado en M-Files. • Esquema de metadatos para clasificar y describir cada documento. • Control de versiones, auditoría y flujos para garantizar autenticidad y trazabilidad. • Ciclo documental TO-BE que define creación, uso, retención y disposición final.	• Falta de clasificación uniforme. • Ausencia de control de versiones. • Trazabilidad nula en Google Drive. • No existían responsabilidades formales sobre los documentos.
ISO 30301Sistema de gestión	• Planificación y diseño del SGD. • Políticas	• Marco de políticas documentales	• No existían políticas ni roles definidos.

Norma ISO	Principios o requisitos clave	Cómo el modelo propuesto los cumple	Brecha identificada que se soluciona
documental	documentales. • Responsabilidades, roles y competencias. • Documentación del sistema y auditoría. • Evaluación del desempeño del SGD.	integrado • Definición formal de roles documentales, propietarios y responsables de proceso. • Modelo ER que documenta la estructura y funcionamiento del sistema. Auditoría automática y reportes para evaluación continua. • Modelo TO-BE que estructura el sistema de gestión documental.	• No había auditorías documentales ni seguimiento. • Sistema documental empírico y desorganizado. • Falta de evaluación del desempeño del sistema.
ISO 27001 Seguridad de la información	• Gestión de riesgos de seguridad. • Control de accesos. • Protección de información en tránsito y reposo. • Registro de eventos y supervisión. • Respaldo, continuidad y recuperación.	• MFA, permisos basados en roles y control de privilegios. • Cifrado en reposo y en tránsito en M-Files y Google Workspace. • Registro automático de eventos mediante entidad Auditoría. • Respaldos automáticos y recuperación por versiones. • Gestión de riesgos	• No había mecanismos de seguridad robustos. • Ausencia de monitoreo y registro de eventos. • No existía plan de continuidad ni recuperación documental. • Control de accesos dependía de configuraciones básicas de Google Drive.

Norma ISO	Principios o requisitos clave	Cómo el modelo propuesto los cumple	Brecha identificada que se soluciona
		incorporada en la sección 6.5 del capítulo.	

Nota: Elaborado por autores

6.9 PRESUPUESTO E IMPACTO DEL PRESUPUESTO

La adopción de un sistema digital para la gestión de documentos con un enfoque mixto exige analizar su viabilidad financiera para la MiPyME Seguro Total. El presupuesto debe incluir no solo los gastos operativos actuales, sino también la inversión necesaria para la adopción de la tecnología y la capacidad de la empresa para mantener el modelo a largo plazo. En este momento, la compañía utiliza Google Workspace para 11 usuarios, con un coste mensual de USD 197, además del pago anual por el dominio institucional. No obstante, esta infraestructura no satisface los requisitos de trazabilidad, control de acceso, retención de documentos, auditoría ni gobernanza estipulados en las normas ISO 15489, ISO 30301 e ISO 27001, lo que obliga a implementar una plataforma especializada como M-Files.

El presupuesto que se presenta a continuación considera la situación operativa de Seguro Total, estimando las licencias necesarias para 11 usuarios, que corresponden a todo el personal involucrado en el proceso documental. Los costos de implementación, formación y configuración se basan en rangos orientativos proporcionados por socios oficiales de M-Files, que se utilizan como referencia estándar para las estimaciones en proyectos de MiPyme.

Tabla 58: Costos mensuales y anuales de Modelo hibrido M-files más Google Workspace

Concepto	Costo mensual	Costo anual	Observaciones
Google Workspace (13 usuarios)	USD 197	USD 2,364	Costo actual de la empresa.
Dominio institucional	—	USD 50	Pago anual.
Licencias M-Files (11 usuarios)	USD 660	USD 7,920	Recomendado para cobertura total de personal involucradas.
Capacitación inicial (única)	—	USD 900 – 1,300	Estimación basada en partners M-Files.
Configuración y parametrización (única)	—	USD 1,800 – 2,800	Implementación total del sistema.

Nota: (Paulhickey, 2025)

La inversión necesaria para implementar el modelo híbrido M-Files más Google Workspace produce un efecto positivo y considerable en Seguro Total, ya que permite mejoras

significativas en la eficiencia de las operaciones, la seguridad de los datos y el cumplimiento de las regulaciones. Aunque el gasto anual estimado para 11 usuarios ronda entre USD 13,034 y 14,434, incluyendo la fase de implementación y la formación, este costo se traduce en una disminución notable de los reprocesos, el tiempo de búsqueda y los riesgos asociados a la documentación. Además, se incorpora controles de seguridad que cumplen con los estándares ISO 27001 y el marco NIST. Un repositorio único, la utilización de metadatos, la gestión de versiones, la auditoría automática y los flujos de aprobación mejoran la trazabilidad, la integridad y la accesibilidad de los documentos, aspectos cruciales en una correduría de seguros.

De la misma forma, el sistema optimiza la capacidad de la institución para Responder a incidentes y facilita el cumplimiento con las normas ISO 15489 e ISO 30301, lo que eleva la fiabilidad operativa y garantiza la continuidad del negocio. En conjunto, el impacto financiero no solo es factible, sino también estratégico, con un retorno de inversión estimado entre 12 y 18 meses gracias al aumento en la productividad y la reducción de riesgos.

6.9.1 PRESUPUESTO CON MENOR INVERSIÓN

Con la propuesta principal de presupuesto se indica una serie de valores que ofrece M-files en el cual se muestra cada uno de los costes que puede inferir la empresa en la adopción, considerando la demanda actual y el alto coste que puede presentar para la empresa existe una forma de reducir costes en factores como:

- M-Files Learning: Ofrece una plataforma oficial con capacitación online donde se pueden encontrar cursos como Introducción a M-files, uso del repositorio, seguridad y permisos o hasta creación de documentos
- Cursos en plataformas de paga: Existen cursos orientados a la seguridad de la información, Normas ISO, ciberseguridad en MiPymes, automatización con herramientas. Sin embargo, no sustituyen la necesidad de capacitación real para el equipo.

Tabla 59: Costos mensuales y anuales reducidos de Modelo hibrido M-files más Google Workspace

Concepto	Costo mensual	Costo anual	Observaciones
Google Workspace (13 usuarios)	USD 197	USD 2,364	Costo actual de operación.
Dominio institucional	—	USD 50	Pago anual.
Licencias M-Files (11 usuarios)	USD 660	USD 7,920	Basado en USD 60 por usuario/mes.
Capacitación oficial M-Files	—	USD 0	Se sustituye por M-Files Learning (gratuita).
Configuración y parametrización del sistema	—	USD 1,800 – 2,800	Incluye metadatos, flujos, permisos, repositorio.
Perfil TI	USD 850	USD 10,200	Rol responsable de configuración, soporte, auditoría y mejora continua

Nota: (Paulhickey, 2025)

El empleo de M-Files Learning elimina los gastos de formación formal, lo que reduce la inversión inicial sin afectar la adopción del sistema. Esto permite que el presupuesto total anual se reduzca entre 800 y 1,200 dólares en comparación con la estimación anterior. El único aspecto que necesita una inversión directa es la parametrización técnica, que es necesaria para adecuar los flujos, metadatos y permisos al modelo TO-BE de Seguro Total. Gracias a esta optimización, la implementación híbrida se mantiene financieramente viable y más accesible para una MiPyme, preservando todos los beneficios operativos, normativos y de seguridad contemplados.

6.9.2 IMPACTO CUALITATIVO Y CUANTITATIVO DEL SISTEMA HIBRIDO

Tabla 60: Impacto cualitativo del sistema hibrido

Categoría de Impacto	Descripción del Beneficio	Valor Estratégico para la Organización
Trazabilidad y auditoría	Registros automáticos de acciones, control de versiones y evidencias conforme a ISO 15489/30301/27001.	Fortalece la gobernanza documental y facilita auditorías internas y externas.
Seguridad de la información	Permisos por rol, cifrado, MFA, retención automática y protección del ciclo de vida del documento.	Reduce riesgos de acceso indebido, fuga de datos y pérdida de información.
Estandarización de procesos	Flujos automáticos, validaciones, plantillas y uso de OCR que eliminan reprocesos.	Mejora la eficiencia operativa y disminuye errores humanos.
Mejora en la experiencia del	Búsquedas rápidas, documentos organizados, accesibilidad desde	Incrementa la productividad y reduce fricción operativa.

usuario	múltiples dispositivos.	
Transparencia y gobernanza	Roles y responsabilidades claramente definidos en el sistema.	Fomenta cumplimiento normativo y control institucional.
Continuidad del negocio	Automatización de respaldos, retención y recuperación.	Reduce el impacto de incidentes y mejora la resiliencia organizacional.

Nota: Elaborada por autores

La Tabla 60 muestra las ventajas cualitativas que surgen de la adopción del sistema híbrido M-Files + Google Workspace. Estos efectos no se cuantifican en números, pero reflejan importantes avances en áreas como seguridad, gobernanza, normatividad y eficacia operativa. La tabla sintetiza de qué manera el nuevo enfoque ayuda a cumplir con las regulaciones, optimiza la trazabilidad y refuerza los métodos internos para la gestión documental. Estas ventajas cualitativas son fundamentales para fundamentar el uso del sistema, ya que convierten prácticas informales en procedimientos organizados y verificables.

Tabla 60: Impacto cuantitativo del sistema hibrido

Indicador Medible	**Situación Actual**	**Situación con M-Files + Google Workspace**	**Impacto Cuantitativo aproximado**
Tiempo de búsqueda de documentos	5–15 min por búsqueda	1–3 min por búsqueda	Reducción del **40–60%** (equivalente a 80–120 horas por empleado/año).
Reprocesos por mala digitalización	Alto nivel de escaneos y errores manuales	OCR + validaciones automáticas	Disminución del **25–40%** de reprocesos.
Riesgo de pérdida de información	Sin respaldo automatizado ni retención	Repositorio central, versiones y retención	Reducción del riesgo en **70–90%**.
Tiempo de aprobación	1–3 días según disponibilidad	Flujos automáticos y notificaciones	Reducción del **30–50%** del tiempo.
Exposición a accesos indebidos	Sin MFA, permisos informales	Control por roles + MFA	Reducción de incidentes en **50–70%**.
Consumo de almacenamiento	Duplicados y versiones múltiples	Eliminación automática de duplicados	Optimización del **20–35%** del espacio.

Nota: Elaborada por autores

La tabla 61 mide los impactos específicos de la puesta en marcha, contrastando el estado actual y rendimiento esperado luego de una posible adopción de este diseño de sistema de gestión documental: Mediante métricas como el tiempo de búsqueda, gestión de versiones, seguridad y plazos se prevén avances cuantificables que se convierten en importantes ahorros operativos. Esta información número ayudará notablemente a validar el retorno de la inversión

que tendrá para la correduría seguros total además de beneficios esperados mediante la adopción.

6.10 PLAN DE CAPACITACIÓN

El plan de capacitación y adopción busca asegurar que los usuarios comprendan, acepten y utilicen las funcionalidades y procesos relacionados con la gestión documental y la seguridad de la información garantizando la sostenibilidad del modelo operativo.

1.Objetivo general:

Asegurar el uso de las mejores prácticas de las Normas ISO y temas de seguridad asociados al marco NIST de Ciberseguridad en la correduría Seguro Total.

2.Alcance:

- Usuarios de negocio (creación, validación y aprobación de documentos).
- Equipo Directivo
- Soporte técnico y administradores del sistema.

La capacitación externa se plantea como un complemento formativo y no sustituye las políticas, procedimientos y controles internos definidos por la organización.

3.Metodología de la capacitación:

Las metodologías de las capacitaciones se realizarán mediante el uso cursos de Coursera en donde se combina el uso de conocimiento practico y teórico para tener un mayor entendimiento sobre la ciberseguridad, uso de las herramientas e importancia de la gobernanza, con el fin de asegurar la adopción efectiva del modelo propuesto.

4.Tipos de capacitación

Tabla 61: Plan de Capacitación

Tipo	Descripción	Público objetivo
Funcional	Uso de la herramienta, flujos de aprobación, almacenamiento de la información, charlas sobre las Normas ISO y el Marco NIST.	Usuarios de Negocios.
Técnica	Configuración de MFA, almacenamiento y eliminación de la información.	Usuarios de Negocios y Equipo Directivo.
Gobernanza sobre los documentos	Mejores prácticas, roles, RACI y procesos de control.	Usuarios de Negocios y Equipo Directivo.

Nota: Elaborada por los autores

5.Roles y Responsabilidades de la Capacitación:

Los siguientes roles y responsabilidades son necesarios para el aseguramiento de la implementación y seguimiento correcto del plan de capacitación:

Tabla 62: Roles y Responsabilidades Plan de Capacitación

Rol	Responsabilidad
Dirección	Aprobar el plan de capacitación y asegurar la participación del personal
Responsable de TI	Coordinar la capacitación técnica y controles de seguridad
Usuarios de negocio	Participar activamente y aplicar lo aprendido
Administrador del sistema	Brindar soporte y seguimiento post-capacitación

Nota: Elaborada por los autores

6.Evaluación y Seguimiento

La efectividad del plan de capacitación será evaluada mediante:

- Validaciones de conocimiento al finalizar las sesiones.
- Retroalimentación de los participantes.
- Verificación del uso correcto de la herramienta y los procesos documentales.
- Seguimiento a incidentes relacionados con errores de gestión documental o seguridad.
- Obtención de certificado de cursos.

7.Indicadores Claves:

Los siguientes indicadores permitirán a los encargados y a la gerencia evaluar la eficiencia y conocimiento adquirido de las capacitaciones a realizarse:

Tabla 63: Indicadores Plan de Capacitación

Indicador	Descripción
% de usuarios capacitados	Relación entre usuarios capacitados y total de usuarios
Nivel de aprobación	Resultado promedio de evaluaciones
Reducción de errores	Disminución de incidentes documentales
Adopción del sistema	Uso efectivo del sistema posterior a la capacitación

Nota: Elaborada por autores

8.Cursos recomendados de capacitación:

Los siguientes cursos representan una propuesta para la correduría en donde los cuales pertenecen a Coursera y M-Files, brindando la facilidad de que los usuarios realicen los cursos en tiempos fuera de la oficina sin comprometer sus tareas diarias. Estos deberán ser completadas en las fechas que la correduría establezca. Cabe destacar que estos cursos son gratuitos para que la corredura no incurra en costos adicionales de capacitación.

Tabla 64: Cursos Plan de Capacitación

Curso	Plataforma	Enfoque	Público objetivo	Relación con el modelo
Curso general de Google Workspace	Coursera	Uso de herramientas colaborativas (Drive, Gmail, gestión documental)	Usuarios de negocio y equipo directivo	Gestión documental, colaboración y almacenamiento seguro
Ciberseguridad para PYMES	Coursera	Principios de ciberseguridad, riesgos y buenas prácticas	Gerencia y Administradores de TI	ISO 27001, NIST CSF (Identificar, Proteger)
Cisco Cybersecurity (especialización)	Coursera	Seguridad de la información, amenazas y controles	Administradores de TI y soporte técnico	NIST CSF, control de accesos, protección de la información
Academia M-Files	M-Files	Fundamentos y funcionalidades	Usuarios, administradores y gerencia	Gestión documental

Nota: Elaborada por los autores

6.11 ROLES Y RESPONSABILIDADES

Con el fin de asegurar el funcionamiento adecuado del Sistema de Gestión Documental y garantizar el cumplimiento de los principios establecidos por las normas ISO 15489, ISO 30301 e ISO 27001, se establecen los siguientes roles y responsabilidades que deberán ser creados dentro de la organización:

1.Responsable de Gestión Documental (Administrador del SGD)

Responsabilidades:

- Administrar la estructurar general del almacenamiento de documentos físicos y digitales
- Verificar el cumplimiento de políticas, procedimientos y lineamientos documentales
- Monitorear y validar la correcta clasificación, carga y actualización de documentos.
- Autorizar la eliminación de documentación según la tabla de retención definida en el capítulo IV.
- Coordinar y realizar procesos de auditoria documental.
- Ser la figura de contacto con las aseguradoras en temas de actualización y validación de documentos.

2.Gerencia:

Responsabilidades:

- Aprobar políticas, normas y directrices con apoyo del responsable de gestión documental.
- Asignar los recursos necesarios para asegurar la operación y continuidad del SGD.
- Definir y asignar s los roles para el SGD.
- Alinear el SGD a los objetivos estratégicos de la correduría.
- Supervisar el cumplimiento de normativas y requisitos regulatorios.

3.Usuarios Funcionales:

Responsabilidades:

- Capturar y cargar correctamente la documentación genera de cada cliente
- Cumplir con las normativas y políticas relacionadas al SGD
- Verificar que los documentos estén completos, legibles y actualizados
- Mantener la confidencialidad de la información.
- Reportar al administrador del SGD inconsistencias, duplicados o documentos ya no vigentes

4.Equipo de TI (Personal de TI)

Responsabilidades:

- Administrar permisos de acceso al SGD.
- Configurar y mantener actualizadas las aplicaciones de la correduría.
- Implementar controles de seguridad informática y asegurar resolución de incidentes.
- Garantizar la disponibilidad y estabilidad de la arquitectura empresarial.

5.Auditor Interno:

Responsabilidades:

- Revisar periódicamente l cumplimiento de las políticas documentales.
- Evaluar el nivel de madurez progresivamente y definir acciones de corrección.
- Validar la trazabilidad, integridad y disponibilidad de la información
- Identificar riesgos documentales y proponer acciones de mitigación.

La siguiente matriz RACI establece de manera clara la distribución de responsabilidades y niveles de participación de cada rol involucrado en el Sistema de Gestión Documental. Este esquema permite asegurar trazabilidad, gobernanza y coherencia operativa, cumpliendo con los lineamientos de ISO 15489, ISO 30301 y los principios de responsabilidad definidos en ISO 27001 y el Marco NIST CSF.

Tabla 65: Matriz RACI de Responsabilidades del SGD

Actividad / Responsabilidad	Gerencia	Responsable	Operaciones	TI	Auditoría
Definir políticas y normas documentales	A	R	C	C	I
Aprobar políticas del sistema documental	R	C	I	I	I
Administrar repositorio institucional	I	R	C	C	I
Definir y mantener la estructura de carpetas	C	R	C	C	I
Clasificar y cargar documentos correctamente	I	C	R	I	I
Verificar integridad, vigencia y completitud de documentos	I	R	C	I	C
Definir roles y permisos de acceso	A	C	I	R	I
Configurar y mantener infraestructura digital (Drive, permisos, MFA)	I	C	I	R	I
Control de versiones y documentos oficiales	I	R	C	I	C
Actualización del expediente del cliente	I	C	R	I	I
Ejecución del plan de respaldo y continuidad	C	C	I	R	I
Reporte y gestión de incidentes de seguridad	I	C	R	R	C
Eliminación segura de documentos	A	R	C	I	C
Auditorías del sistema documental	I	C	I	I	R
Capacitación en gestión documental	C	R	R	I	C
Seguimiento a indicadores del SGD	C	R	C	I	C

Nota: Elaborada por los autores

- R – Responsable: Ejecuta la tarea directamente.
- A – Aprobador: Tiene autoridad final y toma decisiones.
- C – Consultado: Participa aportando información o criterio.
- I – Informado: Debe ser notificado, pero no interviene.

6.12 MEDIDAS DE CONTROL

Para asegurar la mejora continua del Sistema de Gestión Documental y verificar su funcionamiento operativo, es necesario establecer un conjunto de indicadores que permitan medir el desempeño, el cumplimiento y la eficacia del sistema. Estos indicadores servirán como mecanismo de monitoreo y toma de decisiones, en coherencia con los lineamientos de la ISO 30301, que hace hincapié en la importancia del monitoreo continuo y la evaluación del sistema, así como con los principios de control y trazabilidad establecidos por la ISO 15489. A continuación, se presentan los indicadores base que deberán implementarse y revisarse de forma periódica.

Tabla 66: Indicadores Base del Sistema de Gestión de Documentos

Indicador	Descripción	Objetivo	Fórmula	Frecuencia	Umbrales
Actualización del expediente del cliente	Mide si los datos y documentos del cliente están actualizados	Asegurar vigencia de la información clave	% expedientes actualizados / total expedientes	Mensual	Max:90% Alerta:>70 %
Documentos completos por póliza	Verifica si cada póliza tiene todos los documentos requeridos	Garantizar integridad documental	# pólizas completas / # pólizas revisadas	Mensual	Max:95% Alerta:>85 %
Tiempo de carga documental	Tiempo promedio desde que se recibe un documento hasta que se incorpora al sistema	Reducir retrasos operativos y reprocesos	Promedio de horas/días	Semanal / Mensual	Max:3horas Alerta:< 5 horas
Cumplimiento de clasificación documental	Evalúa si los documentos están almacenados según el modelo establecido	Asegurar orden y recuperabilidad	% documentos bien clasificados / total documentos	Trimestral	Max:95% Alerta:75%
Errores de duplicidad	Cantidad de documentos duplicados detectados.	Reducir redundancia y riesgo operativo	# duplicados encontrados	Mensual	Max: %10 Alerta:25%
Accesos no autorizados Detectados	Intentos de acceso fuera de los permisos	Monitoreo de seguridad	Reporte de incidentes	Mensual	Max: 5 Alerta:< 5

	definidos				
Disponibilidad del repositorio	Mide el tiempo que el sistema/documentos están accesibles	Garantizar continuidad operativa	% subida mensual	Mensual	N/A
Índice de digitalización	Cuántos documentos físicos ya están digitalizados	Migrar hacia un sistema más eficiente	# docs digitalizados / # docs totales	Trimestral	Max:95% Alerta:> 50%
Satisfacción del usuario interno	Evalúa la percepción de los colaboradores sobre el SGD	Identificar oportunidades de mejora	Encuesta simple 1–5	Trimestral	Max:4 Alerta:< 2.5
Cumplimiento de políticas documentales	Grado en que los equipos siguen las políticas establecidas	Fortalecer gobernanza	Auditoría interna del SGD	Semestral	N/A

Nota: Elaborada por los autores

La implementación de estos indicadores permitirá evaluar objetivamente el desempeño del Sistema de Gestión Documental, identificar desviaciones, aplicar acciones correctivas y asegurar su mejora continua. Su seguimiento sistemático contribuirá a fortalecer la gobernanza, la seguridad de la información y la eficiencia operativa de la correduría.

6.13 ESTRUCTURA DE ALMACENAMIENTO

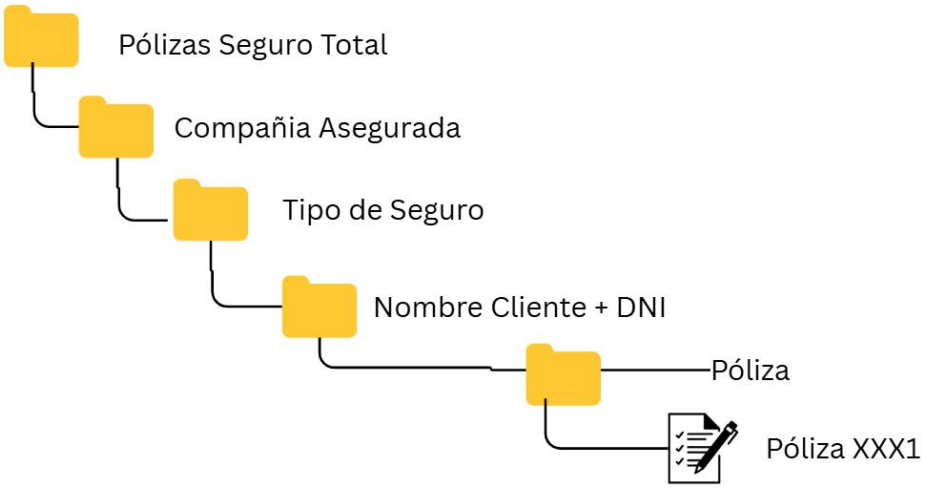
En este caso, la estructura de almacenamiento propuesta para la correduría se organiza en dos modelos complementarios, cada uno orientado a cubrir necesidades documentales distintas:

1.Una estructura dedicada al almacenamiento de pólizas.

2. Una estructura destinada a los documentos de identificación del cliente.

Para la primera estructura, se parte de una carpeta principal denominada “Pólizas Seguro Total”, seguida por subcarpetas corresponde rientes a la compañía aseguradora y posteriormente al tipo de seguro. Dentro de esta clasificación se incorpora una carpeta por cliente, utilizando como convención el formato “Nombre Apellido – DNI”, por ejemplo: *“*FERNANDO ÁLVAREZ 0801-1999-10739*”*, lo cual permite diferenciar correctamente a personas con nombres similares. Finalmente, dentro de cada cliente se incluye una carpeta específica para la póliza corresponde y otra para los documentos anexos, propios del tipo de seguro que se gestione.

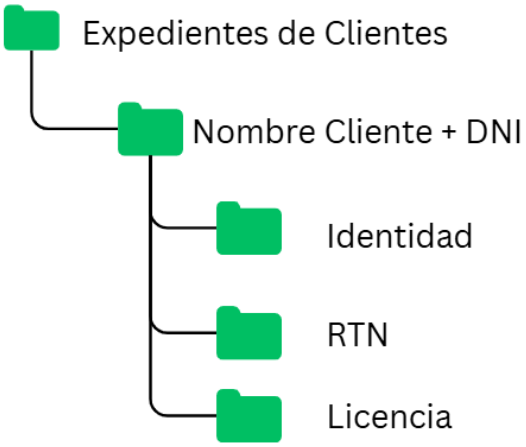
Figura 48: Estructura de Almacenamiento de Pólizas



Nota: Elaborada por los autores

En cuanto al segundo modelo, debido a que documentos clave como el DNI, la licencia de conducir o el RTN son utilizados en múltiples tipos de seguros y procesos internos, se propone una estructura independiente bajo una carpeta principal denominada “Expedientes de Clientes”. Esta mantiene el mismo criterio de identificación del cliente “Nombre Apellido–DNI “y contiene subcarpetas específicas para cada tipo de documento personal. De esta manera se evita la duplicidad de archivos, se facilita la trazabilidad y se garantiza un acceso más rápido y ordenado a la información esencial del cliente.

Figura 49: Estructura de Almacenamiento de Pólizas No.2



Nota: Elaborada por los autores

6.14 METADATOS DE LOS DOCUMENTOS

Como parte integral de la gestión de documentos es necesario mantener los siguientes metadatos los cuales aseguran la integridad y confiabilidad de la información, las cuales se pueden visualizar en las siguientes tablas:

Tabla 67: Metadatos Cliente

Metadato	Descripción	Tipo	Obligatorio
ID_Cliente	Código interno único para identificar al cliente	Texto / Numérico	Sí
Nombre completo	Nombre y apellido del cliente	Texto	Sí
DNI / Identidad	Número de documento nacional	Texto	Sí
RTN	Registro Tributario Nacional	Texto	Sí
Teléfono	Número principal de contacto	Texto	Sí
Correo electrónico	Email del cliente	Texto	Sí
Dirección	Ubicación general del cliente	Texto	No
Tipo de cliente	Individual / Empresa	Lista	Sí
Estado del cliente	Activo / Inactivo / En seguimiento	Lista	Sí
Fecha de alta	Fecha en que se registró al cliente	Fecha	Sí
Ejecutivo asignado	Asesor responsable	Texto	Sí
Última actualización	Última fecha de modificación del expediente	Fecha	Sí

Nota: Elaborada por los autores

Estos metadatos del cliente permiten a la correduría mantener una mayor trazabilidad y control sobre sus clientes, es muy importante destacar que estos metadatos corresponden a los datos maestros que identifican de forma integral a un cliente de la correduría, evitando de esta manera crear clientes duplicados y mantener un registro único dentro del sistema.

Tabla 68: Metadatos Pólizas

Metadato	**Descripción**	**Tipo**	**Obligatorio**
ID_Póliza	Identificador interno único de la póliza	Texto / Numérico	Sí
Número de póliza	Número asignado por la aseguradora	Texto	Sí
Compañía aseguradora	Nombre de la aseguradora	Lista	Sí
Tipo de seguro	Vida, Auto, Salud, Daños, etc.	Lista	Sí
Producto o plan	Varía según aseguradora	Texto	No
Cliente asociado	ID del cliente propietario de la póliza	Relación	Sí
Fecha de emisión	Fecha en que se emitió la póliza	Fecha	Sí
Inicio de vigencia	Inicio de cobertura	Fecha	Sí
Fin de vigencia	Fin de cobertura	Fecha	Sí
Estado	Vigente / Vencida / Cancelada / Propuesta	Lista	Sí

Ejecutivo responsable	Corredor que gestiona la póliza	Texto	Sí
Frecuencia de pago	Mensual / Trimestral / Anual	Lista	No
Documentos asociados	Enlace a carpeta o referencia documental	Relación	Sí

Nota: Elaborada por los autores

Los metadatos de las pólizas permiten a la correduría gestionar de forma ordenada y trazable todo el ciclo de vida de los documentos dentro del SGD. A través de cada uno de estos se garantiza la correcta identificación, relación con el cliente y la aseguradora corresponde. Así como, también el control de su vigencia, estado y condiciones principales. Esta estructura nos facilita la consulta, seguimiento y administración de las pólizas, lo que reduce los errores y asegura la disponibilidad de la información.

Tabla 69: Metadatos Documentos Principales

Metadato	Descripción	Tipo	Obligatorio
ID_Documento	Identificador único interno	Texto / Numérico	Sí
Tipo de documento	DNI, RTN, Licencia, Póliza, Recibo, Endoso, etc.	Lista	Sí
Cliente asociado	ID del cliente	Relación	Sí
Número de documento	Número único (para DNI, RTN, licencia o documentos formales)	Texto	No
Fecha del documento	Fecha en que fue emitido	Fecha	Sí
Fecha de vencimiento	Para licencia, identidad, documentos temporales	Fecha	No
Estado del documento	Vigente / Vencido / Reemplazado / Histórico	Lista	Sí
Usuario que lo cargó	Responsable que subió el documento	Texto	Sí
Fecha de carga	Fecha de incorporación al sistema	Fecha	Sí
Versión del documento	Control de versiones del archivo	Texto	No
Nivel de sensibilidad	Normal / Confidencial / Datos médicos	Lista	Sí
Permisos de acceso	Áreas o roles autorizados	Lista	Sí

Nota: Elaborada por los autores

Los metadatos de los documentos principales permiten asegurar la correcta clasificación, identificación, control y acceso a la documentación que utiliza la correduría. Estos metadatos nos permitirán mantener la trazabilidad del documento desde su alta al sistema, mantener control de versiones, definir niveles de confidencialidad.

6.15 POLÍTICAS

Las siguientes políticas son la base para el diseño y directrices que el Sistema de Gestión Documental debe seguir para asegurar su uso eficiente. Mediante su implementación, la correduría podrá asegurar su trazabilidad, control y correcta administración de la información a través de su objetivo principal, alcance, principios, responsables y consecuencias en caso de incumplimiento de estas.

6.15.1 POLÍTICA DE GESTIÓN DOCUMENTAL

Objetivo:

Establecer y garantizar los lineamientos, responsabilidades y principios que regula todo el ciclo de vida de los documentos en la correduría, en donde se contempla la creación, respaldo, clasificación, acceso, uso, alanceamiento y eliminación de los documentos internos tanto como externos por la correduría Seguro Total, garantizando de esta manera su autenticidad, integridad, confiabilidad y disponibilidad.

Alcance:

Aplica a todos los colaboradores de la correduría que generan, gestionan o almacenen documentación relacionada con clientes, pólizas, reclamos o procesos internos.

Principios:

- Toda la gestión documental debe realizarse conforme a la ISO 15489 e ISO 30301
- Todo documento debe registrarse y almacenarse en el sistema de gestión de documentos
- La información debe ser accesible únicamente para los roles autorizados
- Todo documento debe mantenerse su trazabilidad y evidencia de su ciclo de vida dentro de la correduría.

Responsabilidades:

- Toda la definición de directrices y cambios sobre el sistema de gestión digital deben ser autorizados por la gerencia
- Todo colaborar tiene la responsabilidad de registrar y almacenar correctamente la documentación que genere.
- La figura de responsable documental debe supervisar el cumplimiento de esta aplicación.

Lineamientos generales:

- Los documentos deben clasificarse según la estructura oficial de almacenamiento.
- Se prohíbe almacenar información oficial en cuentas personales o dispositivos no autorizados.
- Toda modificación debe quedar registrada mediante control de versiones.

6.15.2 POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

Objetivo:

Proteger la información documental de Seguro Total garantizando su confidencialidad, integridad y disponibilidad, conforme a ISO 27001 y a la función Gobernar del NIST CSF 2.0.

Alcance:

Aplica a todos los documentos físicos y digitales, llegando hasta las pólizas, aplicaciones, expedientes, documentos internos como externos.

Directrices:

- El equipo de TI debe establecer las normas de contraseñas mediante un mínimo de 8 caracteres, mínimo un carácter numérico, una letra en mayúscula y un carácter especial.
- Queda prohibido compartir documentos sensibles mediante WhatsApp personales u otros canales no institucionales.
- Todo usuario debe autenticarse mediante el uso del MFA.
- El acceso a los archiveros es mediante el uso de una llave física la cual debe ser solicitada al administrador del SGD.
- Se debe reportar inmediatamente cualquier incidente de seguridad o pérdida de documentos.

Clasificación de documentos:

Los documentos seguirán la siguiente clasificación dentro del sistema:

1. Base: Documentos de acceso compartido.
2. Confidencial: Documentos con mayores privilegios de acceso.
3. Alta confidencial: Documentos limitados a alta gerencia, los cuales se necesita autorización para poder visualizarse.

Responsabilidades:

- La administración asigna permisos de acceso por rol.

- Los colaboradores deben proteger credenciales y evitar divulgación no autorizada.
- Todo incidente debe documentarse y analizarse para prevenir recurrencias.

6.15.3 POLÍTICA DE CONTROL DE VERSIONES Y AUTENTICIDAD

Objetivo:

Garantizar que cada documento mantenga su autenticidad, trazabilidad y vigencia mediante un control de versiones que permita identificar cada documento oficial en cualquier del ciclo de vida del proceso.

Alcance:

Aplica a los documentos de pólizas, reclamos, endosos, documentos de clientes y registros internos.

Lineamientos:

- Toda modificación de impacto debe generar una nueva versión del documento
- Solo la versión aprobada y vigente puede utilizarse en procesos operativos.
- Se conservarán versiones históricas cuando representen evidencia relevante.
- El documento oficial debe incluir fecha, responsable de la edición y estado (vigente/histórico).
- Se debe utilizar una convención estandarizada en nombres de archivos.

Responsabilidades:

- El colaborador responsable del proceso debe asegurar que la versión vigente esté en el repositorio oficial.
- No se permite circular documentos fuera del control documental (por correo personal u otros medios no autorizados).

6.15.4 POLÍTICA DE CONSERVACIÓN, RETENCIÓN Y ELIMINACIÓN DOCUMENTAL

Objetivo:

Establecer los criterios para conservar, retener y eliminar documentos de forma segura y conforme a los requisitos legales, regulatorios y normativos aplicables a la correduría.

Principios:

- La información debe conservarse durante el tiempo necesario para fines legales, comerciales y de auditoría.
- La eliminación debe realizarse de manera segura, evitando su recuperación no autorizada tanto de forma física y digital.
- Los documentos que mayores a los últimos 5 años deberán procesarse y enviar con

RANSA para su almacenamiento.

- Todos los documentos sensibles deben manejarse según el nivel de protección requerido.

Lineamientos:

- Documentos de identidad del cliente: conservar mientras el cliente esté activo + 5 años.
- Pólizas: conservar la póliza vigente y las históricas durante 10 años posteriores a su vencimiento.
- Documentos de reclamos: conservar por un mínimo de 10 años por requisitos legales.
- Correspondencia con aseguradoras: conservar por 5 años.
- Eliminación segura: triturado físico y eliminación digital permanente del repositorio institucional.

Responsabilidades:

- El responsable documental autoriza eliminaciones.
- Los colaboradores deben reportar documentos vencidos o duplicados.
- Ningún documento debe eliminarse sin autorización formal.

6.15.5 POLÍTICA DE USO Y ADMINISTRACIÓN DEL REPOSITORIO DOCUMENTAL

Objetivo:

Asegurar que el repositorio institucional funcione como única fuente oficial de documentos, garantizando orden, consistencia, trazabilidad y accesibilidad.

Lineamientos generales:

- El repositorio oficial es el único espacio autorizado para almacenar documentación institucional.
- Se debe seguir estrictamente la estructura de carpetas definida (pólizas y expedientes de clientes).
- Los nombres de archivos deben respetar la convención institucional para facilitar la búsqueda.
- Los documentos deben cargarse inmediatamente después de ser recibidos o generados.
- Se prohíbe crear carpetas paralelas no autorizadas o duplicar información.

Responsabilidades:

- El administrador documental mantiene la estructura general del repositorio.
- Los colaboradores deben cargar documentos con metadatos correctos.

- Cualquier desviación debe corregirse o reportarse.

Control y supervisión:

- Auditorías trimestrales del repositorio.
- Reportes de documentos incompletos, duplicados o mal clasificados.
- Seguimiento del cumplimiento mediante indicadores definidos en el sistema documental.
- Revisión semestral entre los colaboradores para oportunidades de mejora del sistema de gestión de documentos.

6.15.6 INCUMPLIMIENTO DE POLÍTICAS

De forma general el incumplimiento de las políticas mencionadas anteriormente sobre la gestión documental y la seguridad de la información podrá generar consecuencias proporcionales a la gravedad y al nivel de recurrencia de esta, con el objetivo de proteger la información de la compañía tanto interna, como de los clientes y de esta manera asegurar la correcta operación del Sistema de Gestión documental. Las consecuencias podrán incluir.

- Comunicación y notificación forma cunado el incumplimiento es leve o producto de falta de conocimiento.
- Implementación de capacitación obligatorio en casos en donde se identifiquen fallas reiteras en el uso del SGD.
- Corrección inmediate del incumplimiento, incluyendo la reclasificación, reubicación o actualización de los documentos.
- Restricción temporal de acceso cuando se Detectare un uso indebido del sistema el cual representa un riesgo para la información.
- Reporte a gerencia en caso de incumplimiento graves como compartir información fuera o uso indebido de la información que comprometa la integridad de la información y de la correduría, confidencialidad o continuidad del negocio. En este caso recae en la gerencia si el contrato del usuario o usuarios será terminado de manera inmediata.

6.16 MATRIZ DE ESTRATEGIAS DEL FODA

Las estrategias con base a la Matiz FODA nos permiten identificar y potenciar las oportunidades de mejora de la gestión documental dentro de la correduría de Seguro Total, en donde estas complementan nuestra propuesta de directrices y diseño de un SGD con base a las Normas ISO y el Marco de Ciberseguridad del NIST.

- **Estrategias FO (Fortalezas + Oportunidades):** Describen como potencias las

fortalezas internas para traducirse en ventajas estratégicas.

- **Estrategias DO (Debilidades + Oportunidades):** Dan la pauta de como trabajar las
  debilidades internas canalizando, creando nuevas oportunidades.
- **Estrategias FA (Fortalezas + Amenazas):** Indican la forma en que se pueden utilizar
  las fortalezas internas para superar las amenazas del entorno.
- **Estrategias DA (Debilidades + Amenazas):** Indican como reducir el riesgo de las debilidades frente a las amenazas del entorno.

Figura 50: Estrategias Matriz FODA

Matriz FODA	**Fortalezas**	**Debilidades**	**Oportunidades**	**Amenazas**
	Uso de herramientas digitales como ser Google Gmail y Drive, facilitando la colaboración y acceso remoto a documentos. Colaboradores abiertos a la digitalización buscando mejorar la agilidad y organización dentro de la empresa. Estructura organizativa flexible por su tamaño, lo que permite implementar cambios tecnológicos Alto nivel de conciencia de los colaboradores sobre la importancia de la seguridad de la información	Falta de roles y responsabilidades definidas con relación a la gestión documental Falta de un proceso definido de gestión documental Bajo nivel de seguridad en sus herramientas digitales y a sus archivos físicos Desconocimiento parcial de las normas ISO y el marco NIST Bajo nivel de satisfacción frente a la herramienta actual de gestión documental Falta de indicadores para seguimiento y control Falta de planes de acción frente a incidentes Bajo índice de confianza de los colaboradores en base a la gestión de incidentes y resolución de problemas Falta de actualización de documentos asociados a las diferentes pólizas existentes	Existe la posibilidad de implementar un sistema de gestión digital basado en las normas ISO y el marco de Ciberseguridad del NIST Disponibilidad de herramientas o soluciones accesibles en el mercado para fortalecer la gestión documental Aumentar capacitaciones en temas de seguridad de la información y funcionalidades técnicas de la herramienta Existe potencial para mejorar la eficiencia interna enfocado a la accesibilidad, disponibilidad y seguridad de la información Disponibilidad de herramientas que pueden integrarse entre sí Existe la posibilidad de definir roles y responsabilidades con base a la gestión documental	Alto riesgo de ataques de ciberseguridad por bajos niveles de control y monitoreo Perdida de información sensible Falta de continuidad operativa Alto nivel de competencia de corredurías y corredores indivudales de seguros Cambios regulatorios en materia de protección de datos Competencia tecnológica frente a corredurías con sistemas mas actualizados No existe un respaldo de toda la documentación de la empresa
Estrategias	**Estrategias FO (Fortalezas + Oportunidades)**		**Estrategias DO(Debilidades +Oportunidades)**	
	Aprovechar el uso actual de herramientas digitales como Google Drive y Gmail para implementar progresivamente un sistema de gestión documental alineado a normas ISO y al marco NIST.		Definir roles y responsabilidades formales en la gestión documental apoyándose en las buenas prácticas de las normas ISO y el marco NIST.	
	Capitalizar la apertura de los colaboradores hacia la digitalización para facilitar la adopción de prácticas documentales estandarizadas.		Diseñar e implementar un proceso de gestión documental estandarizado aprovechando herramientas accesibles disponibles en el mercado.	
	Utilizar la estructura organizativa flexible para integrar soluciones tecnológicas accesibles que mejoren la eficiencia y disponibilidad de la información.		Reducir el desconocimiento normativo mediante programas de capacitación en gestión documental y seguridad de la información.	
	Fortalecer la cultura de seguridad de la información mediante capacitaciones enfocadas en buenas prácticas documentales.		Implementar indicadores básicos de seguimiento y control utilizando funcionalidades de las herramientas digitales actuales.	
	Estrategias FA (Fortalezas + Amenazas)		**Estrategias DA (Debilidades + Amenazas)**	
	Aprovechar la conciencia existente sobre la seguridad de la información para reducir el riesgo de ataques de ciberseguridad.		Implementar controles básicos de continuidad operativa y respaldo de la información para mitigar el riesgo de pérdida documental.	
	Utilizar las capacidades actuales de las herramientas digitales para establecer controles mínimos de respaldo y acceso a la información.		Establecer políticas mínimas de gestión documental que reduzcan la exposición ante amenazas regulatorias y tecnológicas.	
	Promover la colaboración interna para responder de forma más efectiva ante incidentes de seguridad.		Estandarizar la actualización y control de documentos para disminuir riesgos operativos.	
	Usar la agilidad organizacional para adaptarse oportunamente a cambios regulatorios en protección de datos.		Desarrollar un plan de mejora gradual que permita enfrentar la competencia tecnológica del entorno.	

Nota: Elaborada por los autores

6.17 CRONOGRAMA DE IMPLEMENTACIÓN

Con el objetivo de garantizar el diseño e implementación posterior del SGD y alineada con los estándares internacionales de la gestión documental y seguridad de la información, se define un cronograma de actividades basado en la metodología DIRKS. En donde este cronograma permite estructurar de manera secuencial las fases necesarias y aquellas elaboradas en este estudio de caso para diseñar y consolidar un SGD acordade a las necesidades de la MiPyme Seguro Total.

El cronograma incluye las actividades y objetivos realizados durante la elaboración de esta propuesta y se basa en las Normas ISO 15489, ISO 3301, ISO 27001 y el Marco NIST de Ciberseguridad. Teniendo como finalidad servir como una guía de ejecución que facilite la coordinación de actividades, asignación de responsabilidades y seguimiento de los hitos del proyecto.

El cronograma contempla las fases desde la planificación inicial hasta el diseño del proyecto. Cada una de estas fases agrupa actividades específicas y entregables que Responden a las etapas definidas por la metodología DIRKS y entregables que los investigadores consideran necesarios para el seguimiento y control del SGD, permitiendo de esta manera asegurar la coherencia entre el análisis de la situación actual, diseño conceptual y el diseño del sistema documental. Se busca de forma general minimizar riesgos, evitar reprocesos y asegurar que cada etapa cuente con los insumos necesarios antes de avanzar a la siguiente, en donde se fortalece la gobernanza, la trazabilidad y sostenibilidad del sistema.

Fase 1. Inicial y Planificación del Proyecto

Comprende establecer todas las bases del proyecto para el diseño del SGD, en donde se incluye la definición de roles y responsabilidades, validación del plan de trabajo y la alineación con los objetivos estratégicos. El propósito de esta fase es asegurar que todas las partes involucradas comprendan los objetivos, responsabilidades y expectativas del proyecto antes de iniciar cualquier actividad técnica.

Figura 51: Fase 1 del Cronograma

SGD Diseño y Directrices

Seguro Total
Christian& Jason

GRÁFICO GANTT SIMPLE de Vertex42.com
https://www.vertex42.com/ExcelTemplates/simple-gantt-chart.html

Inicio del proyecto: lun, 10/20/2025
Semana para mostrar: 1

No	TAREA	ASIGNADO A	PROGRESO	INICIO	FIN
	Fase 1.Inicio y Definición del Proyecto				
1	Identificación del problema	Christian & Jason	100%	20-10-25	22-10-25
1.1	Identificación de stakeholders clave	Christian & Jason	100%	22-10-25	22-10-25
1.2	Definición de roles y responsabilidades	Christian & Jason	100%	22-10-25	24-10-25
1.3	Definición del alcance del proyecto	Christian & Jason	100%	24-10-25	28-10-25
1.4	Definición de objetivos del proyecto	Christian & Jason	100%	28-10-25	29-10-25
1.5	Elaboración del caso de negocio / caso de estudio	Christian & Jason	100%	29-10-25	30-10-25
1.6	Presentación del caso de negocio	Christian & Jason	100%	30-10-25	1-11-25
1.7	Aprobación del caso de negocio	Gerencia	100%	1-11-25	3-11-25
1.8	Elaboración del acta del proyecto	Christian & Jason	100%	3-11-25	4-11-25
1.9	Aprobación del acta del proyecto	Gerencia	100%	4-11-25	6-11-25
1.1	Elaboración del plan de trabajo de alto nivel	Christian & Jason	100%	6-11-25	6-11-25
	Entregables				
	Caso de Negocio	Christian & Jason	100%	6-11-25	7-11-25
	Acta del Proyecto	Christian & Jason	100%	7-11-25	8-11-25

Nota: Elaborada por los autores

Fase 2. Investigación Preliminar – DIRKS Etapa A

La presente fase corresponde a la investigación preliminar del contexto organizacional y documental de la correduría. Su objetivo es comprender la situación actual del sistema de gestión documental, identificando los procesos, tipos documentales, herramientas utilizadas y prácticas vigentes. Esta etapa permite establecer un diagnóstico del estado actual (AS-IS) y evaluar el nivel de madurez documental de la organización, sirviendo como punto de partida para los análisis posteriores.

Figura 52: Fase 2 del Cronograma

SGD Diseño y Directrices

Seguro Total
Christian& Jason

Inicio del proyecto: lun, 10/20/2025
Semana para mostrar: 1

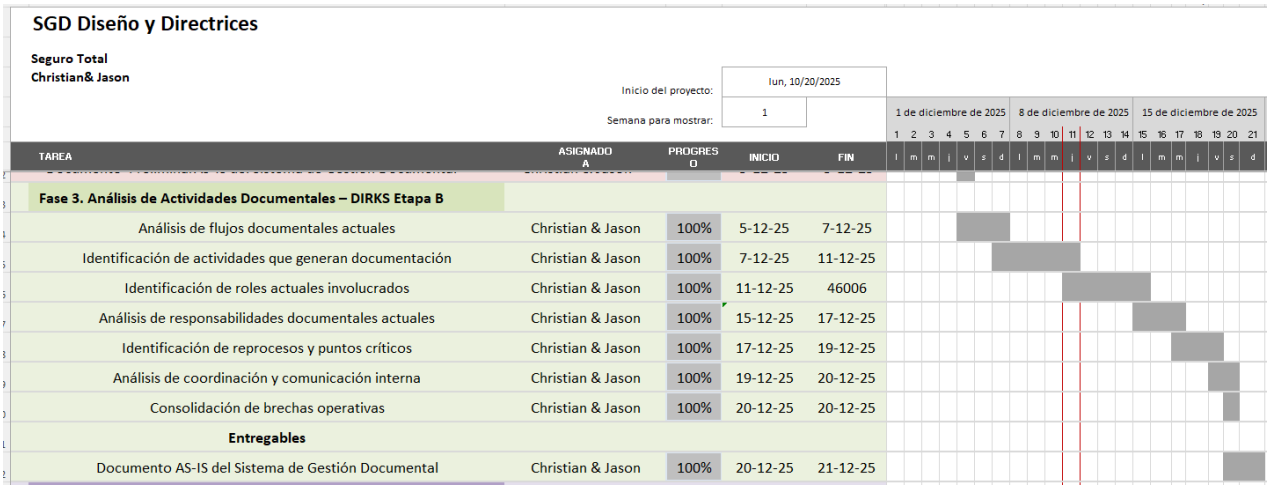
No	TAREA	ASIGNADO A	PROGRESO	INICIO	FIN
	Fase 2. Investigación Preliminar (AS-IS) – DIRKS Etapa A				
2	Levantamiento del contexto organizacional	Christian & Jason	100%	8-11-25	18-11-25
2.1	Identificación de procesos clave de la correduría	Christian & Jason	100%	18-11-25	21-11-25
2.2	Identificación de tipos documentales existentes	Christian & Jason	100%	21-11-25	26-11-25
2.3	Identificación de herramientas actuales de gestión documental	Christian & Jason	100%	26-11-25	27-11-25
2.4	Análisis de prácticas actuales de almacenamiento y uso documental	Christian & Jason	100%	27-11-25	28-11-25
2.5	Análisis del nivel de madurez documental	Christian & Jason	100%	28-11-25	1-12-25
2.6	Consolidación del diagnóstico de la situación actual	Christian & Jason	100%	1-12-25	5-12-25
	Entregables				
	Documento PreliminarAS-IS del Sistema de Gestión Documental	Christian & Jason	100%	5-12-25	5-12-25

Nota: Elaborada por los autores

Fase 3. Análisis de Actividades Documentales – DIRKS Etapa B

En esta fase se analizan de manera detallada las actividades operativas(diarias) que generan, utilizan o requieren documentación dentro de la correduría. Se revisan los flujos de trabajo, los roles involucrados y las responsabilidades actuales, así como también los puntos críticos y reprocesos existentes. Este análisis permite identificar aquellas brechas operativas y problemas de coordinación(comunicación), aportando los insumos necesarios para la definición de roles formales y la mejora de la gestión documental.

Figura 53: Fase 3 del Cronograma



SGD Diseño y Directrices

Seguro Total
Christian& Jason

Inicio del proyecto: lun, 10/20/2025
Semana para mostrar: 1

1 de diciembre de 2025 | 8 de diciembre de 2025 | 15 de diciembre de 2025
1 2 3 4 5 6 7 | 8 9 10 11 12 13 14 | 15 16 17 18 19 20 21
l m m j v s d | l m m j v s d | l m m j v s d

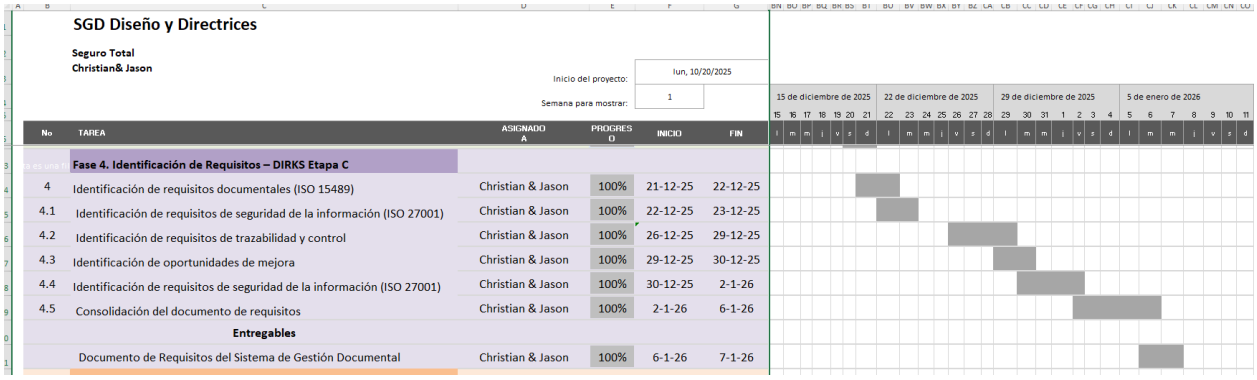
TAREA	ASIGNADO A	PROGRESO	INICIO	FIN
Fase 3. Análisis de Actividades Documentales – DIRKS Etapa B				
Análisis de flujos documentales actuales	Christian & Jason	100%	5-12-25	7-12-25
Identificación de actividades que generan documentación	Christian & Jason	100%	7-12-25	11-12-25
Identificación de roles actuales involucrados	Christian & Jason	100%	11-12-25	46006
Análisis de responsabilidades documentales actuales	Christian & Jason	100%	15-12-25	17-12-25
Identificación de reprocesos y puntos críticos	Christian & Jason	100%	17-12-25	19-12-25
Análisis de coordinación y comunicación interna	Christian & Jason	100%	19-12-25	20-12-25
Consolidación de brechas operativas	Christian & Jason	100%	20-12-25	20-12-25
Entregables				
Documento AS-IS del Sistema de Gestión Documental	Christian & Jason	100%	20-12-25	21-12-25

Nota: Elaborada por los autores

Fase 4. Identificación de Requisitos – DIRKS Etapa C

Esta fase tiene como objetivo identificar y consolidar los requisitos que debe cumplir el Sistema de Gestión Documental para Responder a las necesidades organizacionales y normativas. Se consideran los principios de autenticidad, integridad, disponibilidad y confiabilidad establecidos por la ISO 15489, los requisitos de gobernanza definidos por la ISO 30301 y los controles de seguridad de la información establecidos por la ISO 27001. A partir de este análisis se identifican oportunidades de mejora que orientan el diseño del sistema futuro.

Figura 54: Fase 4 del Cronograma



SGD Diseño y Directrices

Seguro Total
Christian& Jason

Inicio del proyecto: lun, 10/20/2025
Semana para mostrar: 1

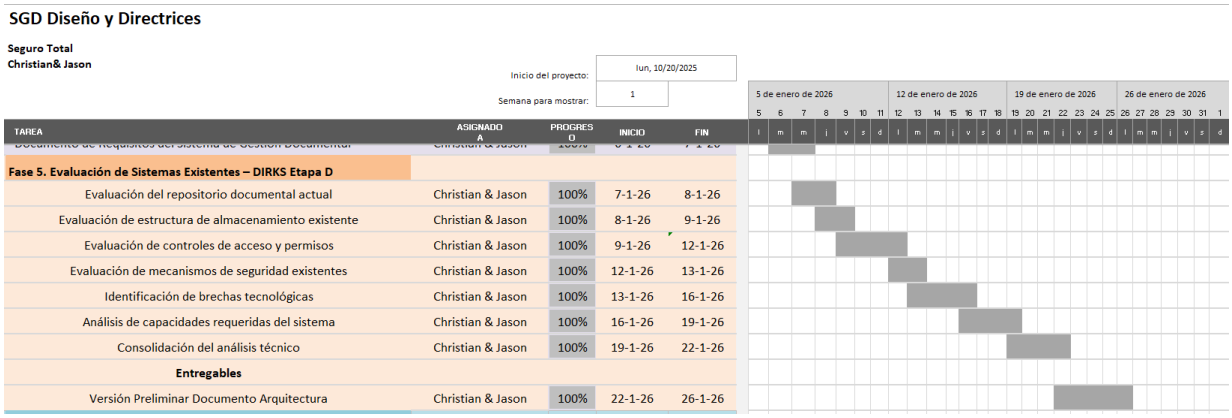
No	TAREA	ASIGNADO A	PROGRESO	INICIO	FIN
	Fase 4. Identificación de Requisitos – DIRKS Etapa C				
4	Identificación de requisitos documentales (ISO 15489)	Christian & Jason	100%	21-12-25	22-12-25
4.1	Identificación de requisitos de seguridad de la información (ISO 27001)	Christian & Jason	100%	22-12-25	23-12-25
4.2	Identificación de requisitos de trazabilidad y control	Christian & Jason	100%	26-12-25	29-12-25
4.3	Identificación de oportunidades de mejora	Christian & Jason	100%	29-12-25	30-12-25
4.4	Identificación de requisitos de seguridad de la información (ISO 27001)	Christian & Jason	100%	30-12-25	2-1-26
4.5	Consolidación del documento de requisitos	Christian & Jason	100%	2-1-26	6-1-26
	Entregables				
	Documento de Requisitos del Sistema de Gestión Documental	Christian & Jason	100%	6-1-26	7-1-26

Nota: Elaborada por los autores

Fase 5. Evaluación de Sistemas Existentes – DIRKS Etapa D

En esta fase se evalúan las herramientas y sistemas actualmente utilizados para la gestión documental, con énfasis en el repositorio digital y los controles de acceso y seguridad. Esta revaluación se apoyó de umbrales establecidos por normas internacionales con el propósito de determinar la capacidad de cumplir con los requisitos identificados y Detectar brechas tecnológicas o funcionales asociadas a los flujos de trabajo. Los resultados de esta evaluación sirven como base para justificar la arquitectura del sistema documental propuesto.

Figura 55: Fase 5 del Cronograma



SGD Diseño y Directrices

Seguro Total
Christian& Jason

Inicio del proyecto: lun, 10/20/2025
Semana para mostrar: 1

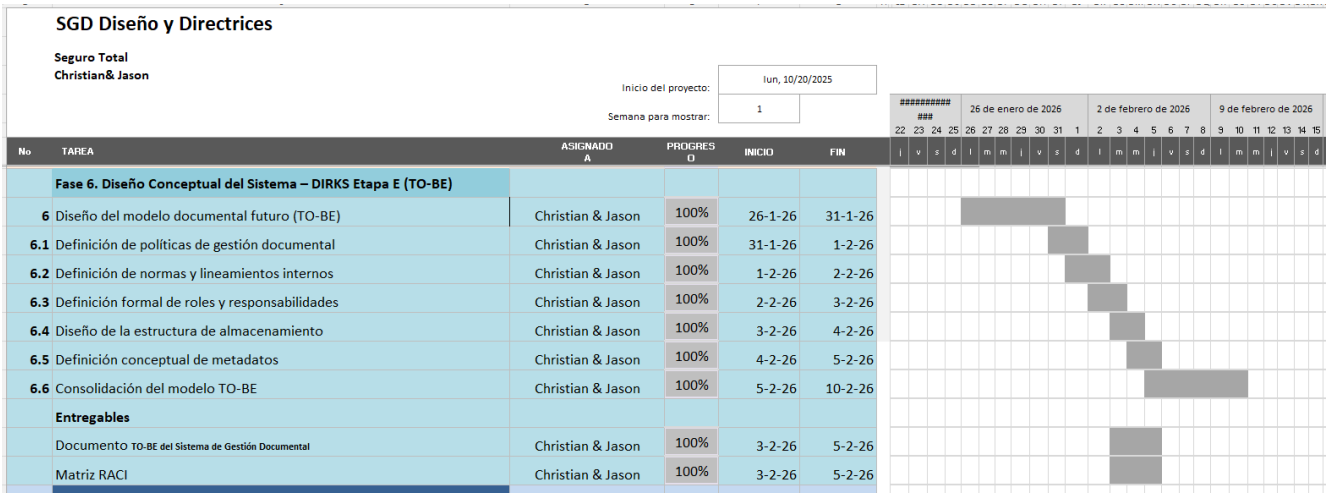
TAREA	ASIGNADO A	PROGRESO	INICIO	FIN
Fase 5. Evaluación de Sistemas Existentes – DIRKS Etapa D				
Evaluación del repositorio documental actual	Christian & Jason	100%	7-1-26	8-1-26
Evaluación de estructura de almacenamiento existente	Christian & Jason	100%	8-1-26	9-1-26
Evaluación de controles de acceso y permisos	Christian & Jason	100%	9-1-26	12-1-26
Evaluación de mecanismos de seguridad existentes	Christian & Jason	100%	12-1-26	13-1-26
Identificación de brechas tecnológicas	Christian & Jason	100%	13-1-26	16-1-26
Análisis de capacidades requeridas del sistema	Christian & Jason	100%	16-1-26	19-1-26
Consolidación del análisis técnico	Christian & Jason	100%	19-1-26	22-1-26
Entregables				
Versión Preliminar Documento Arquitectura	Christian & Jason	100%	22-1-26	26-1-26

Nota: Elaborada por los autores

Fase 6. Diseño Conceptual del Sistema – DIRKS Etapa E

Esta fase se centra en el diseño conceptual del Sistema de Gestión Documental futuro (TO-BE). Incluye la definición de políticas, normas internas, roles y responsabilidades, estructura de almacenamiento y lineamientos de metadatos. El diseño conceptual establece el marco normativo y organizacional que regirá el funcionamiento del sistema, asegurando su alineación con los estándares internacionales y con la realidad operativa de la correduría.

Figura 56: Fase 6 del Cronograma



SGD Diseño y Directrices

Seguro Total
Christian& Jason

Inicio del proyecto: lun, 10/20/2025
Semana para mostrar: 1

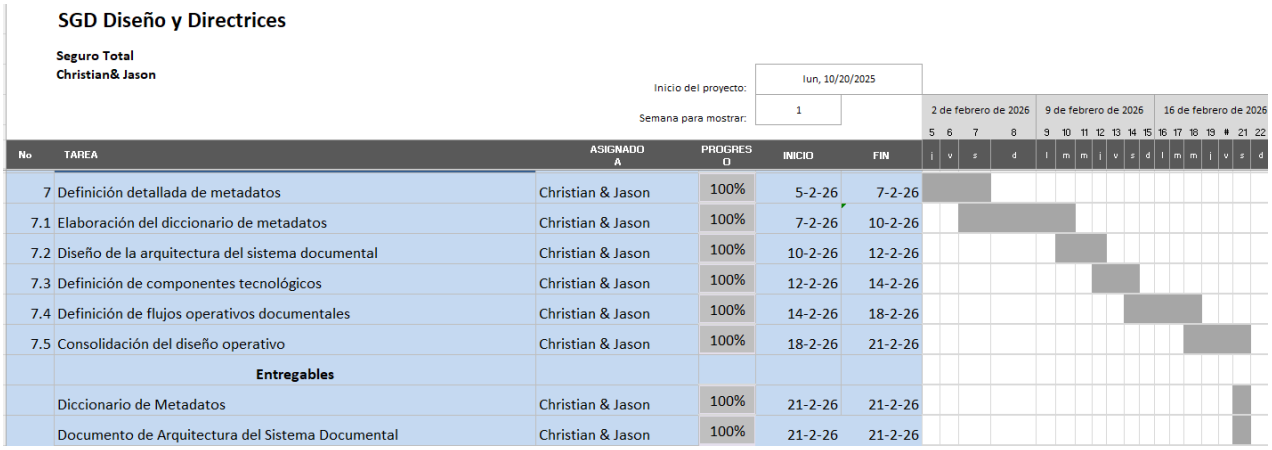
No	TAREA	ASIGNADO A	PROGRESO	INICIO	FIN
	Fase 6. Diseño Conceptual del Sistema – DIRKS Etapa E (TO-BE)				
6	Diseño del modelo documental futuro (TO-BE)	Christian & Jason	100%	26-1-26	31-1-26
6.1	Definición de políticas de gestión documental	Christian & Jason	100%	31-1-26	1-2-26
6.2	Definición de normas y lineamientos internos	Christian & Jason	100%	1-2-26	2-2-26
6.3	Definición formal de roles y responsabilidades	Christian & Jason	100%	2-2-26	3-2-26
6.4	Diseño de la estructura de almacenamiento	Christian & Jason	100%	3-2-26	4-2-26
6.5	Definición conceptual de metadatos	Christian & Jason	100%	4-2-26	5-2-26
6.6	Consolidación del modelo TO-BE	Christian & Jason	100%	5-2-26	10-2-26
	Entregables				
	Documento TO-BE del Sistema de Gestión Documental	Christian & Jason	100%	3-2-26	5-2-26
	Matriz RACI	Christian & Jason	100%	3-2-26	5-2-26

Nota: Elaborada por los autores

Fase 7. Diseño Operativo del Sistema – DIRKS Etapa F

En esta fase se desarrolla el diseño operativo del sistema documental, traduciendo el modelo conceptual en componentes técnicos y operativos concretos. Se define el diccionario de metadatos, la arquitectura del sistema, los flujos documentales y los elementos tecnológicos necesarios para su funcionamiento. Esta etapa permite dejar definido el sistema a un nivel suficiente para su futura implementación.

Figura 57: Fase 7 del Cronograma



SGD Diseño y Directrices

Seguro Total
Christian& Jason

Inicio del proyecto: lun, 10/20/2025
Semana para mostrar: 1

No	TAREA	ASIGNADO A	PROGRESO	INICIO	FIN
7	Definición detallada de metadatos	Christian & Jason	100%	5-2-26	7-2-26
7.1	Elaboración del diccionario de metadatos	Christian & Jason	100%	7-2-26	10-2-26
7.2	Diseño de la arquitectura del sistema documental	Christian & Jason	100%	10-2-26	12-2-26
7.3	Definición de componentes tecnológicos	Christian & Jason	100%	12-2-26	14-2-26
7.4	Definición de flujos operativos documentales	Christian & Jason	100%	14-2-26	18-2-26
7.5	Consolidación del diseño operativo	Christian & Jason	100%	18-2-26	21-2-26
	Entregables				
	Diccionario de Metadatos	Christian & Jason	100%	21-2-26	21-2-26
	Documento de Arquitectura del Sistema Documental	Christian & Jason	100%	21-2-26	21-2-26

Nota: Elaborada por los autores

6.18 CONCORDANCIA DE LOS SEGMENTOS DE LA TESIS CON LA PROPUESTA

Tabla 70: Concordancia de capítulos con tesis propuesta

Capítulo I			Capítulo II	Capítulo III				Capítulo 5	Capítulo VI	
Título de Investigación	**Objetivo General**	**Objetivos Específicos**	**Teorías de sustento**	**Metodología**	**Variables**	**Población**	**Técnicas**	**Conclusiones**	**Nombre de la Propuesta**	**Objetivos de la Propuesta**
Diseño de un Sistema Digital de Gestión Documental en MiPymes de Servicios Profesionales, estructurado con Normas ISO y Marco NIST de Ciberseguridad: Caso de Estudio	Diseñar un sistema digital de gestión documental centralizado que garantice la seguridad, accesibilidad y correcto manejo de información privada sensible, con las Normas ISO y como	Analizar los procesos actuales de gestión documental en la MiPyme Seguro Total para identificar riesgos y debilidades en el manejo de PII, contrastándolos con los principios de la ISO 15489 1:201	Normas ISO Cuarta Revolución Industrial	Cualitativo	Diseño del sistema digital de gestión documental bajo normas ISO y marco NIST de ciberseguridad.		Guía de entrevista semiestructurada Listas de verificación Observación Matriz de análisis de datos Matriz NIST	La organización cuenta con una base digital operativa, pero carece de controles formales y trazabilidad alineada a estándares internacionales.	Propuesta de estrategia de fortalecimiento de la gestión documental y la protección de la información en la empresa seguro total.	La organización cuenta con una base digital operativa, pero carece de controles formales y trazabilidad alineada a estándares internacionales.

Seguro Total Correduría de Seguros	referencia base el Marco NIST de Ciberseguridad que apoyea las MiPymes del rubro servicios profesionales aplicado a la Correduría de Seguro Total.	6 y ISO27001 y el Marco NIST de Ciberseguridad.								
		Evaluar herramientas o sistemas existentes que cumplan con los requisitos de las ISO 30301:2019, IS0 27001 y el Marco NIST de Ciberseguridad que permitan a Seguro Total tener un sistema estandarizad		Mixto	Herramientas de Gestión Documental		Entrevista semiestructurada Cuestionario abierto Matriz FODA	La organización cuenta con una base digital operativa, pero carece de controles formales y trazabilidad alineada a estándares internacionales.		La organización cuenta con una base digital operativa, pero carece de controles formales y trazabilidad alineada a estándares internacionales.

		o, seguro y escalable.								
		Evaluar una arquitectura de gestión documental alineada a los estándares de las ISO 15489 1:2016, ISO 30301 :2019 y ISO27 001 y bajo el Marco NIST de Ciberseguridad que sea resiliente, accesible y se integre con la gobernanza empresarial		Cualitativo	Arquitectura de Gestión Documental		Encuesta tipo Likert	La organización cuenta con una base digital operativa, pero carece de controles formales y trazabilidad alineada a estándares internacionales.		Se identificaron indicadores clave de desempeño (KPIs) para evaluar eficiencia, trazabilidad y seguridad de la gestión documental.

		de Seguro Total.								
		Evaluar y recomendar las funciones y categorías del Marco NIST de Ciberseguridad permiten a la MiPyme Seguro Total mejorar sus procesos actuales de gestión documental.		Mixto	Funciones Guía NIST para Pequeñas Empresas		Guía rápida NIST	La organización cuenta con una base digital operativa, pero carece de controles formales y trazabilidad alineada a estándares internacionales.		La organización cuenta con una base digital operativa, pero carece de controles formales y trazabilidad alineada a estándares internacionales.
		Identificar y proponer oportunidades de mejora en los proces		Cualitativo	Oportunidades de Mejora Proceso de Gestión Documenta		Entrevista semiestructurada Diagrama de procesos Matriz de	La organización cuenta con una base digital operativa, pero		Se definieron políticas y estrategias orientadas a fortalecer la

		os de gestión documental, tomando como referencia los requisitos de la ISO 30301:2019, las guías funcionales de la ISO 15489 y los controles de seguridad de la ISO/IEC 27001			1		análisis de datos	carece de controles formales y trazabilidad alineada a estándares internacionales.		protección de la información, la gobernanza documental y la continuidad del negocio.

Nota: Elaborada por los autores

REFERENCIAS BIBLIOGRÁFICAS

Adobe. (2023). *PDF y firma electrónica*. https://www.adobe.com/es/acrobat/resources/whatisdms.html

AIIM. (n.d.). *What is document management (DMS)?* https://www.aiim.org/whatisdocumentimaging

Alfresco. (n.d.). *Security, privacy, and compliance for government*. https://www.alfresco.com/es/industrias/government/securityprivacycompliance

Banco Interamericano de Desarrollo. (2020, 20 de octubre). *Apoyo a la modernización tecnológica de las MIPYME en Honduras*. https://www.iadb.org/es/proyecto/HOT1456

Banco Interamericano de Desarrollo. (2020, 20 de octubre). *Digitalización del sector del micro y pequeño emprendimiento – Digital Hub 504*. https://www.iadb.org/es/proyecto/HOG1256

Banco Interamericano de Desarrollo. (2020, 20 de octubre). *Digitalización del sector del micro y pequeño emprendimiento – Digital Hub 504*. https://www.iadb.org/es/proyecto/HOT1375

Banco Interamericano de Desarrollo. (2020, 20 de octubre). *Transformación digital para una mayor competitividad*. https://www.iadb.org/es/proyecto/HOL1202

Banco Interamericano de Desarrollo. (2024, 14 de febrero). *El poder de los datos: Impulsando la transformación digital de las pymes de América Latina*. https://blogs.iadb.org/innovacion/es/elpoderdelosdatosimpulsandolatransformaciondigitaldelaspymesdeamericalatina/

Bianchi, M. (2024). *SME digitalization in 2024*. OECD. https://www.oecd.org/digital/sme

Calderón, J. S. R., Pérez, N. P. G., & Villabona, M. V. (2021). *Insurtech Colombia 2021:*

Reflexiones del ecosistema asegurador.

https://revista.fasecolda.com/index.php/revfasecolda/article/view/755

Cárdenas Giler, D. X., Wilches Medina, A. M., Peñate Santana, Y., & Lozada Núñez, D. (2018). La gestión documental en la Universidad de Guayaquil: Situación actual y retos futuros. *Revista Espacios, 39*(43), 10.

https://www.revistaespacios.com/a18v39n43/18394310.html

Cardona Giraldo, L., Fajardo Sánchez, M. P., Yepes Molina, Y. E., & Viasus, E. (2023). *Implementación de tecnologías en el sector asegurador (Insurtech)*.

https://doi.org/10.26495/z64mt088

CEPAL. (2023). *CEPAL lanzó Observatorio de Desarrollo Digital para contribuir a la transformación digital de América Latina y el Caribe*.

https://www.cepal.org/es/comunicados/cepallanzoobservatoriodesarrollodigitalcontribuirlatransformaciondigitalamerica

Comisión Nacional de Bancos y Seguros. (2019). *Sistema de gestiones electrónicas de la CNBS*. Tegucigalpa, Honduras.

Comisión Nacional de Bancos y Seguros. (2022). *Normas para la gestión de tecnologías de información, ciberseguridad y continuidad del negocio*. Tegucigalpa, Honduras.

Concepto. De. (2025, 11 de septiembre). *Fuentes de información: Qué son, tipos y ejemplos*.

https://concepto.de/fuentesdeinformacion/

Consultoría de Procesos. (2015, 28 de diciembre). *Arquitectura empresarial*.

https://gestionprocesosblog.wordpress.com/2015/12/30/arquitecturaempresarial/

Cordero Guzmán, A. (2015). *La gestión documental del sistema de gestión de calidad*. Universidad de La Habana.

https://revistas.unah.edu.cu/index.php/cu/article/download/1436/2665/5714

CrowdStrike. (2025, 27 de febrero). *2025 global threat report*.

https://www.crowdstrike.com/en-us/global-threat-report/

DanaConnect. (2024). *Descripción general regulatoria de las firmas digitales y electrónicas en América Latina: Un análisis detallado*. https://www.danaconnect.com/regulatoryoverviewofdigitalandelectronicsignaturesinlatinamericaadetailedanalysis/

De Lucca Caetano, B. (2025, 17 de junio). *M-Files QMS (Quality Management System)*. SimplerQMS. https://simplerqms.com/m-files-qms/

Dirección General de Gobierno Digital. (2024). *Plan Nacional de Gobierno Digital 2023–2026*. https://www.diger.gob.hn/sites/default/files/202402/Plan%20de%20Gobierno%20Digital%20Honduras.pdf

DocuWare Europe GmbH. (n.d.). *Compliance & certifications*. https://start.docuware.com/compliance-and-certifications

Docunecta. (2019, 11 de junio). *Gestión documental en las PYMES: Claves para mejorar*. https://www.docunecta.com/blog/gestion-documental-en-las-pymes

Dropbox. (n.d.). *Security with Dropbox*. https://www.dropbox.com/business/trust/security

Edicom. (2024, 12 de septiembre). *Enmiendas a la Ley de Firma Digital de Argentina*. https://edicomgroup.com/blog/digital-signature-argentina

Ekon. (2025, 21 de enero). *Diagrama de procesos y su importancia para tu empresa*. https://www.ekon.es/blog/diagrama-procesos-empresa/

European Commission. (2024, julio). *Industry 5.0*. https://research-and-innovation.ec.europa.eu/research-area/industrial-research-and-innovation/industry-50_en

Fortinet. (2025). *¿Qué es la tríada del CID y por qué es importante?* https://www.fortinet.com/lat/resources/cyberglossary/ciatriad

Gartner. (2024, 18 de diciembre). *Magic Quadrant for Document Management Applications*.

https://sergroup.com/en/knowledge-center/analysis-reports/gartner.html

Gómez, J. E., & Caro, M. F. (2022). *Transformación digital en las pymes: Un análisis desde la perspectiva de los recursos y capacidades*. https://dialnet.unirioja.es/servlet/articulo?codigo=8890768

GS1 US. (n.d.). *GS1 US marks 50 years, advances next-gen barcodes*. https://www.gs1us.org/industries-and-insights/media-center/press-releases

Hyland Software, Inc. (2022). *Alfresco Content Services datasheet*. https://www.hyland.com/media/project/hyland/common/pdfs/factsheet/2022_acs_contentservices_datasheet.pdf

IBM. (2024, 11 de octubre). *Ciberseguridad*. https://www.ibm.com/es-es/topics/cybersecurity

International Organization for Standardization. (2016). *ISO 15489-1: Information and documentation—Records management—Part 1*. ISO.

La Gaceta. (2013). *Ley sobre firmas electrónicas*. https://www.sefin.gob.hn/wp-content/uploads/2020/11/Ley_firmas_electronicas_2013.pdf

Laoyan, S. (2025, 12 de febrero). *Metodologías de mejora de procesos y cómo hacer una propuesta*. Asana. https://asana.com/es/resources/process-improvement-methodologies

McKinsey & Company. (2018, 29 de octubre). *Unlocking success in digital transformations*. https://www.mckinsey.com/capabilities/people-and-organizational-performance/our-insights/unlocking-success-in-digital-transformations

Microsoft. (n.d.). *Cloud data integrity and compliance*. Microsoft Trust Center. https://www.microsoft.com/en-us/trustcenter

Mountain, I. (2025). *How to choose the right digital document management system (DMS)*. Iron Mountain. https://www.ironmountain.com/en-au/resources/blogs-and-articles/h/how-to-choose-the-right-digital-document-management-system-dms

National Institute of Standards and Technology. (2020). *Security and privacy controls for*

information systems and organizations (SP 800-53 Rev. 5).

https://doi.org/10.6028/nist.sp.800-53r5

Novatech. (2025, 28 de agosto). *Secure and compliant: Using DocuWare's power for information security and regulatory compliance*. https://novatech.net/blog/secure-and-compliant-using-docuwares-power-for-information-security-and-regulatory-compliance

OECD. (2023, 3 de mayo). *Habilidades en América Latina*. https://www.oecd.org/en/publications/skills-in-latin-america_5ab893f0-en.html

Onfinity. (2025). *Document management system overview*. https://onfinity.io/es/dms-overview.php

OpenKM. (n.d.). *Document management system software*. https://www.openkm.com/

Papertrail. (2024, 19 de agosto). *What are the key functions of a document management system?* https://www.egissoftware.com/key-functions-of-a-document-management-system/

Paulhickey. (2025, 6 de julio). *M-Files compliance*. https://www.m-files.com/m-files-compliance/

Paulhickey. (2025, 2 de noviembre). *Partners*. https://www.m-files.com/partners/

Schwab, K. (2020). *The Fourth Industrial Revolution*. World Economic Forum.

Trust Center. (n.d.). *Security, privacy, and compliance*. Google Cloud. https://cloud.google.com/trustcenter

Udoagwu, K. (2025, 7 de agosto). *What is a document management system (DMS)?* Wrike. https://www.wrike.com/blog/what-is-document-management-system/

World Bank. (2021). *Transformación digital inclusiva en América Latina*. https://live.worldbank.org/en/event/2023/beyond-connectivity-inclusive-digital-transformation-latin-america-and-caribbean

Yarasca Chávez, S. (2024). *Efectos de la norma ISO 15489 en la gestión documental de una institución pública*. Universidad Nacional Agraria La Molina.

https://repositorio.lamolina.edu.pe/items/fc216b8d852c4813afb84c32f1a753ce

ANEXO 2: CARTA AUTORIZACIÓN DE LA EMPRESA

ANEXO 3: INSTRUMENTOS METODOLOGÍA DIRKS

Proceso/Actividad	Tipo de Documento	Responsable de Generación	Formato	Tiempo de Retención	Disposición Final	Norma/Referencia

ANEXO 4: INSTRUMENTOS METODOLOGÍA GUÍA NIST PARA PYMES 2.0

Establecimiento del contexto organizativo	
Nuestra misión empresarial:	
¿Qué riesgos de seguridad cibernética pueden impedirnos lograr esta misión?	

Documentación de los requisitos de seguridad cibernética	
Enumere sus requisitos legales:	
Enumere sus requisitos normativos:	
Enumere sus requisitos contractuales:	

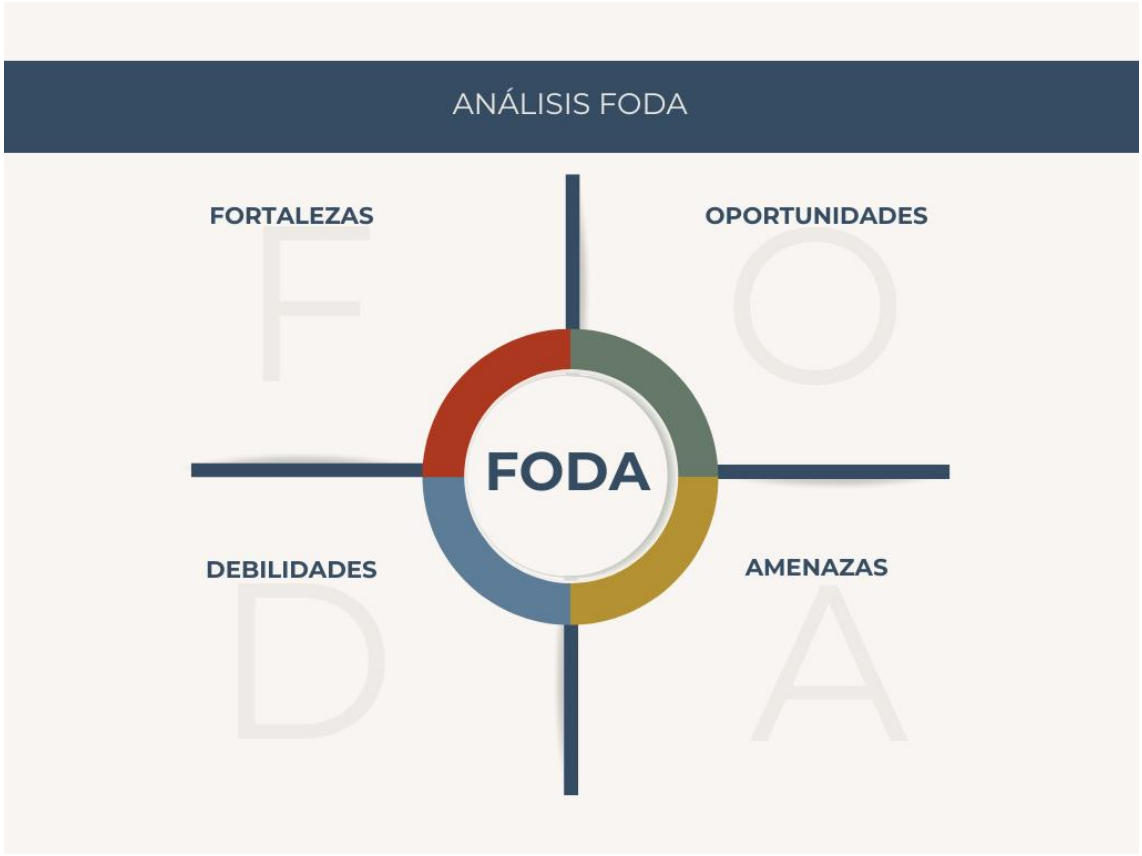
Software/ hardware/ sistema/ servicio	Uso oficial del activo	Administrador o propietario del activo:	Identifique los datos sensibles a los que tiene acceso el activo:	¿Se requiere autenticación de múltiples factores para acceder a este activo?	Riesgo para la empresa si perdemos el acceso a este activo

Account	MFA habilitado (sí/no)
Cuenta(s) bancaria(s)	
Cuenta(s) contable(s) y fiscal (es	
Cuenta(s) comercial (es	
Cuentas de Google, Microsoft y/o ID de Apple	
Cuenta(s) de correo electrónico Gestor(es) de	
Cuentas de sitios web	

ANEXO 5: LISTA DE VERIFICACIÓN NIST MARCO DE CIBERSEGURIDAD

COMPONENTES DEL NÚCLEO			PERFIL ACTUAL	PERFIL OBJETIVO
FUNCIÓN	CATEGORÍA	SUBCATEGORÍA	NIVEL	NIVEL

ANEXO 6: FODA



ANEXO 7: CUESTIONARIO

unitec®
Universidad Tecnológica Centroamericana

Gestión Documental y Manejo de Información en MiPymes del Sector Asegurador

Esta encuesta tiene como objetivo conocer
su opinión y experiencia sobre la forma en que la empresa organiza protege y utiliza los documentos e información. Sus respuestas son muy importantes para identificar áreas de mejora y fortalecer la manera en que se maneja la

información en la empresa.

La información que usted proporcione en esta encuesta será tratada con estricta confidencialidad.
Sus respuestas serán utilizadas únicamente con fines académicos y de investigación. No se recopilarán nombres ni datos personales que permitan identificarle directamente. Los resultados serán analizados de forma agregada y anónima, sin mencionar a personas específicas.

* Indica que la pregunta es obligatoria

Sección A: Datos Demográficos

1. 1. Edad: *

Selecciona todos los que corresponden.

- [ ] 21 30 años.
- [ ] 3140 años.
- [ ] 4150 años.
- [ ] 5160 años.
- [ ] 61 o más.

2. 2. Género: *

Marca solo un óvalo.

- Masculino
- Femenino

3. 3. Nivel educativo: *

Marca solo un óvalo.

- Secundaria

Técnico

Universitario o Posgrado

4. 4. Tiempo de trabajar en la empresa: *

Selecciona todos los que corresponden.

- [ ] Menos de 2 años
- [ ] 24 años
- [ ] 47 años
- [ ] Más de 7 años

Sección B: Conocimiento General

5. 1. ¿Ha escuchado hablar de las normas ISO relacionadas con empresas y organizaciones? *

Marca solo un óvalo.

- Sí *Salta a la pregunta 6*
- No *Salta a la pregunta 18*

ANEXO 8: ENTREVISTA SEMIESTRUCTURADA PARA DIRECTIVOS

MAESTRÍA EN GESTIÓN DE TECNOLOGÍAS DE LA INFORMACIÓN

Diseño de un Sistema Digital de Gestión Documental en MiPymes de Servicios Profesionales, estructurado con Normas ISO y Marco NIST de Ciberseguridad: Caso de Estudio Seguro Total Correduría de Seguros

Objetivo:
Diseñar un Sistema Digital de Gestión Documental en MiPymes de Servicios Profesionales, estructurado con Normas ISO y el Marco de Ciberseguridad NIST, tomando como caso de estudio a Seguro Total Correduría de Seguros.

Contexto:
Su participación y respuestas como entrevistado son de gran valor para esta investigación académica. Se solicita su mayor colaboración, procurando que sus aportes sean claros, completos y reflejan la realidad actual de la organización en materia de gestión documental y seguridad de la información.

Participación Voluntaria:
La participación en esta entrevista es totalmente voluntaria. Usted tiene la libertad de no Responder a alguna de las preguntas planteadas o retirarse de la sesión en cualquier momento, sin que ello genere inconvenientes.

Duración:
La entrevista tendrá una duración aproximada de 25 a 45 minutos, dependiendo del nivel de detalle de sus aportes.

Confidencialidad:
Toda la información compartida en el marco de esta entrevista será tratada de manera

confidencial, utilizada únicamente para fines académicos en el desarrollo de la presente tesis. Se mantendrá en todo momento el anonimato de los participantes.

Beneficios y Riesgos:

- **Riesgos:** No existen riesgos directos asociados a su participación en esta actividad.
- **Beneficios:** Entre los beneficios se pueden destacar:
    - Contribuir a identificar áreas de mejora en los procesos de gestión documental digital en Pymes.
    - Proponer soluciones que fortalezcan la seguridad de la información, la eficiencia operativa y el cumplimiento normativo bajo estándares internacionales (ISO y NIST).
    - Generar un insumo académico que puede servir como referencia futura para la organización en la mejora continua de sus prácticas documentales.

Consentimiento:
Se solicita que firme este documento para confirmar que comprende los detalles descritos, que está conforme en participar en la entrevista.

Firma del Participante: _____
Fecha: _____

Preguntas para directores – Gestión Documental

Preguntas	Respuesta
¿Cuáles considera que son las principales fortalezas del sistema actual de gestión documental en la organización?	
¿Qué debilidades o limitaciones observa en los procesos de gestión documental que deberían atenderse prioritariamente?	
Desde su perspectiva, ¿cómo ha impactado la digitalización de documentos en la eficiencia de su área o de la organización en general?	
¿Qué riesgos de seguridad percibe en el manejo actual de documentos y qué medidas propondría para reducirlos?	
¿Qué indicadores o métricas considera más relevantes para evaluar la efectividad de la gestión documental?	
¿Qué retos principales enfrenta la organización para lograr una gestión documental más eficiente?	
¿Qué beneficios específicos ha observado en la implementación de sistemas digitales de gestión documental?	
¿Qué nivel de inversión o recursos considera necesarios para fortalecer la gestión documental en la organización?	
¿Qué acciones de capacitación cree necesarias para que el personal utilice de forma adecuada los sistemas de gestión documental?	
¿Cómo imagina la gestión documental ideal en la	

organización dentro de los próximos 3 a 5 años?	

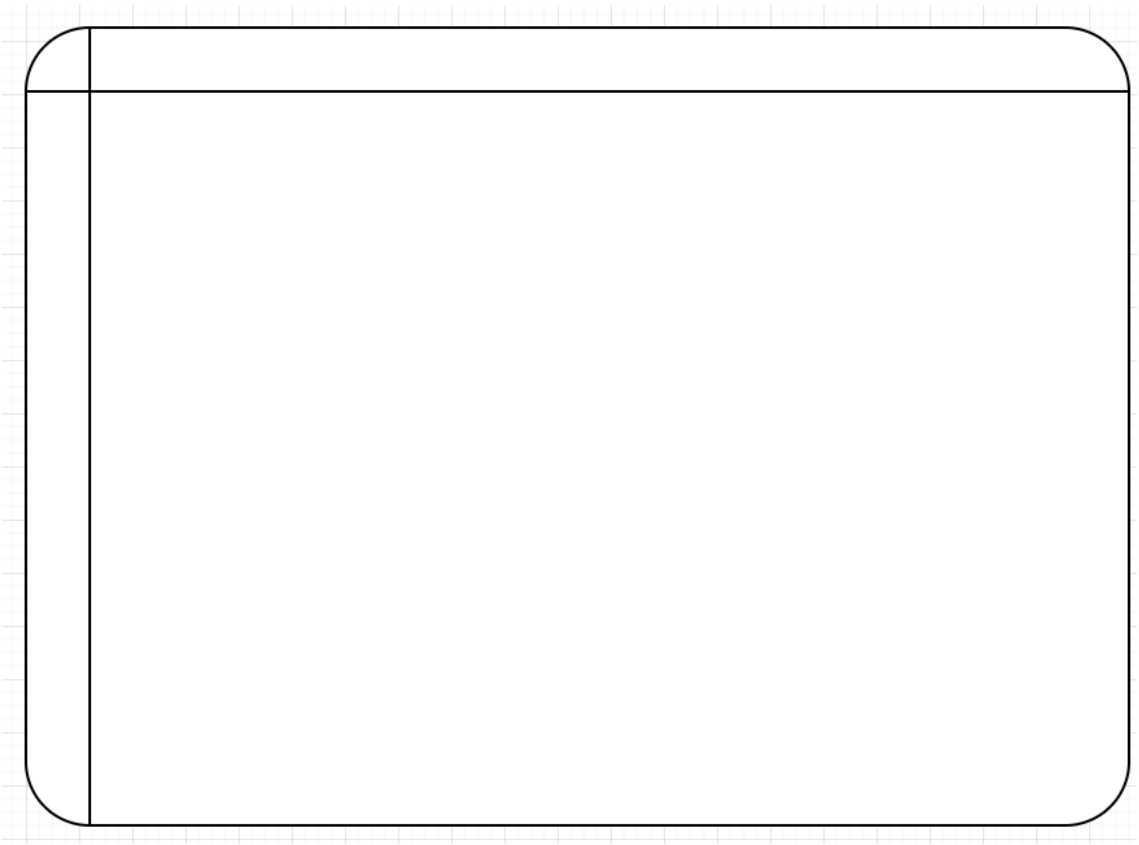
ANEXO 9: MATRIZ DE ANÁLISIS DE DATOS

Instrumento	Sección	Pregunta	Participante X	Participante X

ANEXO 10: FLUJOS DE PROCESOS

Diseño de un Sistema Digital de Gestión Documental en MiPymes de Servicios Profesionales, estructurado con Normas ISO y Marco NIST de Ciberseguridad: Caso de Estudio Seguro Total Correduría de Seguros

Diagramas de Procesos:



ANEXO 11: MATRIZ DE EVALUACIÓN DE HERRAMIENTAS

Herramienta	Seguridad	Facilidad de Uso	Inversión Inicial	Actualizaciones	Cumplimiento Normativo	Experiencia del Usuario	Funcionalidades Claves

ANEXO 12: LISTA DE VERIFICACIÓN ISO 15489

Lista de verificación basada en los principios y directrices de la norma ISO 15489, para evaluar la gestión documental a lo largo del ciclo de vida de los documentos.

N.º	Elemento por verificar	Cumple (Sí/No/En Progreso)	Comentarios / Evidencias
1	La organización tiene una política de gestión documental aprobada por la dirección.		
2	Se identifican los requisitos legales, regulatorios y normativos aplicables.		
3	Existen responsables designados para la gestión documental en todas las áreas.		
4	Los documentos creados son completos, auténticos y fiables.		

N.º	Elemento por verificar	Cumple (Sí/No/En Progreso)	Comentarios / Evidencias
5	Los procedimientos para la captura y registro de documentos están implementados.		
6	Los documentos tienen metadatos asignados (autor, fecha, asunto, clasificación).		
7	Existe un esquema de clasificación documental aprobado y actualizado.		
8	Se aplican reglas de acceso y confidencialidad a los documentos.		
9	Los documentos son recuperables de manera eficiente por usuarios autorizados.		
10	Los documentos están protegidos contra pérdida, acceso no autorizado o destrucción.		
11	Se mantienen copias de seguridad y planes de contingencia para documentos críticos.		
12	Almacenamiento físico y digital cumple condiciones de seguridad y conservación.		
13	Existe un calendario de conservación y disposición documental.		
14	Se aplican procesos documentados para eliminación o transferencia a archivo histórico.		
15	Se realizan auditorías o revisiones periódicas del sistema de gestión documental.		
16	Política y procedimientos de gestión documental se revisan y actualizan regularmente.		
17	El personal recibe capacitación en gestión de documentos.		
18	Se utilizan indicadores o métricas de eficacia en la gestión documental.		
19	Se fomenta la mejora continua en la gestión documental.		

ANEXO 13: LISTA DE VERIFICACIÓN ISO 30301

Lista de verificación basada en los requisitos de la norma ISO 30301, enfocada en la implementación de un Sistema de Gestión de Documentos (SGD).

N.º	Elemento por verificar	Cumple (Sí/No/En Progreso)	Comentarios / Evidencias
1	Se ha definido el contexto interno y externo de la organización en relación con los documentos.		
2	Se han identificado las partes interesadas y sus requisitos respecto a los documentos.		
3	Está definido el alcance del Sistema de Gestión de Documentos (SGD).		

N.º	Elemento por verificar	Cumple (Sí/No/En Progreso)	Comentarios / Evidencias
4	Existe una política de gestión documental comunicada en toda la organización.		
5	La alta dirección demuestra liderazgo y compromiso con el SGD.		
6	Roles, responsabilidades y autoridades para el SGD están claramente definidos.		
7	Se han identificado riesgos y oportunidades relacionados con la gestión documental.		
8	Existen objetivos medibles para la gestión documental y planes para lograrlos.		
9	Se asignan recursos suficientes (humanos, tecnológicos, financieros).		
10	El personal tiene competencia y recibe formación en gestión documental.		
11	Existe concientización sobre la importancia de los documentos.		
12	Se definen y mantienen los canales de comunicación interna y externa sobre gestión documental.		
13	Se mantiene la documentación necesaria para el SGD (‘información documentada’).		
14	Los procesos de gestión documental están planificados y controlados.		
15	Se determinan los documentos que deben crearse, conservarse y cómo hacerlo.		
16	Se implementan controles y sistemas para la gestión documental de forma efectiva.		
17	Se monitorean y miden los procesos del SGD.		
18	Se realizan auditorías internas al SGD.		
19	La alta dirección revisa regularmente el sistema de gestión documental.		
20	Se gestionan no conformidades y acciones correctivas para el SGD.		
21	Se promueve la mejora continua del SGD.		

ANEXO 14: LISTA DE VERIFICACIÓN ISO 27001

Lista de verificación basada en los requisitos de la norma ISO 27001, enfocada en la implementación de un Sistema de Gestión de Documentos (SGD) y adaptada al rubro de MiPymes de Servicios Profesionales.

N.º	Control adaptado	Aplicado (Sí/No)	Observaciones

1	La empresa cuenta con políticas internas de confidencialidad y resguardo de datos de clientes asegurados.		.
2	Se han definido roles de seguridad de la información, incluyendo al responsable ante la CNBS.		
3	Existe un inventario actualizado de sistemas críticos: plataforma de emisión de pólizas, CRM, bases de datos de clientes.		
4	El acceso a sistemas de pólizas y bases de datos está restringido por roles y autenticación multifactorial.		
5	Se gestionan vulnerabilidades en aplicaciones de clientes (web y móviles) y se validan con pruebas periódicas de seguridad.		
6	Los datos personales y financieros de los asegurados se encuentran cifrados en reposo y en tránsito.		
7	Se realizan pruebas de penetración enfocadas en portales de clientes y sistemas de pago electrónico.		
8	Se cuenta con un registro de incidentes relacionados con fraude digital, fuga de datos o caídas de sistemas.		
9	La organización revisa periódicamente los controles de seguridad conforme a ISO 27001, Ley de Protección de Datos y normativa CNBS.		