Propuesta para la Implementación de la Norma ISO 27001 en el Archivo Central de la Gobernación del Departamento del Magdalena

Lourdes María Campo Cucunuba

Universidad De La Salle

Maestría en Gestión de la Información Documental

Bogotá D.C. 2024

Propuesta para la Implementación de la Norma ISO 27001 en el Archivo Central de la Gobernación del Departamento del Magdalena

Lourdes María Campo Cucunuba

Trabajo de Grado para Optar el Titulo de Magister en Gestión de la Información Documental

Director

Nelson Javier Pulido Daza

Universidad De La Salle

Maestría en Gestión de la Información Documental

Bogotá D.C. 2024

Nota de Aceptación

_____

_____

_____

_____

_____

_____

Firma del Director

_____

Firma del Jurado

_____

Firma del Jurado

_____

Dedicatoria

Dedico este triunfo que he adquirido a la divinidad porque me ha dado la vida, las fuerzas y los medios para culminar mi carrera. A mis profesores por su sabiduría y guía constante de aprendizaje, a mis compañeros que han sido la motivación para todos los esfuerzos, aún en los momentos más difíciles he sentido apoyo y la enseñanza que he necesitado para realizarme como profesional. A mis hijas Mariluz y Brady les dedico este triunfo por creer en mí, gracias por impulsarme a dar siempre lo mejor de mí.

Resumen

La investigación se centra en la implementación de la Norma ISO 27001 en el Archivo Central de la Gobernación del Magdalena, con el objetivo de garantizar la seguridad de la información, esta se fundamenta en el marco teórico de la norma ISO 27001 y en las normativas archivísticas vigentes, como la Ley 594/2000 y el Decreto 2609/2012, su metodología propuesta sigue el ciclo PHVA, abarca la planificación, la evaluación de riesgos, la definición de políticas y procedimientos, y la capacitación del personal, entre los resultados se evidencian la viabilidad y necesidad de la implementación, al destacar la identificación de riesgos y presenta un plan detallado para su ejecución; la propuesta incluye una implementación por fases conforme al ciclo PHVA, integrando el sistema INFODOC y la infraestructura física del archivo central.

Palabras claves: Seguridad de la Información, Sistema de Gestión, Infraestructura Tecnológica y Gobernación del Magdalena

Abstract

The research focuses on the implementation of the ISO 27001 Standard in the Central Archive of the Government of Magdalena, with the objective of guaranteeing the security of the information, this is based on the theoretical framework of the ISO 27001 standard and archival regulations. current, such as Law 594/2000 and Decree 2609/2012, its proposed methodology follows the PHVA cycle, encompasses planning, risk assessment, definition of policies and procedures, and staff training, among the results are evident the feasibility and necessity of implementation, highlighting the identification of risks and presenting a detailed plan for their execution; The proposal includes a phased implementation according to the PHVA cycle, integrating the INFODOC system and the physical infrastructure of the central archive.

Keywords: Information Security, Management System, Technological Infrastructure and Government of Magdalena

Tabla de contenido

Tabla de figuras

Indice de tablas

Introducción

El Archivo Central de la Gobernación del Departamento del Magdalena, que contiene una vasta colección de documentos históricos y administrativos, enfrenta desafíos significativos en la protección de la información debido a la falta de un sistema de seguridad robusto. En un contexto de creciente digitalización y amenazas cibernéticas, la Norma ISO 27001 emerge como una solución integral para mejorar la seguridad de la información, proporcionando un marco para proteger los datos contra accesos no autorizados, pérdidas y alteraciones. A pesar de la legislación nacional que enfatiza la seguridad documental, como la Ley 594/2000 y el Decreto 2609/2012, el archivo aún carece de una infraestructura adecuada que garantice la integridad y confidencialidad de sus documentos.

El objetivo principal de esta investigación es implementar la Norma ISO 27001 en el Archivo Central para fortalecer la seguridad de la información. Esto incluye evaluar el estado actual de la seguridad, identificar riesgos y vulnerabilidades, diseñar un plan de implementación, desarrollar políticas y procedimientos específicos, y capacitar al personal en prácticas de seguridad. La hipótesis del estudio es que la aplicación de la norma mejorará significativamente la protección de la información y ayudará a cumplir con las regulaciones vigentes.

Este estudio es para mejorar la seguridad de datos sensibles en una entidad gubernamental, fortaleciendo la confianza pública y estableciendo un modelo para otras instituciones similares. La metodología incluirá una combinación de revisión documental, encuestas y análisis de riesgos, con la implementación de la norma en fases y auditorías internas para evaluar la eficacia del Sistema de Gestión de Seguridad de la Información (SGSI). El documento se estructurará en capítulos que abarcarán desde la introducción hasta la evaluación y conclusiones, buscando proporcionar directrices claras y adaptadas a las necesidades del archivo

Esta investigación busca establecer una base sólida para la mejora de la seguridad de la información en el Archivo Central de la Gobernación del Departamento del Magdalena, proporcionando directrices claras y prácticas adaptadas a las necesidades específicas de la entidad, y contribuyendo al fortalecimiento de la gestión documental en el sector público.

1. Capítulo, Problema de Investigación

En la actualidad, la protección de la información es esencial para garantizar la integridad y confidencialidad de los datos en las organizaciones, el Archivo Central de la Gobernación del Magdalena enfrenta una problemática significativa debido a la falta de implementación de la norma ISO 27001, un estándar internacional clave para la gestión de la seguridad de la información. Esta ausencia expone a la entidad a diversos riesgos, derivados de causas como la falta de concienciación sobre la importancia de la seguridad de la información, recursos financieros limitados y resistencia al cambio organizacional.

Este capítulo aborda en profundidad las causas y consecuencias de la falta de implementación de ISO 27001, destacando cómo estas deficiencias afectan la protección de datos sensibles y la eficiencia operativa. La investigación busca responder a la pregunta central: ¿Qué elementos deben ser considerados en la propuesta de implementación de la norma ISO 27001 en el archivo central de la Gobernación del Departamento del Magdalena? los objetivos incluyen diagnosticar debilidades en el sistema actual, comparar las prácticas existentes con los requisitos de la norma y estructurar una propuesta integral para su implementación.

1.1. Planteamiento del Problema

La falta de implementación de la norma ISO 27001 en el Archivo Central de la Gobernación del Magdalena es un problema que tiene múltiples causas y consecuencias, en términos de causas, una de las principales es la falta de conciencia sobre la seguridad de la información, muchos empleados no comprenden el valor de proteger la información y los riesgos asociados a su manejo inadecuado. La ausencia de campañas de concientización efectivas y continuas agrava esta situación, ya que, sin una formación adecuada, el personal no puede adoptar prácticas seguras.

Los recursos limitados para la implementación de ISO 27001 representan otro obstáculo crítico, la certificación y mantenimiento de esta norma requieren una inversión considerable en términos de presupuesto, herramientas tecnológicas y capacitación. Sin estos recursos, es difícil establecer y mantener los controles necesarios para garantizar la seguridad de la información.

Otra causa significativa es la resistencia al cambio y el liderazgo inadecuado dentro de la organización, la implementación de nuevas políticas y procedimientos puede generar oposición entre el personal, especialmente si no se comunica de manera efectiva la necesidad y los beneficios de estos cambios, si el liderazgo no está comprometido con la seguridad de la información, es probable que falte el impulso necesario para llevar a cabo la implementación de ISO 27001.

Las consecuencias de la falta de implementación de esta norma son igualmente preocupantes, un efecto inmediato es el escaso compromiso del personal para adoptar prácticas de seguridad de la información, lo que puede resultar en la pérdida o filtración de datos sensibles. Además, la carencia de personal especializado en seguridad de la información dificulta la identificación y mitigación de riesgos, exponiendo a la organización a posibles incidentes de seguridad.

La resistencia a la implementación de nuevas políticas y procedimientos puede causar retrasos significativos, afectando la eficiencia operativa y creando un ambiente laboral negativo, acá se ahonda en sus posibles consecuencias, en primer lugar, la creciente necesidad de la seguridad de la información en la era digital destaca la urgencia de proteger la integridad, confidencialidad y disponibilidad de los datos y documentos, el cumplimiento con estándares internacionales como ISO 27001 garantiza la seguridad de la información y el respeto de las regulaciones.

En segundo lugar, la relevancia de este problema se acentúa por la cantidad de datos sensibles y confidenciales que maneja el archivo central de la Gobernación del Magdalena, lo que requiere una protección adecuada; La falta de medidas de seguridad adecuadas podría exponer a la Gobernación a riesgos significativos, como la pérdida de datos o daños a la reputación, el siguiente árbol de problemas lo explica:

Figura 1, Causas y consecuencias del problema

Causas	**Falta de conciencia sobre la de la seguridad de la información**	**Recursos limitados para la implementación de ISO 27001**	**Resistencia al cambio y falta de liderazgo inadecuado en la organización**
Problema central	**Falta de Implementación de la Norma ISO 27001 en el Archivo Central de la Gobernación del Magdalena**		
Efectos	Escaso compromiso del personal para adoptar prácticas de seguridad de la información.	Carencia de personal especializado en seguridad de la información.	Personal que se opone a la implementación de nuevas políticas y procedimientos de seguridad.

Nota: Se muestran las causas y consecuencias halladas en relación con el problema, autoría propia.

Para finalizar, la implementación de ISO 27001 minimizaría riesgos, y también mejoraría la eficiencia operativa al estandarizar los procesos relacionados con la seguridad de la información, al fortalecer la confianza de las partes interesadas en la Gobernación. En conjunto, estos argumentos respaldan la necesidad de abordar este problema de investigación para garantizar una gestión efectiva de la seguridad de la información en el archivo central de la Gobernación del Magdalena.

Con lo anterior, en la actualidad desde una perspectiva global, la seguridad de la información en los archivos se ha vuelto un tema de suma importancia debido a diversos factores globales, uno de los motivos principales es el aumento de las amenazas cibernéticas, con el crecimiento de la tecnología, los ciberdelincuentes han intensificado sus ataques, convierten los archivos en objetivos valiosos y la falta de seguridad adecuada podría resultar en la pérdida o robo de datos (Martelo et al., 2015, p. 130).

Por consiguiente, las regulaciones de protección de datos han aumentado en todo el mundo, normativas en Europa y en Estados Unidos imponen estrictos requisitos de seguridad de dato, esto significa que los archivos deben cumplir con estándares rigurosos para proteger la información almacenada, lo que añade presión para garantizar la seguridad (F. Valencia Duque & Orozco-

Alzate, 2017, p. 77). La digitalización de documentos ha influido en la seguridad de la información en archivos, a medida que más documentos se vuelven digitales, la necesidad de mantener su integridad y confidencialidad se vuelve urgente, esta exposición a amenazas digitales requiere medidas de seguridad sólidas.

La seguridad de la información tiene un impacto directo en la reputación y la confianza de las organizaciones, los incidentes de seguridad dañan gravemente la imagen de una empresa y erosionar la confianza de sus clientes o socios comerciales, esto puede resultar en pérdida de ingresos y litigios legales, se debe considerar la seguridad como la base de estos sistemas (Terán Terranova, 2021, pp. 15-16).

La globalización y la colaboración internacional hacen que la seguridad de la información sea un asunto complejo y global, las organizaciones deben asegurar la protección de datos en colaboraciones transfronterizas, lo que agrega un nivel adicional de desafío a la gestión de la seguridad de la información.

La seguridad de la información en archivos es crítica en el mundo actual debido al aumento de las amenazas cibernéticas, regulaciones más estrictas, digitalización de documentos, impacto en la reputación, y la necesidad de seguridad en la colaboración global. La protección de datos sensibles y el cumplimiento de estándares de seguridad son imperativos para garantizar la integridad y confidencialidad de la información.

Seguido, en el ámbito regional, la seguridad de la información en archivos en América Latina es un tema de prioridad, debido a varios factores. Primero, las amenazas cibernéticas están en aumento en la región, lo que significa que los archivos pueden ser blanco de ataques como el ransomware y el phishing, poniendo en riesgo la confidencialidad de los datos almacenados (Ramos et al., 2017, pp. 91-92).

Segundo, muchos distintos de América Latina enfrentan limitaciones económicas y carecen de recursos para invertir en medidas de seguridad sólidas, por tanto, la falta de fondos y de personal capacitado puede dificultar la implementación de políticas de seguridad efectivas en archivos (Rodriguez Baca et al., 2020, pp. 7-8).

Tercero, la región aún está en proceso de desarrollar regulaciones de protección de datos, lo que crea un entorno legal incierto para las organizaciones. Adaptarse a diferentes requisitos legales puede ser un desafío, especialmente para las empresas que operan en varios países de la región (Martelo et al., 2015, pp. 132-133).

El crecimiento de la digitalización de documentos y procesos en América Latina amplía el espectro de la seguridad de la información, ya que los archivos deben asegurar tanto los documentos en papel como los datos digitales, lo que demanda una estrategia de seguridad completa (F. Valencia Duque & Orozco-Alzate, 2017, p. 80); la falta de seguridad de la información erosiona la confianza de los inversionistas extranjeros en la región, disuadiendo la inversión extranjera directa, esencial para el desarrollo económico.

La seguridad de la información en archivos en América Latina enfrenta desafíos relacionados con amenazas cibernéticas, recursos limitados, regulaciones en desarrollo, digitalización creciente y su impacto en la confianza y la inversión, solucionar estos desafíos es sirve para proteger los datos y fomentar el crecimiento económico en la región.

En Colombia actualmente es una preocupación este problema, debido a diversos factores; Las amenazas cibernéticas están en constante aumento, lo que pone en riesgo la confidencialidad y la integridad de los datos almacenados, esto es una preocupación tanto para organizaciones gubernamentales como para empresas privadas (Arévalo Ascanio et al., 2015, p. 127).

El proceso de digitalización y modernización de archivos o sistemas de gestión documental en el país también ha ampliado la necesidad de una sólida seguridad de la información, la información digitalizada es susceptible a ataques cibernéticos y accesos no autorizados. El país ha implementado regulaciones de protección de datos que exigen altos estándares de seguridad de la información, estas regulaciones requieren que las organizaciones protejan de forma adecuada los datos personales, lo que agrega presión para mantener la seguridad de la información (Estrada-Esponda et al., 2021, p. 105).

La falta de seguridad de la información podría tener un impacto negativo en la confianza de los ciudadanos y las empresas en las instituciones gubernamentales y las organizaciones, esto

afecta la estabilidad económica y la inversión en el país, ya que la seguridad de la información sirve para mantener la integridad de los datos y la confianza en las operaciones comerciales.

En un entorno donde la transparencia y la responsabilidad son vez clave, la seguridad de la información en archivos es útil para cumplir con las leyes o regulaciones y demostrar una gestión adecuada de los datos y documentos públicos (Arévalo Ascanio et al., 2015, p. 130). La seguridad de la información en archivos en Colombia es crítica debido al aumento de las amenazas cibernéticas, las regulaciones de protección de datos, la digitalización en curso, el impacto en la confianza y la estabilidad económica, así como la necesidad de cumplimiento y transparencia. Es necesario que este problema sea estudiado para proteger datos sensibles y mantener la integridad en conjunto con la confianza en las instituciones u organizaciones del país.

1.2. Pregunta de Investigación

Según las conceptualizaciones hechas surge la pregunta ¿Qué elementos deben ser considerados en la propuesta de implementación de la norma ISO 27001 en el archivo central de la Gobernación del Departamento del Magdalena?

1.3. Objetivos

1.3.1. Objetivo General

Determinar los elementos de seguridad del acervo documental del archivo central de la Gobernación del Magdalena en el marco de la norma ISO 27001.

1.3.2. Objetivos Específicos

- Diagnosticar las debilidades y falencias del acceso a la información administrada por el software INFODOC.
- Identificar las prácticas actuales de gestión de seguridad de la información en el Archivo Central de la Gobernación del Magdalena y compararlas con los requisitos establecidos por la Norma ISO 27001.
- Estructurar los elementos que configuran la propuesta para la implementación de la Norma ISO 27001 en el Archivo Central de la Gobernación del Magdalena.

1.4. Justificación

La justificación de esta investigación radica en la creciente importancia de abordar el problema de la seguridad de la información en archivos en Colombia, se destacan las siguientes razones fundamentales que respaldan la necesidad de llevar a cabo este estudio; En un mundo cada vez más digitalizado y globalizado, la seguridad de la información es esencial. Colombia no está exenta de las amenazas cibernéticas en constante evolución, lo que hace que la investigación en este campo sea relevante y actual.

Además, los incidentes de seguridad de la información pueden tener un impacto económico significativo al afectar la inversión, la estabilidad económica y la reputación de las empresas u organizaciones, esta investigación identifica estrategias para mitigar estos riesgos y promover un entorno empresarial seguro.

Desde una perspectiva normativa, Colombia cuenta con regulaciones de protección de datos que imponen requisitos estrictos para garantizar la seguridad de la información, la investigación ayuda a las organizaciones a comprender y cumplir adecuadamente con estas regulaciones, para evitar posibles sanciones legales.

También la información almacenada en archivos incluye datos sensibles y confidenciales de ciudadanos y empresas, la seguridad de la información es necesaria para proteger la privacidad y la integridad de esta información, lo que justifica una investigación en este campo; Así como la transparencia y la confianza pública, en las instituciones gubernamentales y las organizaciones depende de la seguridad de la información que manejan. Esta investigación contribuye a fortalecer la transparencia en la confianza pública al analizar deficiencias en la seguridad de la información.

La investigación sobre seguridad de la información en archivos en Colombia es necesaria debido a su relevancia, impacto económico y empresarial, cumplimiento normativo, protección de datos, confianza pública y alineación con estándares internacionales. Abordar este problema es fundamental para proteger datos sensibles, promover un entorno empresarial seguro y fortalecer la confianza en las instituciones y organizaciones en Colombia.

2. Capítulo, Marco Teórico

La Gobernación del Magdalena, ubicada en la región Caribe de Colombia, desempeña un papel en la administración y desarrollo del departamento, su estructura organizativa, que incluye diversas dependencias y secretarías, facilita la gestión de políticas y programas en áreas como salud, educación y desarrollo económico, su contexto institucional presenta desafíos únicos, influenciados por su ubicación geográfica y las relaciones intergubernamentales que mantiene. En este marco, la Gobernación debe adherirse a un complejo sistema normativo y regulatorio que guía su operación, la Ley 1712 de 2014 garantiza el acceso a la información pública y promueve la transparencia, mientras que el Decreto 2150 de 1995 regula las actividades archivísticas y la conservación documental.

La Resolución 3573 de 2011 establece los requisitos para los Sistemas de Gestión de Seguridad de la Información (SGSI) en el sector público, y la norma ISO 27001:2013 proporciona un estándar internacional para la gestión sistemática de la seguridad de la información, estas normativas no solo aseguran la adecuada gestión documental y protección de la información, sino que también abordan los desafíos específicos que enfrenta la Gobernación en la implementación de políticas de seguridad y transparencia.

2.1. Antecedentes

Este análisis de antecedentes parte del trabajo “Análisis de los riesgos de seguridad de la información del sistema de gestión documental de la Alcaldía Municipal de Ibagué” (Bautista & Denys, 2021), el objetivo principal del proyecto es proporcionar a la Alcaldía de Ibagué un plan de mitigación de riesgos a través del análisis de seguridad de la información en el Sistema de Gestión Documental PISAMI. Este plan busca perfeccionar la metodología de análisis de riesgos MARGERIT, basándose en la Norma Internacional ISO 27001:2013, con el fin de identificar vulnerabilidades en los activos (hardware y software) y proponer controles para su gestión y minimización.

Los pilares teóricos del proyecto se basan en la Norma Internacional ISO 27001:2013, que establece los requisitos para un sistema de gestión de seguridad de la información. Además, se hace referencia a la ISO 31000:2018, que proporciona principios y directrices para la gestión de

riesgos en general. La metodología utilizada se centra en la mejora de la metodología de análisis de riesgos MARGERIT, alineándola con los estándares de la Norma Internacional ISO 27001:2013. Se lleva a cabo un análisis exhaustivo de los activos, identificando posibles vulnerabilidades y proponiendo medidas de control, este proceso incluye la evaluación de hardware y software para garantizar la integridad, disponibilidad o confidencialidad de la información.

Los resultados principales del proyecto incluyen un análisis detallado de los riesgos de seguridad de la información en el Sistema de Gestión Documental PISAMI, se identifican y documentan las vulnerabilidades presentes en los activos, y se proponen controles específicos para abordar estas vulnerabilidades. Los resultados apuntan a fortalecer la seguridad del sistema y proteger la información sensible manejada por la Alcaldía Municipal de Ibagué.

El proyecto concluye que el perfeccionamiento de la metodología de análisis de riesgos MARGERIT, basada en la Norma ISO 27001:2013, es necesario para identificar y abordar eficazmente las amenazas a la seguridad de la información. La implementación de controles específicos propuestos en el plan de mitigación contribuirá a garantizar la integridad, disponibilidad y confidencialidad de la información en el Sistema de Gestión Documental PISAM, la urgencia de cumplir con estándares internacionales en seguridad de la información se destaca como una medida crucial para proteger los activos de la Alcaldía Municipal de Ibagué contra posibles riesgos y amenazas.

Otro trabajo analizado es "Implantación de Buenas Prácticas Empresariales y Tecnologías en la Serie Documental Historias Laborales de la Gobernación del Valle del Cauca." (Pulido-Daza & Pérez, 2019) la investigación se centra en analizar el caso de estudio de la serie documental "Historias Laborales" de la Gobernación del Valle del Cauca. El objetivo principal es evaluar cómo la instalación y apropiación de buenas prácticas empresariales, junto con el manejo archivístico eficiente o la implementación de herramientas tecnológicas, generan valor en las respuestas del usuario final de la información y contribuyen a la aplicación eficiente de procesos con procedimientos en la organización.

Los referentes teóricos se basan en las buenas prácticas empresariales, la gestión archivística, y la influencia de las tecnologías en el manejo documenta, consideran teorías

relacionadas con la gestión del conocimiento, la eficiencia organizacional y la transformación digital. La metodología de la investigación incluye un enfoque cualitativo, donde se analizan casos específicos de la serie documental "Historias Laborales"; se emplean técnicas de recopilación de datos, como entrevistas, análisis documental y posiblemente encuestas, para evaluar la percepción y el impacto de la implantación de buenas prácticas y tecnologías en el manejo documental.

Los resultados principales revelan cómo la instalación y apropiación de buenas prácticas empresariales en la Gobernación del Valle del Cauca generan valor en las respuestas del usuario final de la información. Asimismo, se destaca cómo el buen manejo archivístico y la implantación de herramientas tecnológicas influyen positivamente en la eficiencia de los procesos y procedimientos organizacionales, se proporcionan ejemplos específicos de mejoras y beneficios observados.

Las conclusiones de la investigación resaltan la implantación de buenas prácticas empresariales, el manejo archivístico eficiente y la implementación de tecnologías en el contexto de la serie documental "Historias Laborales" de la Gobernación del Valle del Cauca. Se destacan los impactos positivos en el nexo laboral de los empleados y se sugieren posibles recomendaciones para fortalecer aún más estos procesos en la organización.

De la misma forma el trabajo "Seguridad de la información en el comercio electrónico basado en ISO 27001: Una revisión sistemática." (Rodríguez et al., 2023), el objetivo principal del estudio es analizar el estado actual de la gestión de la seguridad de la información en el ámbito del comercio electrónico (e Commerce), centrándose en la aplicación de la norma ISO 27001, se busca evaluar las evidencias proporcionadas por la investigación para comprender las vulnerabilidades existentes en estos sistemas y proponer mejoras en la gestión de la seguridad de la información.

Los principales referentes teóricos se enfocan en la seguridad de la información en el contexto del comercio electrónico y la aplicación de la norma ISO 27001, se podrían citar teorías y conceptos relacionados con la gestión de riesgos, ciberseguridad, y estándares internacionales de seguridad de la información. La metodología utilizada es una revisión sistemática que sigue las directrices PRISMA, se analizaron 6 artículos publicados en Scopus para recopilar evidencia sobre la seguridad de la información en el eCommerce.

La revisión se enfocó en identificar vulnerabilidades en estos sistemas de eCommerce y evaluar la efectividad de la gestión de la seguridad de la información, especialmente cuando se implementa la norma ISO 27001. Los resultados destacan consistentemente la alta vulnerabilidad de los sistemas, se subraya la necesidad de mejorar la gestión de la seguridad de la información y adoptar una gestión de riesgos más consciente de las amenazas emergentes. Además, se señala que, aunque existen gestores de seguridad en el mercado, la norma ISO 27001 abarca de manera integral muchas áreas de seguridad, ofreciendo así una mayor protección y confianza en los datos de los clientes.

Las conclusiones del estudio resaltan una gestión efectiva de la seguridad de la información en el contexto del comercio electrónico, se concluye que, debido al aumento de las amenazas, es crucial implementar medidas preventivas y correctivas. Se sugiere que la adopción de la norma ISO 27001 puede ser una estrategia eficaz para fortalecer la ciberseguridad en entornos de comercio electrónico, proporcionando una visión integral y robusta para abordar las vulnerabilidades específicas de estos sistemas.

Otra referencia es el trabajo "Desarrollo de Aplicación Web Para La Gestión de La Documentación En ISO 27001 Haciendo Uso de Herramientas de Software Libre." (Egea Sossa & López Rodríguez, 2021), el objetivo principal del proyecto es desarrollar una aplicación web que facilite a las empresas la gestión de la documentación utilizada en la norma ISO 27001. Se busca optimizar los procesos de revisión, corrección, aprobación y publicación de documentos para garantizar una implementación eficiente de los estándares de seguridad de la información establecidos por la norma.

El proyecto hace referencia a la norma ISO 27001 como un marco de estándares para la gestión de seguridad de la información, se asume que se han consultado y aplicado principios de desarrollo de software y gestión de proyectos. La metodología empleada es el modelo en cascada, que se desarrolla en cinco etapas: análisis, diseño, implementación, verificación e implementación, esta metodología proporciona un enfoque estructurado para el desarrollo de software, con monitoreo del progreso y metas específicas en cada fase.

El proyecto culminó en el desarrollo exitoso de una aplicación web funcional, los resultados principales incluyen una herramienta que permite a las empresas gestionar

eficientemente la documentación relacionada con la norma ISO 27001. La aplicación facilita las tareas de revisión, corrección, aprobación y publicación de documentos, contribuyendo así a una implementación efectiva de los estándares de seguridad de la información.

Las conclusiones del proyecto subrayan la importancia de la aplicación desarrollada, destacando su papel en mejorar la gestión documental relacionada con la norma ISO 27001, se presume que la implementación exitosa de la aplicación proporcionará a las empresas una opción eficaz y fácil para cumplir con los estándares de seguridad de la información. Se enfatiza la utilidad y accesibilidad de la aplicación para optimizar los procesos asociados a la norma ISO 27001.

Por esta línea conceptual también se encuentra "Análisis del Sistema de Información de Planificación Avanzada (APS) basado en la Norma de Seguridad Informática ISO 27001-2013 para la Reducción de Vulnerabilidades en la Empresa Privada Atimasa S.A. de la Ciudad de Guayaquil."(Preciado Cortez, 2022), como objetivo principal la investigación analiza el Sistema de Información de Planificación Avanzada (APS) de la empresa Atimasa S.A., con un enfoque en la norma de seguridad informática ISO 27001-2013, el objetivo es identificar y reducir las posibles vulnerabilidades en el sistema.

Los principales referentes teóricos se basan en la norma de seguridad informática ISO 27001-2013, que establece estándares y prácticas para la gestión de la seguridad de la información, se incluyen conceptos relacionados con la planificación avanzada (APS) y las mejores prácticas en seguridad informática. La metodología utilizada se describe como cualitativa e incluye aspectos descriptivos, bibliográficos, de campo y explicativos, esto sugiere un análisis en profundidad del contexto, se revisó la literatura relevante, se recopilaron datos en el campo y se explicaron los resultados obtenidos.

Entre los resultados principales, se destaca la identificación de debilidades en el sistema de información, principalmente relacionadas con la falta de control y procedimientos. Como respuesta a estos resultados, se desarrolló un plan de acción basado en la norma ISO 27001-2013, este plan de acción se presenta como una herramienta para abordar las debilidades identificadas y reducir las posibles vulnerabilidades futuras en el sistema de planificación avanzada de Atimasa S.A.

Las conclusiones del trabajo señalan que las debilidades en el sistema de información se originan por la falta de control y procedimientos adecuados. Se destacan los principios de la norma ISO 27001-2013 como una estrategia clave para mejorar la seguridad del sistema y proteger la integridad de la información en el futuro, el plan de acción propuesto se presenta como una solución concreta para fortalecer la seguridad del sistema de planificación avanzada utilizado por la empresa Atimasa S.A. y reducir las vulnerabilidades identificadas.

Al finalizar realizamos el análisis del estudio "Implicaciones de la Inteligencia Artificial en la Transformación Digital Empresarial: Un Estudio de Caso en el Sector Financiero", se planteó como objetivo general analizar las consecuencias de la inteligencia artificial en la transformación digital de empresas del sector financiero, con el propósito de identificar oportunidades y desafíos asociados a esta integración. Los principales referentes teóricos abordaron las teorías de la transformación digital en el ámbito empresarial, conceptos clave de inteligencia artificial y su aplicación específica en el sector financiero, así como estudios previos relacionados con la adopción de tecnologías emergentes en entornos empresariales.

La metodología empleada fue la de un estudio de caso, seleccionando tres instituciones financieras de distintos tamaños como muestra, para recopilar información se utilizaron instrumentos como entrevistas semiestructuradas, análisis documental y observación participante. El procedimiento consistió en evaluar la implementación de soluciones basadas en inteligencia artificial, identificar oportunidades y desafíos, así como recopilar y analizar datos relevantes.

Los resultados principales revelaron áreas específicas en las cuales la inteligencia artificial ha mejorado tanto los procesos internos como externos en las instituciones financieras estudiadas. Se evaluó el impacto positivo en términos de eficiencia operativa, experiencia del cliente y toma de decisiones estratégicas. Sin embargo, también se identificaron desafíos y obstáculos, tales como la necesidad de capacitación continua del personal y la gestión de la seguridad de los datos.

En las conclusiones del estudio, se destacó que la implementación de soluciones basadas en inteligencia artificial ha sido beneficioso para mejorar la eficiencia operativa y la experiencia del cliente en las instituciones financieras. Aunque se evidenciaron beneficios significativos, se reconoció la existencia de desafíos, lo que llevó a la recomendación de una estrategia integral de

implementación que aborde tanto los aspectos positivos como los desafíos asociados con la adopción de tecnologías de inteligencia artificial en el sector financiero.

2.2. Estado del Arte

El origen de las prácticas de seguridad en archivos gubernamentales se encuentra arraigado en la necesidad de salvaguardar información sensible y esencial para el funcionamiento efectivo del Estado (Estrada-Esponda et al., 2021, p. 103), desde las primeras etapas de la civilización, las entidades gubernamentales han manejado datos para la administración, legislación, seguridad y otros aspectos del gobierno. La sensibilidad inherente de esta información generó la imperativa tarea de protegerla contra accesos no autorizados y posibles amenazas.

En sus primeras manifestaciones, la seguridad se centraba predominantemente en la protección física de los documentos, los registros, pergaminos y documentos escritos eran almacenados en lugares seguros, como archivos y bibliotecas gubernamentales (Macedonio, 2018, pp. 77-78), la restricción de acceso físico a estos lugares se establecía como una medida esencial para prevenir el robo, la pérdida o la manipulación no autorizada de la información sensible. El almacenamiento seguro se convertía en una práctica estándar, por el uso de cajas fuertes, cerraduras y otros dispositivos de seguridad física para garantizar la integridad de la información o su disponibilidad cuando fuera requerida.

Estas primeras medidas de seguridad se fundamentaban en la necesidad intrínseca de proteger la información sensible, y también respondían a preocupaciones históricas o políticas, eventos como guerras, conflictos o cambios políticos generaron una creciente conciencia sobre las potenciales repercusiones de la pérdida o manipulación de información en manos equivocadas, destacando la vital importancia de establecer prácticas de seguridad sólidas (Macedonio, 2018, pp. 77-78).

A medida que el tiempo avanzaba, la evolución tecnológica introdujo nuevos desafíos y oportunidades en la gestión de la seguridad de la información, las medidas físicas continuaron siendo relevantes, pero la seguridad se expandió más allá de estas hacia enfoques más complejos, al incluir la seguridad electrónica. Este enfoque inicial sentó las bases para el desarrollo de

prácticas más avanzadas a lo largo de la historia y hasta la actualidad, delineando la evolución continua de la seguridad en archivos gubernamentales (Antonow, 2021, p. 3).

El desarrollo de medidas de seguridad experimentó una transformación significativa con el avance de la tecnología y el crecimiento exponencial en la complejidad de la gestión de la información, en las últimas décadas del siglo XX, se evidenció un cambio sustancial hacia la implementación de medidas de seguridad más sofisticadas, impulsado por una conjunción de factores determinantes. El aumento en la cantidad de información a gestionar integro la necesidad de evolucionar las prácticas de seguridad, con la expansión de las funciones gubernamentales y la digitalización de los procesos administrativos, la magnitud y diversidad de la información se multiplicaron. Este incremento en la escala y complejidad de los datos generó una presión adicional para establecer medidas de seguridad más avanzadas y adaptables (Estrada-Esponda et al., 2021, p. 105).

La informatización de los procesos gubernamentales fue otro factor que determino la transformación de las prácticas de seguridad, a medida que las entidades gubernamentales adoptaban sistemas informáticos para agilizar y mejorar la eficiencia de sus operaciones, la seguridad de la información se volvía una preocupación crítica (Macedonio, 2018, p. 78). La transición de archivos físicos a sistemas electrónicos ofrecía ventajas en términos de accesibilidad o eficiencia, también introducía nuevos desafíos relacionados con la protección de datos sensibles.

La creciente amenaza de ataques informáticos constituyó un imperativo para el cambio en las medidas de seguridad, la era digital trajo consigo la proliferación de amenazas cibernéticas, desde virus y malware hasta intentos de intrusiones más sofisticadas (Antonow, 2021, p. 3). Este panorama amenazante hizo evidente la necesidad de fortalecer las defensas para resguardar la integridad, confidencialidad y disponibilidad de la información gubernamental.

En respuesta a estos desafíos, la implementación de medidas de seguridad más avanzadas se convirtió en una prioridad estratégica. Los controles de acceso, cifrado de datos, auditorías de seguridad y la adopción de estándares y normativas específicas se volvieron elementos esenciales en la protección de la información gubernamental (Mori, 2021, p. 170). Este cambio de paradigma refleja la adaptabilidad y la respuesta proactiva de las entidades gubernamentales frente a un entorno digital en constante evolución, en conjunto, estos factores marcaron un hito en la evolución

de las prácticas de seguridad, al llevar la implementación de medidas más avanzadas o adecuadas para enfrentar los desafíos emergentes de la era digital.

La evolución de las medidas de seguridad en el ámbito gubernamental revela una adaptación clave a la era digital y a los desafíos contemporáneos en torno a la protección de la información, el cambio hacia prácticas más sofisticadas responde, en gran medida, a un aumento exponencial en la cantidad de información que las entidades gubernamentales manejan. En este contexto, la informatización de procesos gubernamentales se convirtió en una realidad inevitable, generando la necesidad de estrategias avanzadas para asegurar la integridad, confidencialidad y disponibilidad de los datos.

La complejidad de los desafíos actuales en seguridad de la información se manifiesta en la creciente amenaza de ataques de tipo informático, la era digital ha expandido el espectro de amenazas, desde ataques tradicionales hasta modalidades más sofisticadas como el ransomware y el phishing. Esta realidad exige respuestas de seguridad más integrales, capaces de hacer frente a la diversidad y sofisticación de las amenazas digitales.

La implementación de medidas de seguridad más avanzadas implica una comprensión profunda de la necesidad de la protección proactiva, ya no es suficiente reaccionar ante incidentes; es esencial anticipar posibles amenazas y establecer barreras sólidas para prevenir la pérdida de datos y la violación de la seguridad. En este contexto, la adopción de estándares y normativas específicas se presenta como una herramienta, proporciona un marco de referencia claro que guía a las entidades gubernamentales en la evaluación y mejora constante de sus prácticas de seguridad.

La transición de archivos físicos a sistemas electrónicos subraya el desafío de encontrar un equilibrio entre la accesibilidad y la seguridad, la digitalización aporta beneficios significativos en términos de eficiencia y accesibilidad a la información, de forma simultánea introduce riesgos que deben gestionarse de manera eficaz para mantener la confianza en la gestión de la información gubernamental. En conjunto, estas apreciaciones resaltan la complejidad y la importancia crítica de la seguridad de la información en el contexto gubernamental, exigiendo enfoques estratégicos y multifacéticos para proteger la información sensible en un entorno digital dinámico y desafiante.

Seguido, para explorar la seguridad, una empresa que ha sido pionera y ha desempeñado un rol en la gestión de la seguridad de la información es IBM (International Business Machines Corporation), IBM ha sido un líder histórico en la industria de la tecnología y ha contribuido de manera significativa al desarrollo de prácticas de seguridad modernas en diversos sectores, incluye el gubernamental (Buitrago Rojas & Alvarado Romero, 2018, pp. 42-43).

IBM ha estado a la vanguardia de la investigación y desarrollo de soluciones de seguridad, proporcionando tecnologías innovadoras y asesoramiento estratégico en el ámbito de la ciberseguridad (F. J. Valencia Duque, 2021, pp. 87-88), la empresa ha participado activamente en la implementación de estándares y mejores prácticas de seguridad, influyendo en la forma en que las organizaciones, incluyendo las gubernamentales, abordan la protección de la información sensible.

A lo largo de las décadas, IBM ha desarrollado y ofrecido una amplia gama de productos y servicios de seguridad, desde sistemas de cifrado hasta soluciones avanzadas de gestión de amenazas (F. J. Valencia Duque, 2021, pp. 87-88), la empresa ha liderado iniciativas para promover la conciencia y la educación en seguridad cibernética, contribuyendo al fortalecimiento de la capacidad de respuesta y prevención de incidentes en el ámbito gubernamental y empresarial.

La experiencia y liderazgo de IBM en el campo de la seguridad de la información han influenciado directamente la evolución de las prácticas de seguridad en archivos gubernamentales y en el manejo de datos sensibles. Su enfoque integral, que abarca desde la investigación hasta la implementación práctica, ha contribuido significativamente a la construcción de un entorno digital más seguro y confiable. En este sentido, IBM se destaca como un pionero corporativo que ha dejado una marca duradera en la gestión de la seguridad de la información a nivel global.

Por otro lado, la adopción y desarrollo de normativas y estándares internacionales en el ámbito de la seguridad de la información han sido fundamentales para establecer marcos coherentes y efectivos que guíen a organizaciones en la protección de datos sensibles, un destacado referente en este contexto es la norma ISO 27001, cuya aparición y evolución han marcado la promoción de mejores prácticas a nivel global (Navarro Martínez, 2018, p. 27).

La necesidad de un marco estandarizado para la gestión de la seguridad de la información se hizo evidente a medida que las organizaciones se enfrentaban a amenazas cibernéticas cada vez más complejas y sofisticadas. En respuesta a este desafío, la ISO (Organización Internacional de Normalización) desarrolló la norma ISO 27001, que establece los requisitos para un Sistema de Gestión de Seguridad de la Información (SGSI) (Sepúlveda & Jaramillo, 2018, pp. 89-90).

La ISO 27001 proporciona un conjunto claro de requisitos y controles de seguridad, que también se adapta a la evolución continua de las amenazas o tecnologías, su enfoque basado en el riesgo permite a las organizaciones personalizar sus enfoques de seguridad de manera que se alineen con sus contextos específicos y riesgos particulares (Navarro Martínez, 2018, p. 27).

A lo largo del tiempo, la ISO 27001 ha evolucionado para abordar los cambios en la tecnología, las regulaciones y las amenazas emergentes; su flexibilidad y aplicabilidad a una variedad de sectores la han convertido en un estándar internacional ampliamente aceptado y respetado. La norma ISO 27001 se ha convertido en un referente global para organizaciones que buscan establecer, implementar, mantener y mejorar continuamente un SGSI.

La adopción generalizada de la ISO 27001 ha contribuido a la armonización de prácticas de seguridad en todo el mundo, las organizaciones que buscan cumplir con los requisitos de seguridad internacionalmente reconocidos encuentran en la ISO 27001 un marco sólido (Sepúlveda & Jaramillo, 2018, pp. 89-90). La norma promueve la transparencia y la confianza entre partes interesadas al demostrar un compromiso serio con la seguridad de la información.

El desarrollo de normativas y estándares internacionales, con especial énfasis en la norma ISO 27001, han proporcionado a las organizaciones herramientas efectivas y un marco común para la gestión de la seguridad de la información. La ISO 27001 ha jugado un papel central al establecer un referente global que ha contribuido significativamente a la mejora continua de las prácticas de seguridad a nivel internacional.

Por otra parte, la exploración y evaluación detallada de software de gestión documental representan un componente crítico en el marco de la investigación orientada a mejorar la seguridad del acervo documental en el Archivo Central de la Gobernación del Magdalena, identificar

debilidades y falencias en estas herramientas sirve para fortalecer la infraestructura y garantizar un manejo seguro de la información.

La alineación de un software con normativas y estándares, especialmente aquellos relacionados con la seguridad de la información, sirve en un entorno gubernamental, la norma ISO 27001, que establece requisitos específicos para la gestión de la seguridad de la información, actúa como un marco de referencia (Chávarry Bonilla, 2021, p. 12). La evaluación de software debe considerar su funcionalidad como su capacidad para cumplir con estas normativas, al garantizar así que la implementación se realice en concordancia con estándares reconocidos internacionalmente.

La búsqueda de mejores prácticas en seguridad documental es un objetivo inherente a esta evaluación. La identificación de funciones específicas de seguridad, como controles de acceso robustos, cifrado de datos y auditorías exhaustivas, contribuye a fortalecer la protección de la confidencialidad, integridad y disponibilidad de la información gubernamental (Macedonio, 2018, p. 75). Esto reduce los riesgos asociados a posibles brechas de seguridad al sentar las bases para una gestión documental más resiliente.

La adaptabilidad del software a necesidades específicas es otro factor crítico, dado que cada institución tiene requerimientos únicos, la evaluación de software debe revelar su capacidad para personalizarse y satisfacer las necesidades particulares del Archivo Central, esta adaptabilidad garantiza que la herramienta seleccionada sea efectiva y beneficie directamente a la institución en cuestión.

Como tema principal surge entonces la tecnología como impulsor del cambio, la adopción de tecnologías de la información y comunicación (TIC) ha sido un impulsor de cambio en diversos sectores, y el ámbito gubernamental no es la excepción, durante este periodo de transformación, la informatización de procesos gubernamentales ha contribuido significativamente a mejorar la eficiencia en la gestión de la información. Sin embargo, este avance tecnológico también ha planteado nuevos desafíos, especialmente en el ámbito de la seguridad de la información (Rodriguez Zapata, 2021, p. 8).

La transición de archivos físicos a sistemas electrónicos ha sido un hito en este proceso de cambio, aunque ha proporcionado beneficios considerables, como mayor accesibilidad y eficiencia en la manipulación de datos, también ha destacado la necesidad urgente de implementar medidas de seguridad más avanzadas (Garcia Cruz, 2021, pp. 62-63). La digitalización de los procesos gubernamentales ha expuesto la información a amenazas cibernéticas cada vez más sofisticadas, como virus, malware y ataques informáticos.

Este contexto resalta la necesidad de adaptar las prácticas de seguridad de la información a la era digital, la protección de la integridad, confidencialidad y disponibilidad de los datos se convierte en una prioridad estratégica. La implementación de medidas de seguridad avanzadas, como controles de acceso robustos, cifrado de datos y protocolos de auditoría, se vuelve urgente para mitigar los riesgos asociados con la gestión electrónica de la información gubernamental (Rodriguez Zapata, 2021, p. 9).

La adopción de tecnologías de la información y comunicación ha sido un catalizador de cambio en el ámbito gubernamental, al mejorar la eficiencia operativa pero también introduce desafíos en términos de seguridad, la transición a sistemas electrónicos destaca la necesidad crítica de fortalecer las prácticas de seguridad de la información para garantizar la protección y preservación de los datos gubernamentales en un entorno digital en constante evolución.

Desde el comienzo, los pioneros en la gestión de la seguridad de la información han dejado un legado que influencia a lo largo del tiempo, los primeros esfuerzos y contribuciones han moldeado el panorama actual de la seguridad en archivos gubernamentales. Este legado es notable en la evolución de estándares y normativas, destacando la significativa influencia que han tenido en la formulación y desarrollo de la norma ISO 27001(Buitrago Rojas & Alvarado Romero, 2018, p. 39).

El análisis del estado del arte sobre la seguridad en archivos gubernamentales revela una evolución significativa desde sus primeras manifestaciones hasta la era digital actual. La necesidad intrínseca de proteger información sensible ha sido la fuerza impulsora detrás de esta evolución, y las prácticas de seguridad han pasado de centrarse en la protección física de documentos a abordar desafíos más complejos en el ámbito electrónico.

En sus inicios, la seguridad se centraba en la protección física mediante medidas como cajas fuertes y restricciones de acceso, sin embargo, con la digitalización de los procesos gubernamentales y el aumento exponencial de la cantidad de información, las entidades gubernamentales se vieron obligadas a adoptar prácticas de seguridad más avanzadas y adaptables. La informatización, aumentó la eficiencia al introducir nuevos desafíos, especialmente con la creciente amenaza de ataques cibernéticos.

La respuesta proactiva de las entidades gubernamentales a estos desafíos se refleja en la implementación de medidas de seguridad más avanzadas, como controles de acceso, cifrado de datos y auditorías de seguridad. Este cambio de paradigma demuestra la adaptabilidad de las instituciones ante un entorno digital en constante evolución, la evolución hacia prácticas más sofisticadas también se ve respaldada por la adopción de estándares y normativas específicas, como la norma ISO 27001.

La figura destacada de IBM como pionero en la gestión de la seguridad de la información destaca la importancia de la innovación y el liderazgo corporativo en la evolución de las prácticas de seguridad. IBM ha desempeñado un papel crucial al proporcionar tecnologías innovadoras, asesoramiento estratégico y liderar iniciativas para fortalecer la seguridad cibernética en entornos gubernamentales.

La norma ISO 27001 emerge como un referente global, proporcionando un marco claro y flexible para la gestión de la seguridad de la información, su evolución continua y su aceptación generalizada contribuyen a la armonización de prácticas de seguridad a nivel internacional, al promover la transparencia y la confianza en la gestión de la información sensible.

La evaluación detallada del software de gestión documental resalta la importancia de alinear las herramientas con normativas y estándares, en especial para aquellos relacionados con la seguridad de la información. La adaptabilidad del software a necesidades específicas y su capacidad para cumplir con normativas reconocidas internacionalmente son elementos clave en la selección de herramientas que fortalezcan la seguridad de la información gubernamental.

El papel de la tecnología como impulsor del cambio es evidente en la transición de archivos físicos a sistemas electrónicos, si bien ha mejorado la eficiencia, también ha introducido nuevos

desafíos, la necesidad de fortalecer las prácticas de seguridad se convierte en una prioridad estratégica para mitigar los riesgos asociados con la gestión electrónica de la información gubernamental.

En conclusión, la evolución de las prácticas de seguridad en archivos gubernamentales revela la adaptación continua a los desafíos de cada era, desde la protección física de documentos hasta la implementación de medidas avanzadas en la era digital. La combinación de liderazgo corporativo, estándares internacionales y la adopción de tecnologías avanzadas impacta en la construcción de un entorno digital más seguro y confiable para la gestión de la información gubernamental.

2.3. Categorías Conceptuales

La investigación sobre la seguridad del acervo documental en entidades gubernamentales se sustenta en la comprensión detallada de diversas categorías conceptuales que desempeñan roles fundamentales en este ámbito. Estas categorías conceptuales abarcan desde la Gestión de la Seguridad de la Información (GSI), que constituye un marco conceptual esencial, hasta la Norma ISO 27001, que es una referencia clave en la seguridad de la información. Además, se analiza la naturaleza y relevancia del acervo documental en contextos gubernamentales, considerando teorías que resaltan la importancia de la integridad, confidencialidad y disponibilidad de la información.

La exploración se extiende a la infraestructura tecnológica y al software de gestión documental, en este contexto, se examinan teorías relacionadas con la selección y gestión de software, al estudiar aspectos de seguridad, y se aborda la influencia de la cultura organizacional en la implementación efectiva de medidas de seguridad, junto con teorías sobre la conciencia de seguridad, la capacitación del personal o la promoción de una cultura proactiva frente a amenazas de seguridad.

Esta estructura conceptual proporciona una base teórica sólida y contextualiza la investigación dentro del panorama histórico y conceptual relevante. Al explorar teóricos y conceptos fundamentales, se busca lograr un entendimiento profundo de la seguridad del acervo documental en el contexto gubernamental, cada categoría conceptual contribuye de manera única

a la comprensión integral de los desafíos y oportunidades asociados con la protección de la información gubernamental en un entorno digital en constante evolución.

2.3.1. Sistema de Gestión de Seguridad de la Información (SGSI)

El Sistema de Gestión de Seguridad de la Información (SGSI) se posiciona como un enfoque esencial y completo para salvaguardar los activos de información críticos en el contexto empresarial actual, su carácter holístico se deriva de la consideración integral del ciclo de vida de la información, desde su concepción hasta su eliminación, abarcando todas las etapas intermedias (Martín, 2021, p. 499) Este enfoque integral reconoce que la seguridad de la información no es un evento aislado, sino un proceso continuo que implica la gestión diligente de la información en todas sus formas.

El SGSI va más allá de la implementación de controles tecnológicos al reconocer que la seguridad de la información es una tarea multifacética que involucra aspectos técnicos, humanos y organizacionales, al incorporar procesos, políticas y prácticas organizacionales, el SGSI se convierte en un marco completo que se adapta a la dinámica cambiante del entorno empresarial (Benites Durand, 2019, p. 146). La inclusión de procesos implica una planificación estratégica que abarca desde la identificación de activos de información hasta la evaluación de riesgos y la implementación de controles proporcionados.

Las políticas establecen las directrices y normas que orientan el comportamiento de los empleados y las prácticas organizacionales, mientras que las prácticas organizacionales eficaces garantizan la ejecución coherente y sostenible de las políticas y procesos, este enfoque holístico tiene como objetivo garantizar la confidencialidad, integridad y disponibilidad de la información, constituyendo los pilares fundamentales de la seguridad de la información (Martín, 2021, p. 505).

La confidencialidad asegura que la información esté protegida contra accesos no autorizados, la integridad se enfoca en prevenir la modificación no autorizada de datos, y la disponibilidad se centra en garantizar que la información esté accesible cuando sea necesaria. Estos principios fundamentales se entrelazan en el SGSI, al establecer un equilibrio entre la protección de la información sensible y la facilitación de su uso legítimo y eficiente (Benites Durand, 2019, p. 150).

En un entorno empresarial dinámico, donde la información fluye a través de diversos canales y plataformas, la necesidad de un enfoque estructurado como el SGSI se vuelve útil, la rápida evolución tecnológica, las crecientes amenazas cibernéticas y la complejidad de las operaciones empresariales exigen una respuesta integral y coordinada para garantizar la seguridad de la información; en este sentido, el SGSI es el guardián de la integridad y la confidencialidad de la información, proporcionando un marco sólido que se adapta a la naturaleza dinámica o cambiante del entorno empresarial contemporáneo.

La evolución continua del Sistema de Gestión de Seguridad de la Información (SGSI) es un testimonio de su capacidad para adaptarse de manera proactiva a las transformaciones en el panorama de la seguridad de la información, en un entorno donde la información predominaba en formatos físicos, el enfoque del SGSI se centraba en controles de acceso físico y medidas destinadas a salvaguardar documentos impresos (Garcia Cruz, 2021, p. 77). La seguridad estaba intrínsecamente ligada a la protección de activos tangibles y la restricción del acceso físico a archivos y registros.

Con la llegada de la era digital, la explosión de datos electrónicos y la proliferación de amenazas cibernéticas, el SGSI se vio obligado a expandir su enfoque más allá de las medidas tradicionales, la transición a entornos digitales presentó desafíos significativos, dando origen a la necesidad de controles tecnológicos avanzados (Lema Vinlasaca, 2018, p. 56). La seguridad ya no podía depender únicamente de la custodia física; ahora, la protección debía abordar riesgos como el robo virtual, el malware y otros ataques informáticos.

La maduración del SGSI se evidencia en su cambio estratégico hacia un enfoque proactivo basado en la gestión de riesgos, la anticipación de amenazas potenciales se convirtió en una prioridad, al reconocer que la prevención es tan crucial como la reacción ante incidentes, la implementación de medidas preventivas se volvió central para mitigar riesgos antes de que se materialicen, y la adaptación continua a las dinámicas cambiantes del entorno digital se convirtió en una característica distintiva del SGSI moderno.

La introducción de prácticas ágiles y flexibles marca otra fase crucial en la evolución del SGSI. La seguridad de la información ya no es concebida como un objetivo estático y rígido, sino como un proceso continuo de mejora y adaptación, en un mundo donde las amenazas evolucionan

constantemente, la capacidad de ajustar estrategias y controles de seguridad de manera ágil se vuelve esencial (Garcia Cruz, 2021, p. 80).

Esta adaptabilidad garantiza que el SGSI permanezca eficaz frente a las amenazas emergentes y los cambios en la tecnología, manteniendo la integridad, confidencialidad y disponibilidad de la información en un entorno empresarial dinámico y desafiante, la evolución del SGSI refleja su habilidad para mantenerse a la vanguardia en la protección de la información en un mundo digital en constante cambio.

2.3.2. Norma ISO 27001

La ISO 27001 es un estándar desarrollado por la Organización Internacional de Normalización (ISO), lo que confiere a esta norma un estatus globalmente aceptado, su adopción y reconocimiento internacional proporcionan un marco coherente para la gestión de la seguridad de la información en organizaciones de diversos sectores o ubicaciones geográficas (Torres Chango, 2020, pp. 59-60). Este estatus global facilita la comunicación y colaboración entre entidades que buscan alinear sus prácticas de seguridad con estándares reconocidos a nivel mundial.

La ISO 27001 establece principios generales y proporciona un marco detallado de requisitos específicos que las organizaciones deben cumplir para implementar un SGSI eficaz, desde la definición de políticas de seguridad hasta la gestión de riesgos y la mejora continua, la norma aborda exhaustivamente los elementos esenciales de la seguridad de la información (Argüezo Ramirez, 2019, p. 49).Esto facilita a las organizaciones la creación de un sistema de gestión robusto y adaptado a sus necesidades específicas.

Esta norma está diseñada para garantizar la confidencialidad, integridad y disponibilidad de la información, estos principios fundamentales de la seguridad de la información se abordan a través de la implementación de controles específicos y la gestión proactiva de riesgos (Torres Chango, 2020, p. 62). Al enfocarse en estos aspectos cruciales, la ISO 27001 ayuda a las organizaciones a construir una base sólida para la protección de sus activos de información.

La gestión de riesgos es un componente esencial de la Norma ISO 27001, desempeña un papel crucial en el establecimiento y mantenimiento efectivo de un Sistema de Gestión de

Seguridad de la Información (SGSI), La importancia de este enfoque sistemático se manifiesta en varios aspectos clave, la norma promueve la identificación proactiva de riesgos de seguridad de la información (Argüezo Ramirez, 2019, p. 52). Este enfoque preventivo implica analizar de manera exhaustiva los diferentes aspectos de las operaciones de una organización para identificar posibles amenazas y vulnerabilidades que puedan afectar la confidencialidad, integridad y disponibilidad de la información.

La anticipación de riesgos permite a la organización tomar medidas antes de que se conviertan en problemas significativos, una vez identificados, la norma prescribe la evaluación y cuantificación de los riesgos, este paso implica determinar la probabilidad de que un riesgo se materialice y evaluar el impacto potencial en caso de ocurrencia (Yungán Cazar & Narváez Contero, 2022, pp. 6-7). La combinación de la probabilidad y el impacto ayuda a clasificar y priorizar los riesgos, permitiendo a la organización enfocar sus recursos en abordar aquellos que representan las mayores amenazas para la seguridad de la información.

La gestión de riesgos según la ISO 27001 no se limita a la identificación y evaluación; también incluye la implementación de medidas para mitigar o aceptar los riesgos, esta fase activa implica la aplicación de controles de seguridad y salvaguardas diseñados para reducir la probabilidad de ocurrencia de los riesgos identificados o disminuir su impacto en caso de materialización(Lema Vinlasaca, 2018, pp. 38-39), estas medidas pueden abarcar desde controles tecnológicos hasta procedimientos operativos y educación del personal.

La norma subraya la importancia de la revisión continua del panorama de riesgos a medida que la organización evoluciona. La dinámica del entorno empresarial y tecnológico implica que los riesgos también evolucionan con el tiempo. La ISO 27001 propone que las evaluaciones de riesgos sean periódicas y que se ajusten en respuesta a cambios en la organización, en las amenazas externas o en las condiciones del mercado. Esta capacidad de adaptación garantiza que el SGSI se mantenga relevante y efectivo en el enfrentamiento de riesgos emergentes.

En resumen, la gestión de riesgos en el contexto de la Norma ISO 27001 constituye un proceso integral que abarca desde la identificación proactiva de amenazas hasta la evaluación, cuantificación y tratamiento proactivo de los riesgos identificados, este enfoque sistemático se

completa con una revisión continua que asegura la eficacia del Sistema de Gestión de Seguridad de la Información (SGSI) en un entorno empresarial dinámico y cambiante.

La norma ISO 27001 destaca como referencia clave en la seguridad de la información gracias a su estatus internacional, requisitos detallados y enfoque holístico, contribuyendo significativamente a fortalecer la postura de seguridad de una organización, al adoptar esta norma, las organizaciones cumplen con estándares reconocidos a nivel mundial que también fortalecen su seguridad y generan confianza entre las partes interesadas en un entorno empresarial cada vez más digitalizado.

2.3.3. Conservación Documental en Entidades del Gobierno

La conservación documental en entidades gubernamentales desempeña un papel crítico al asegurar la preservación a largo plazo, el acceso eficiente y la integridad de los documentos que constituyen su acervo, este proceso va más allá de la simple acumulación de documentos; implica estrategias planificadas diseñadas para salvaguardar la riqueza de la información contenida en ellos (Dominguez et al., 2022, pp. 68-69).

En primer lugar, la preservación a largo plazo sirve para garantizar que los documentos históricos y administrativos perduren a lo largo del tiempo, esto contribuye a la conservación de la memoria institucional para proporcionar una base sólida en la comprensión de la evolución de políticas, decisiones gubernamentales y prácticas administrativas (Rodríguez Bustos, 2019, pp. 22-23).

El acceso eficiente a la información es otro aspecto de la conservación documental, la organización cuidadosa y la implementación de sistemas efectivos permiten a los funcionarios gubernamentales, investigadores y al público en general encontrar o utilizar los documentos de manera rápida con efectividad, esto facilita la rendición de cuentas y la transparencia que respalda la toma de decisiones informadas (Dominguez et al., 2022, p. 73).

La integridad de los documentos, garantizada a través de estrategias de conservación planificadas, asegura que la información permanezca auténtica y exacta a lo largo del tiempo; esto preserva la confiabilidad de los documentos históricos, sino que también fortalece la seguridad y privacidad de la información administrativa contemporánea.

La naturaleza y relevancia del acervo documental en entidades gubernamentales se profundizan al considerar su contribución clave a la transparencia, rendición de cuentas y toma de decisiones informadas, la preservación de documentos históricos desencadena una comprensión completa de la evolución de políticas y prácticas gubernamentales, proporcionando una base sólida para la toma de decisiones actuales (Montalvo Cisneros, 2021, pp. 27-28). Estos documentos históricos actúan como testigos fidedignos de eventos pasados, al permitir a los líderes y ciudadanos entender el contexto o las lecciones aprendidas a lo largo del tiempo.

Los documentos administrativos contemporáneos son esenciales para respaldar la rendición de cuentas en el presente, la documentación detallada de acciones gubernamentales, políticas y procesos proporciona una trazabilidad necesaria para evaluar la eficacia o eficiencia de las decisiones tomadas (Moscaiza Moncada, 2018, p. 23). Este registro sirve como un mecanismo de responsabilidad interna y también está disponible para el escrutinio público, fomentando la transparencia o fortaleciendo la confianza de los ciudadanos en las instituciones gubernamentales.

En conjunto, la preservación y disponibilidad del acervo documental gubernamental enriquecen la comprensión histórica para servir como pilares fundamentales en una gobernanza transparente y una la toma de decisiones en el presente y el futuro, la conservación documental en entidades gubernamentales es un proceso de acumulación estratégica que aborda la preservación, el acceso y la integridad de la información. Al implementar estas estrategias planificadas, las instituciones gubernamentales aseguran la continuidad de su memoria institucional, promueven la transparencia y facilitan un entorno propicio para la toma de decisiones basada en información precisa y confiable.

2.3.4. Infraestructura Tecnológica y Software de Gestión Documental

La necesidad de una infraestructura tecnológica en la seguridad del acervo documental es innegable en la era digital actual, la transición de los documentos físicos a formatos digitales ha introducido una complejidad y una cantidad de información que requieren sistemas avanzados para su gestión efectiva o segura (Montalbán et al., 2020, pp. 230-231).

En primer lugar, la infraestructura tecnológica proporciona el marco necesario para la digitalización y almacenamiento seguro de documentos, los avances en tecnología permiten la

creación de copias digitales exactas, al preservar la integridad de la información a lo largo del tiempo (Rosales Montalban, 2019, pp. 19-20). La capacidad de almacenamiento en sistemas digitales garantiza la disponibilidad y accesibilidad rápida a los documentos cuando se necesiten, mejorando la eficiencia operativa.

La seguridad del acervo documental se ve reforzada por la infraestructura tecnológica a través de medidas como el cifrado de datos, el control de acceso y la implementación de firewalls o sistemas de detección de intrusiones., estas capas de seguridad protegen la información contra accesos no autorizados, al mitigar riesgos como pérdida de documentos físicos, daños por desastres naturales o deterioro con el tiempo (Montalbán et al., 2020, p. 235).

La infraestructura tecnológica facilita la aplicación de políticas de retención y disposición de documentos, lo que contribuye a una gestión eficiente del ciclo de vida de la información, la automatización de procesos mediante sistemas tecnológicos reduce errores humanos, por la garantía del cumplimiento de regulaciones y normativas relacionadas con la retención o eliminación de documentos (Rosales Montalban, 2019, p. 22)..

La necesidad de una infraestructura tecnológica en la seguridad del acervo documental radica en su capacidad para ofrecer una gestión eficiente, accesibilidad, protección contra amenazas o cumplimiento de normativas, en un entorno donde la información es un activo crítico, la inversión en infraestructura tecnológica se presenta como un requisito esencial para garantizar la seguridad y la integridad del acervo documental en entidades gubernamentales u organizaciones en general.

En síntesis, la conservación documental en entidades gubernamentales sirve para salvaguardar la integridad, confidencialidad y disponibilidad de la información a lo largo del tiempo, la aplicación de teorías que destacan estos principios garantiza un enfoque equilibrado que considera tanto la preservación histórica como la utilidad práctica de los documentos. En un entorno gubernamental, donde la información es un activo crítico y la transparencia es fundamental, la conservación documental emerge como un componente para la eficacia y la legitimidad institucional a lo largo del tiempo.

2.3.5. Cultura Organizacional y Conciencia de Seguridad

La influencia de la cultura organizacional en la implementación efectiva de medidas de seguridad es un factor determinante en la capacidad de una organización para proteger sus activos de información, la cultura organizacional, que abarca valores compartidos, normas y comportamientos dentro de la entidad, crea el contexto en el cual las iniciativas de seguridad se desarrollan y son adoptadas (Giraldo Bedoya & Arias Vanegas, 2020, pp. 9-10).

Una cultura organizacional sólida y orientada hacia la seguridad establece las bases para que la seguridad sea una prioridad en todos los niveles de la organización, cuando la seguridad es parte integral de los valores y principios de la empresa, los empleados tienden a internalizar la urgencia de proteger la información sensible (Cardona Fernández & Restrepo Granada, 2020, pp. 7-8), este compromiso cultural no solo impulsa el cumplimiento de políticas de seguridad, sino que también fomenta un sentido de responsabilidad colectiva hacia la protección de activos críticos.

La influencia cultural se refleja en la actitud de los empleados hacia la seguridad de la información, en un entorno donde la cultura promueve la conciencia y la responsabilidad en seguridad, los empleados están más propensos a seguir buenas prácticas, reportar incidentes y participar activamente en programas de capacitación (Giraldo Bedoya & Arias Vanegas, 2020, p. 10). Esta actitud proactiva es esencial para mitigar riesgos, ya que los empleados son la primera línea de defensa contra amenazas internas y externas.

Por otro lado, en organizaciones con una cultura menos orientada hacia la seguridad, las medidas de seguridad pueden enfrentar resistencia o ser percibidas como obstáculos para la eficiencia operativa, en estos casos, la implementación de políticas y controles puede encontrarse con desafíos, y la conciencia sobre la importancia de la seguridad puede ser baja (Garzón Barón, 2018, pp. 57-58).

La cultura organizacional influye directamente en cómo se percibe y se implementa la seguridad en una organización. Una cultura sólida y orientada hacia la seguridad crea un entorno propicio para la adopción efectiva de medidas de seguridad, mientras que una cultura débil puede obstaculizar la implementación y eficacia de estas medidas. Por lo tanto, la promoción de una

cultura organizacional proactiva en seguridad es esencial para fortalecer la postura de una organización frente a las crecientes amenazas de seguridad (Cardona Fernández & Restrepo Granada, 2020, p. 10).

La influencia de la cultura organizacional en la implementación de medidas de seguridad es fundamental, una cultura sólida y orientada hacia la seguridad establece normas y expectativas claras en cuanto a prácticas seguras al fomentar la conciencia de seguridad entre los empleados, en contraste, una cultura débil puede generar resistencia a la adopción de medidas de seguridad, incluso si están formalmente establecidas (Garzón Barón, 2018, p. 60).

La cultura organizacional proactiva en seguridad impulsa la colaboración, la responsabilidad compartida y la valoración de la seguridad como parte integral de las operaciones diarias, este enfoque se centra en la implementación de controles técnicos, para abarcar la participación activa y la toma de decisiones informadas por parte de todo el personal. La promoción de una mentalidad de seguridad en todos los niveles de la organización contribuye a crear un entorno en el que la seguridad se considera una responsabilidad colectiva.

2.4. Contexto Institucional

El contexto institucional de la Gobernación del Magdalena hace referencia al entorno organizativo, administrativo y político que rodea a esta entidad gubernamental. La Gobernación del Magdalena es la máxima autoridad ejecutiva del departamento colombiano de Magdalena y desempeña un papel en la gestión y coordinación de políticas, programas y recursos para el desarrollo y bienestar de la región, a continuación, se proporcionan aspectos clave que definen el contexto institucional de la Gobernación del Magdalena (Gobernación del Magdalena, 2023):

Ubicación Geográfica: La Gobernación opera en el departamento de Magdalena, situado en la región Caribe de Colombia, la ubicación geográfica puede influir en las prioridades y desafíos específicos que enfrenta la entidad, como cuestiones relacionadas con el desarrollo económico, la infraestructura y la gestión ambiental.

Estructura Organizativa: La Gobernación cuenta con una estructura organizativa que incluye diversas dependencias y secretarías encargadas de áreas específicas, como salud,

educación, desarrollo económico, entre otras. La forma en que estas unidades interactúan y colaboran puede impactar la eficacia en la implementación de políticas y proyectos.

Funciones y Competencias: La Gobernación del Magdalena tiene competencias y responsabilidades específicas en áreas como la planificación del desarrollo, la ejecución de proyectos de inversión, la atención a la población vulnerable, y la coordinación con los municipios dentro de su jurisdicción. Comprender estas funciones es esencial para evaluar su impacto en el contexto más amplio.

Marco Normativo y Legal: La actuación de la Gobernación está sujeta a un marco normativo y legal que establece las reglas y regulaciones para su funcionamiento. Esto incluye leyes nacionales y normativas específicas que rigen las actividades gubernamentales a nivel departamental.

Relaciones Intergubernamentales: La Gobernación del Magdalena mantiene relaciones con otras entidades gubernamentales a nivel local, regional y nacional, la colaboración y coordinación con estas instituciones sirven para abordar temas que trascienden los límites del departamento y para acceder a recursos y apoyo adicionales.

En el ámbito de la seguridad de la información y gestión documental, el contexto institucional puede influir en las políticas, prácticas y desafíos específicos que la Gobernación del Magdalena enfrenta al proteger su acervo documental o garantizar la confidencialidad, integridad y disponibilidad de la información.

2.5. Marco Normativo y Regulatorio

Dado que la investigación se centra en el contexto gubernamental, especialmente en la Gobernación del Magdalena, es importante considerar las normas y regulaciones aplicables en el ámbito colombiano, se presenta un cuadro con normativas relevantes, sus objetivos y alcances.

Tabla 1, Normas y regulaciones

Nombre de la Norma o Regulación	Objetivo	Alcance
Ley 1712 de 2014 - Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional (Congreso de la República, 2014)	Garantizar el derecho fundamental de acceso a la información y promover la transparencia en la gestión pública.	Se aplica a todas las entidades públicas, incluyendo la Gobernación del Magdalena, y establece obligaciones para la publicación de información.
Decreto 2150 de 1995, Reglamentario del Archivo General de la Nación (Congreso de la República, 1995)	Regular las actividades archivísticas del Estado y garantizar la conservación y acceso a los documentos.	Aplica a todas las entidades públicas y establece normas para la gestión documental, archivo y acceso a la información pública.
Resolución 3573 de 2011 , por la cual se establecen los requisitos del Sistema de Gestión de Seguridad de la Información para el sector público (Congreso de la Republica, 2011)	Definir los requisitos mínimos para implementar un Sistema de Gestión de Seguridad de la Información (SGSI) en entidades públicas.	Se aplica a todas las entidades del sector público, incluyendo la Gobernación del Magdalena, que manejan información sensible.
ISO 27001:2013, Sistemas de Gestión de Seguridad de la Información (SGSI) (Rodriguez Baca et al., 2020)	Establecer requisitos para implementar, mantener y mejorar un SGSI que permita a una organización gestionar	Aplicable a cualquier tipo de organización, incluyendo entidades gubernamentales como la Gobernación del Magdalena, independientemente de su

	de manera sistemática la seguridad de la información.	tamaño o sector. Se centra en proteger la confidencialidad, integridad y disponibilidad de la información.

Nota: Normas y regulaciones concernientes a la investigación, autoría propia.

3. Capítulo, Marco Metodológico

En el capítulo de Marco Metodológico, se establece un enfoque mixto que combina elementos inductivos y deductivos, ofreciendo una estrategia integral para la investigación sobre la implementación de ISO 27001 en el Archivo Central de la Gobernación del Magdalena, este enfoque mixto permite explorar y comprender a fondo el contexto de la seguridad documental, integrando observaciones específicas con teorías generales para una visión completa del fenómeno.

La investigación adopta un diseño descriptivo comparativo, permitiendo un análisis detallado de las prácticas actuales en relación con los estándares internacionales, a través de un método de estudio de caso comparativo, se profundiza en las particularidades del Archivo Central, facilitando la identificación de debilidades y áreas de mejora en el acceso a la información gestionada por INFODOC. El análisis de contenido se utiliza como técnica principal para examinar documentos relevantes, mientras que la matriz de análisis documental actúa como instrumento clave para la recopilación y organización de datos, estas fases metodológicas, desde la exploración y preparación hasta la formulación de conclusiones y propuestas de mejora, aseguran un análisis riguroso y contextualizado, proporcionando una base sólida para la mejora de la seguridad documental en la institución.

3.1. Enfoque de Investigación

El enfoque mixto, que amalgama tanto elementos inductivos como deductivos, es útil como una estrategia metodológica integral para enfrentar los objetivos de investigación de manera holística, al fusionar la capacidad de descubrimiento inherente al enfoque inductivo con la estructura lógica característica del enfoque deductivo, se posibilita la obtención de una visión más completa y detallada del fenómeno bajo estudio (Binda & Balbastre-Benavent, 2013, p. 180). En el marco de este enfoque, la investigación inductiva se inicia con observaciones específicas que actúan como puntos de partida para derivar conclusiones generales, este proceso permite explorar a fondo el contexto, identificar patrones emergentes y capturar matices que podrían pasar desapercibidos en un enfoque más rígido.

Por otro lado, la investigación deductiva comienza desde un nivel más abstracto al partir de teorías generales, estas teorías sirven como marco conceptual para formular hipótesis específicas que, a su vez, se someten a prueba mediante la recopilación y análisis de datos, la solidez lógica del enfoque deductivo aporta una estructura robusta a la investigación, permitiendo la evaluación sistemática de las hipótesis y la validación de las conclusiones alcanzadas (Hernández Sampieri & Mendoza Torres, 2018, p. 320). Esta combinación de enfoques potencia la capacidad del investigador para interpretar y comprender tanto la amplitud como la profundidad del fenómeno estudiado.

El enfoque mixto ofrece una estrategia metodológica equilibrada que optimiza las fortalezas de la investigación inductiva y deductiva, al integrar la exploración inductiva con la validación deductiva, se maximiza la comprensión del fenómeno, al generar conocimientos robustos y fundamentados, este enfoque se revela como una herramienta valiosa para abordar la complejidad inherente a la investigación, al permitir al investigador capturar la riqueza contextual del fenómeno y validar sus descubrimientos dentro de un marco teórico sólido (Binda & Balbastre-Benavent, 2013, p. 188).

Este enfoque mixto resulta particularmente beneficioso al aplicar técnicas cualitativas, como el análisis documental, en la fase deductiva, se establece una sólida revisión teórica que defina categorías y variables de interés, proporcionando una estructura inicial para el análisis documental. En la fase inductiva, el análisis documental permite descubrir patrones y características emergentes en los documentos, sin imponer estructuras predefinidas, esto posibilita una exploración más profunda de la información contenida en los documentos y la captura de matices no anticipados.

La complementariedad de ambos enfoques brinda una integralidad a la investigación, permitiendo una comprensión más completa y contextualizada del fenómeno estudiado. En el contexto del análisis documental, esta combinación resulta en una investigación más rigurosa y fundamentada, aprovechando la flexibilidad de los métodos cualitativos y la validez de los enfoques deductivos.

3.2. Tipo de Investigación

La investigación descriptiva comparativa es una modalidad que combina dos enfoques esenciales para obtener una comprensión completa y detallada del fenómeno bajo estudio, la investigación descriptiva se caracteriza por su capacidad para describir con precisión las características y propiedades de un fenómeno, al proporcionar un análisis detallado de la situación actual, este enfoque es especial útil cuando se busca entender la naturaleza y las particularidades de un contexto específico (Bernal Torres, 2016, p. 25).

La vertiente comparativa añade un componente valioso al proceso, para contrastar la situación actual con estándares, modelos o referencias reconocidas, la comparación facilita la identificación de similitudes, diferencias y brechas entre las prácticas observadas y los criterios establecidos. En este sentido, la investigación comparativa proporciona una base objetiva para evaluar el desempeño y la eficacia de las prácticas en relación con un marco de referencia externo (Briones, 2022, p. 39).

En el contexto específico de la investigación sobre la seguridad documental en el Archivo Central de la Gobernación del Magdalena, la elección de una investigación descriptiva comparativa está justificada por la necesidad de abordar dos objetivos cruciales: identificar debilidades existentes y comparar las prácticas actuales con los estándares establecidos por ISO 27001.

La investigación descriptiva permite realizar un análisis detallado de las prácticas de seguridad documental en el Archivo Central, proporciona una descripción completa de la situación actual, este enfoque descriptivo sirve para comprender las complejidades y particularidades del entorno de gestión documental de la institución.

La vertiente comparativa, por su parte, se utiliza para evaluar la eficacia de las prácticas actuales al confrontarlas con los estándares de la norma ISO 27001, esta comparación permite identificar áreas de conformidad, pero también señala las debilidades y discrepancias existentes. Asimismo, proporcionará un marco sólido para proponer mejoras y ajustes que alineen las prácticas del Archivo Central con los estándares internacionales de seguridad de la información.

La elección de una investigación descriptiva comparativa se justifica por su capacidad para proporcionar un análisis detallado de las prácticas actuales del Archivo Central, al mismo tiempo que facilita la evaluación objetiva de su conformidad con los estándares ISO 27001, contribuyendo así a la identificación de debilidades y la propuesta de soluciones fundamentadas.

3.3. Método

La elección del método de estudio de caso comparativo para investigaciones ofrece una perspectiva metodológica robusta y versátil que puede aplicarse a una variedad de contextos, este enfoque metodológico se destaca por su capacidad para proporcionar una comprensión detallada y contextualizada de fenómenos específicos, al tiempo que permite comparaciones estructuradas o rigurosas entre casos particulares (Muñoz, 2015, pp. 22-23). Desde una perspectiva general, el estudio de caso comparativo se convierte en una herramienta valiosa para explorar, entender y analizar complejidades dentro de situaciones específicas.

La elección de emplear un método de estudio de caso comparativo en la investigación del Archivo Central de la Gobernación del Magdalena se justifica por su adaptabilidad y profundidad analítica en contextos específicos. Este enfoque metodológico se alinea de manera efectiva con los objetivos de la investigación, al proporcionar una estructura que aborda las complejidades inherentes a la seguridad documental en una institución gubernamental

El estudio de caso comparativo permite una inmersión detallada en el análisis de situaciones específicas, como el acceso a la información administrada por INFODOC, esta metodología posibilita una comprensión exhaustiva de las debilidades identificadas, permitiendo un abordaje detallado y contextualizado.

La naturaleza contextual del estudio de caso garantiza que las debilidades identificadas estén arraigadas en las circunstancias particulares del Archivo Central, esta contextualización facilita la formulación de soluciones específicas y adaptadas a la realidad de la institución. Al incorporar un enfoque comparativo, el método proporciona un marco objetivo para evaluar las prácticas actuales en relación con la norma ISO 27001, esto permite destacar las brechas y similitudes, fundamentales para la identificación de áreas de mejora.

El análisis comparativo señala debilidades como áreas de fortaleza, esto faculta al Archivo Central reconocer y fortalecer aquellas prácticas que cumplen con los estándares, fomentando una mejora continua. Aunque el estudio de caso se centra en una institución específica, sus resultados ofrecen percepciones valiosas para instituciones similares, la generalización es limitada pero las conclusiones pueden ser aplicables y transferibles a contextos afines.

El método de estudio de caso comparativo se elige debido a su capacidad para proporcionar una exploración detallada y contextualizada de las debilidades en el acceso a la información administrada por INFODOC, además, facilita una comparación estructurada de las prácticas actuales con los estándares ISO 27001, al garantizar resultados específicos y pertinentes para mejorar la seguridad documental en el Archivo Central de la Gobernación del Magdalena.

3.4. Técnica de Investigación

El análisis de contenido es una técnica útil en esta investigación, centrada en la implementación de la norma ISO 27001 en el Archivo Central de la Gobernación del Magdalena. Esta técnica se basa en un enfoque sistemático y objetivo para examinar documentos relevantes, permitiendo una comprensión profunda y detallada de la información contenida en ellos (Barrón de Olivares & D'Aquino, 2020, pp. 56-57).

El proceso comienza con la definición clara de los objetivos de la investigación y la identificación de las variables clave que se investigarán, esto establece el marco para la selección de documentos pertinentes, asegurando que solo se analicen aquellos que proporcionen información valiosa y relevante, a continuación, se crea una matriz estructurada para facilitar la categorización y codificación de la información. Esta matriz permite la recopilación de datos cualitativos y cuantitativos de manera organizada (Bernal Ibarra, 2018, pp. 7-8).

Una vez completada la matriz para cada documento, se procede al análisis detallado de la información recopilada, este análisis no solo incluye aspectos cualitativos, como la identificación de temas, tendencias y patrones, sino también aspectos cuantitativos cuando sea posible, al interpretar los resultados, se consideran los objetivos de la investigación para proporcionar una visión completa y contextualizada de los hallazgos, que luego se presentan claramente en un informe.

La elección del análisis de contenido como técnica se justifica por su capacidad para permitir una recopilación detallada y exhaustiva de información tanto cualitativa como cuantitativa. Esta técnica es versátil y estructurada, facilitando la sistematización y análisis de documentos, lo que se alinea perfectamente con los objetivos de la investigación en el Archivo Central de la Gobernación del Magdalena.

El análisis de contenido proporciona una estructura organizada para la recopilación de datos al asignar categorías específicas y criterios de evaluación. Esto no solo facilita la sistematización de la información contenida en los documentos, sino que también permite un análisis eficiente y estructurado, esta técnica faculta la captura detallada de información cualitativa a través de categorías específicas y campos de análisis, registrando detalles, tendencias y patrones cualitativos relevantes que enriquecen la visión del contenido documental (Ferreiro Gravié, 2017, p. 9).

El análisis de contenido facilita la comparación entre diferentes documentos y casos, al tener criterios estandarizados, es posible identificar patrones comunes o discrepancias, lo que contribuye significativamente a la comparación de las prácticas actuales con los estándares ISO 27001. Esta técnica es adaptable a diversos tipos de documentos, desde políticas y procedimientos hasta informes y registros, asegurando su aplicabilidad a una amplia gama de materiales documentales presentes en el Archivo Central.

El análisis de contenido se destaca como una técnica que combina la capacidad de capturar información cualitativa detallada con la posibilidad de cuantificar aspectos relevantes. Su estructura organizada y adaptable la convierte en una herramienta idónea para esta investigación, proporcionando una recopilación de datos rigurosa y un análisis posterior que respalda de manera efectiva los objetivos de la investigación en el Archivo Central de la Gobernación del Magdalena.

3.5. Instrumento

La matriz de análisis documental se basa en un enfoque sistemático para examinar documentos relevantes en una investigación., inicia con la definición clara de objetivos y variables, seguida de la selección de documentos pertinentes. La creación de una matriz estructurada facilita la categorización y codificación de la información, permite la recopilación de datos cualitativos y

cuantitativos (Bernal Ibarra, 2018, pp. 7-8). Tras llenar la matriz para cada documento, se procede al análisis, al incluir aspectos cuantitativos donde sea posible, los resultados se interpretan en el contexto de los objetivos y se presentan de manera clara en un informe.

La elección de la matriz de análisis documental como instrumento para la recolección de datos se basa en su eficacia para permitir una recopilación detallada de información cualitativa y cuantitativa, este instrumento se revela como una herramienta versátil y estructurada que facilita la sistematización con el análisis exhaustivo de documentos, alineándose con los objetivos de la investigación en el Archivo Central de la Gobernación del Magdalena.

La matriz de análisis documental proporciona una estructura organizada para la recopilación de datos, al asignar categorías específicas y criterios de evaluación, se facilita la sistematización de la información contenida en los documentos, permite un análisis eficiente y estructurado, faculta la captura detallada de información cualitativa presente en los documentos, a través de categorías específicas y campos de análisis, se pueden registrar detalles, tendencias y patrones cualitativos relevantes, proporcionando una visión enriquecida del contenido documental (Ferreiro Gravié, 2017, p. 9).

La estructura de la matriz facilita la comparación entre diferentes documentos y casos, al tener criterios estandarizados, se pueden identificar patrones comunes o discrepancias, contribuyendo significativamente a la comparación de prácticas actuales con estándares ISO 27001. La matriz puede adaptarse a diversos tipos de documentos, desde políticas y procedimientos hasta informes y registros, esta versatilidad asegura que el instrumento sea aplicable a una amplia gama de materiales documentales presentes en el Archivo Central.

La matriz de análisis documental se destaca como un instrumento que combina la capacidad de capturar información cualitativa detallada con la posibilidad de cuantificar aspectos relevantes, su estructura organizada y adaptable lo convierte en una herramienta idónea para la investigación en el Archivo Central de la Gobernación del Magdalena, con una recopilación de datos rigurosa y su posterior análisis que respalde de manera efectiva los objetivos de la investigación.

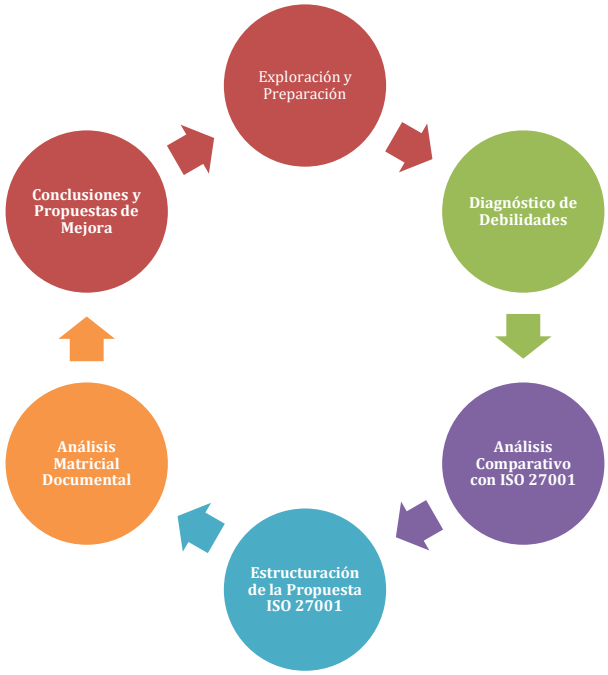
3.6. Fases de Investigación

Estas fases se articulan de manera lógica y secuencial, permitiendo abordar de manera integral los objetivos de la investigación y proporcionando una base sólida para el análisis y la discusión de los resultados en el capítulo subsiguiente.

a. **Exploración y Preparación:** En esta fase inicial, se lleva a cabo una revisión bibliográfica para comprender el marco teórico y contextual de la seguridad documental, la investigación inductiva permite explorar observaciones específicas y patrones emergentes en la gestión documental del Archivo Central de la Gobernación del Magdalena.
b. **Diagnóstico de Debilidades:** Se implementa un método analítico centrado en el análisis documental para diagnosticar las debilidades en el acceso a la información gestionada por INFODOC, utiliza la técnica de análisis de distintas fuentes, se identifican áreas susceptibles de mejora y se establece una base para la fase deductiva.
c. **Análisis Comparativo con ISO 27001:** En esta etapa, se emplea la investigación deductiva para analizar las prácticas actuales en el Archivo Central y compararlas con los estándares de la norma ISO 27001, la elección de la investigación descriptiva comparativa permite evaluar la conformidad y destacar similitudes o discrepancias.
d. **Estructuración de la Propuesta ISO 27001:** Basándose en los resultados obtenidos, se procede a estructurar la propuesta para la implementación de la norma ISO 27001 en el Archivo Central de la Gobernación del Magdalena, esta fase involucra la formulación de recomendaciones específicas basadas en las debilidades identificadas y la comparación con los requisitos ISO.
e. **Análisis Matricial Documental:** La técnica de investigación seleccionada, el análisis documental mediante una matriz estructurada se aplica en esta fase para recopilar datos cualitativos y cuantitativos, la matriz de análisis documental actúa como un instrumento eficaz para organizar, categorizar y evaluar la información contenida en documentos clave relacionados con la seguridad documental.
f. **Conclusiones y Propuestas de Mejora:** La fase final implica la síntesis de los resultados obtenidos a lo largo de la investigación, se analizan las debilidades identificadas, las comparaciones con ISO 27001 y la información recopilada mediante la matriz de análisis

documental. Se formulan conclusiones detalladas y se proponen recomendaciones específicas para fortalecer la seguridad documental en el Archivo Central.

Figura 2, Fases de Investigación



Nota: El grafico muestra las respuestas de los 16 participantes a la pregunta uno del instrumento, autoría propia.

4. Capítulo, Análisis y Discusión de Resultados

La propuesta para la implementación de la Norma ISO 27001 en el Archivo Central de la Gobernación del Departamento del Magdalena se sustenta en una investigación metódica y estructurada que busca asegurar la seguridad del acervo documental, el objetivo general es determinar los elementos de seguridad necesarios en el marco de esta norma internacional, para alcanzar este objetivo, se han delineado varios objetivos específicos y fases de investigación.

En primer lugar, el diagnóstico de las debilidades y falencias del acceso a la información administrada por el software INFODOC es clave, este diagnóstico se aborda en la fase de Diagnóstico de Debilidades, donde se utiliza un método analítico centrado en el análisis documental, se identifican áreas susceptibles de mejora mediante la técnica de análisis de distintas fuentes, este proceso proporciona una base sólida para entender las deficiencias actuales y establece la dirección para las siguientes fases de la investigación.

A continuación, la fase de Análisis Comparativo con ISO 27001 se enfoca en identificar las prácticas actuales de gestión de seguridad de la información en el Archivo Central y compararlas con los requisitos de la Norma ISO 27001, la investigación deductiva y la descriptiva comparativa son empleadas para evaluar la conformidad de las prácticas existentes con los estándares internacionales, esta comparación resalta las similitudes y discrepancias, sino que también subraya las áreas que requieren mejoras para alinearse con la norma.

La fase de Estructuración de la Propuesta ISO 27001 sigue lógicamente, donde se formulan recomendaciones específicas basadas en los resultados de las fases anteriores, esta etapa es necesaria para estructurar los elementos necesarios para la implementación de la norma en el Archivo Central, asegurando que las recomendaciones sean precisas y fundamentadas en las debilidades diagnosticadas y las comparaciones realizadas.

El Análisis Matricial Documental, otra fase fundamental, se centra en recopilar datos cualitativos y cuantitativos sobre la seguridad documental, por el uso de una matriz estructurada, esta técnica permite organizar, categorizar y evaluar la información contenida en documentos clave, este análisis actúa como un instrumento eficaz para entender mejor los aspectos críticos de la seguridad documental.

Finalmente, la fase de Conclusiones y Propuestas de Mejora sintetiza todos los hallazgos, se analizan las debilidades identificadas, las comparaciones con ISO 27001 y los datos recopilados mediante la matriz documental, las conclusiones detalladas y las recomendaciones específicas se formulan para fortalecer la seguridad documental en el Archivo Central, esta fase asegura que los resultados de la investigación sean prácticos y aplicables, proporcionando una guía clara para la implementación efectiva de la Norma ISO 27001.

Cada fase de la investigación está diseñada para abordar de manera integral los objetivos específicos, asegurando que la propuesta para la implementación de la Norma ISO 27001 en el Archivo Central de la Gobernación del Departamento del Magdalena sea exhaustiva, precisa y basada en un análisis riguroso y detallado.

4.1. Norma ISO 27001

La elección estratégica de incorporar la Norma ISO 27001 y el Plan Institucional de Archivos (PINAR) de la Gobernación del Magdalena para el periodo 2020-2023 como documentos de análisis documental, se respalda en su relevancia y funciones complementarias. La Norma ISO 27001, reconocida globalmente en el ámbito de la seguridad de la información, emerge como un marco de referencia internacional al establecer los requisitos para un sistema de gestión de seguridad de la información, su inclusión en la metodología permite evaluar las prácticas del Archivo Central en consonancia con estándares globalmente aceptados, facilitando así la identificación de posibles brechas y áreas de mejora.

En paralelo, el Plan Institucional de Archivos (PINAR) de la Gobernación del Magdalena para el periodo 2020-2023, como documento interno, constituye la política interna de la institución al delinear las directrices, procesos y procedimientos internos para la organización y seguridad de documentos. Al analizar este documento, se busca comprender la realidad interna de la institución y contrastarla con los estándares externos establecidos por la ISO 27001.

El diagnóstico de las debilidades y falencias en el acceso a la información, administrada por el software INFODOC, se realiza mediante el análisis del PINAR, este enfoque se orienta a identificar las posibles deficiencias en la gestión de la información, considerando tanto los lineamientos internos establecidos por el PINAR como los estándares internacionales propuestos

por la Norma ISO 27001. De esta manera, se busca una comprensión integral de las prácticas actuales de gestión de seguridad de la información en el Archivo Central de la Gobernación del Magdalena.

La matriz comparativa actúa como una herramienta en este análisis, al propiciar una estructura organizada para visualizar sistemáticamente las similitudes o diferencias entre la normativa internacional y la política interna de gestión documental, esta herramienta facilita la identificación de áreas de convergencia y divergencia, ofreciendo una base objetiva que evalúa el grado de alineación entre las prácticas internas de la Gobernación del Magdalena y los estándares internacionales en seguridad de la información.

4.1.1. Objetivos de la Norma

La ISO 27001 tiene como objetivo principal proporcionar un marco sistemático y efectivo para la gestión de la seguridad de la información en organizaciones, este estándar, de la era digital, busca instaurar un enfoque proactivo y basado en riesgos para identificar, gestionar y mitigar amenazas a la seguridad de la información, para asegurar la confidencialidad, integridad y disponibilidad de los datos, a través de un ciclo de mejora continua, la norma aborda aspectos técnicos, considera el contexto organizacional y se adapta a las particularidades de cada entidad, contribuyendo no solo a la protección de la información, sino también al logro de objetivos estratégicos y al desarrollo sostenible (Arévalo Ascanio et al., 2015, p. 128).

La ISO 27001 establece directrices estáticas y proporciona un marco dinámico adaptable, incorporando la seguridad de la información como un proceso integral que se alinea con los objetivos organizacionales, permitiendo a las empresas enfrentar los desafíos digitales de manera efectiva.

4.1.2. Planificar, Hacer, Verificar, Actuar (PHVA)

La ISO 27001 adopta un enfoque basado en el ciclo PHVA (Planificar, Hacer, Verificar, Actuar), que constituye un pilar para la implementación y mantenimiento efectivo de un Sistema de Gestión de Seguridad de la Información (SGSI), en la fase de Planificar, se establecen los objetivos y procesos necesarios para alcanzar resultados específicos, para identificar riesgos y definir estrategias de seguridad (Chávarry Bonilla, 2021, p. 56). La etapa de Hacer implica la

implementación de los planes y procesos diseñados, poniendo en práctica las medidas de seguridad previamente definidas.

La fase de Verificar implica la monitorización y evaluación constante del desempeño del SGSI, mediante auditorías internas y revisiones periódicas. Esta evaluación busca asegurar que se estén cumpliendo los objetivos de seguridad y, en caso necesario, se realicen ajustes para mejorar la efectividad del sistema. Finalmente, en la etapa de Actuar, se implementan acciones correctivas y preventivas derivadas de las evaluaciones anteriores, cerrando así el ciclo PDCA; este enfoque cíclico no solo garantiza la implementación inicial de medidas de seguridad, sino que también promueve la adaptabilidad del SGSI a medida que evolucionan las amenazas y cambios en el entorno organizacional.

4.1.3. Contexto Organizacional Según ISO

La consideración del contexto organizacional, como enfatiza la ISO 27001, es útil para la investigación en el Archivo Central de la Gobernación del Magdalena, esta atención al contexto implica una evaluación profunda de los factores tanto externos como internos que influyen en la seguridad de la información. En el ámbito externo, se deben analizar las dinámicas gubernamentales, las regulaciones específicas del sector y las posibles amenazas que puedan afectar la seguridad documental, a nivel interno, se debe tener en cuenta la estructura organizativa, las políticas y los procesos de gestión documental existentes.

La alineación del Sistema de Gestión de Seguridad de la Información (SGSI) con los objetivos estratégicos de la organización refuerza la relevancia de esta consideración, la investigación busca identificar debilidades en la seguridad documental, al evaluar cómo estas prácticas se integran con la misión y visión más amplias de la Gobernación del Magdalena, el entendimiento de este contexto mejora la efectividad del SGSI, al fortalecer el argumento para proponer mejoras y ajustes que estén alineados con los objetivos estratégicos específicos de la institución.

4.1.4. Sobre los Riesgos

Esta norma establece la necesidad de que las organizaciones realicen un análisis exhaustivo de los riesgos asociados a la seguridad de la información, en el contexto de la investigación, este

enfoque implica identificar las posibles amenazas a la seguridad documental, evaluar tanto su impacto potencial como la probabilidad de ocurrencia, para desarrollar estrategias o medidas que gestionen y mitiguen los riesgos.

La aplicación de la evaluación de riesgos en la investigación contribuye directamente a la identificación de debilidades en la seguridad documental del Archivo Central, al comprender los riesgos específicos a los que se enfrenta la gestión documental en la institución, se pueden proponer soluciones y mejoras más efectivas y adaptadas. Este enfoque proactivo, basado en la identificación y gestión de riesgos, fortalece la seguridad de la información, al establecer un marco para la toma de decisiones informadas y estratégicas en el ámbito de la gestión documental.

4.1.5. La Protección de los Datos

Se establece la obligación en las organizaciones de crear y documentar una política de seguridad de la información que refleje el compromiso de la alta dirección con la seguridad de los datos, en el contexto de la investigación, la formulación de esta política se convierte en un pilar para el desarrollo y la implementación efectiva del Sistema de Gestión de Seguridad de la Información (SGSI).

Al proporcionar un marco claro y formal que guie las prácticas de seguridad en el Archivo Central, se establecen estas políticas, la alta dirección manifiesta su compromiso con la protección de la información y son sentadas las bases para una planificación estructurada del SGSI. Este enfoque asegura que la seguridad de la información sea considerada una prioridad estratégica y que se integre de manera coherente en todas las operaciones y procesos del Archivo Central, la existencia de una política documentada facilita la comunicación interna y externa de los principios o compromisos de seguridad, al promover la transparencia y la confianza en la gestión documental de la institución.

4.1.6. Los Responsables de la Seguridad

Este requisito se alinea directamente con la investigación del Archivo Central de la Gobernación del Magdalena, ya que aborda la necesidad de establecer un marco organizativo sólido para la gestión de la seguridad de la información. La norma establece que la asignación de

roles y responsabilidades garantiza que las funciones relacionadas con la seguridad de la información sean claramente definidas y entendidas en toda la institución.

En el contexto de la investigación, este aspecto cobra relevancia al identificar la necesidad de designar un responsable de seguridad de la información en el Archivo Central, la definición de roles específicos, como el responsable de seguridad de la información, asegura que haya una supervisión efectiva del SGSI, la participación activa de la alta dirección en la supervisión del SGSI fortalece el compromiso institucional con la seguridad de la información. Establecer roles y responsabilidades claros contribuye a la eficacia y eficiencia en la implementación y mantenimiento del SGSI, se asegura que cada componente esté bajo la supervisión adecuada y fomenta una cultura organizacional centrada en la seguridad documental.

4.1.7. Planificación y Control

La planificación se vuelve básica para anticipar y abordar posibles amenazas a la seguridad de la información, la norma establece la necesidad de desarrollar controles operativos en áreas clave como el acceso, la adquisición y el desarrollo de sistemas, y la gestión de incidentes de seguridad. En el contexto de la investigación, estos elementos pueden traducirse en la implementación de políticas y procedimientos específicos para regular el acceso a la información, asegurar la seguridad en el desarrollo de sistemas y establecer un marco robusto para gestionar incidentes de seguridad.

Este enfoque se alinea con la metodología propuesta para la investigación, que incluye un análisis documental detallado al usar la Norma ISO 27001 como referencia, al considerar la planificación y el control operativo, la investigación evalúa cómo el Archivo Central de la Gobernación del Magdalena aborda estas áreas críticas, se identifican posibles brechas y proponen mejoras específicas para fortalecer la seguridad documental en cada uno de estos aspectos.

4.1.8. Sobre la Auditoria Interna y Revisión

La norma ISO 27001, al enfocarse en auditorías internas y revisiones por la dirección, establece una sólida estructura para evaluar y mejorar continuamente el Sistema de Gestión de Seguridad de la Información (SGSI), las auditorías internas, al ser realizadas de manera periódica, ofrecen una evaluación detallada de los controles de seguridad implementados, identifican posibles

vulnerabilidades y áreas de mejora; por otro lado, la revisión por la dirección garantiza una evaluación estratégica del SGSI, para asegurar su alineación con los objetivos más amplios de la organización.

En el contexto de la investigación propuesta para el Archivo Central de la Gobernación del Magdalena, estas prácticas son valiosas, ya que proporcionan un marco estructurado para la mejora continua y la adaptabilidad del sistema de seguridad documental en respuesta a cambios organizativos y de seguridad, los requisitos de auditoría interna y revisión por la dirección, según la ISO 27001, refuerzan la importancia de la supervisión activa y el compromiso de la alta dirección en la seguridad de la información.

4.1.9. Mejora Continua

La ISO 27001, al destacar la mejora continua, establece un principio clave para la adaptabilidad y eficacia a largo plazo del Sistema de Gestión de Seguridad de la Información (SGSI), este enfoque implica una revisión constante de la eficacia de los controles de seguridad implementados, lo que permite identificar áreas de oportunidad y ajustar estrategias en respuesta a la evolución de las amenazas y al entorno organizativo.

La mejora continua también aborda la necesidad de adaptarse a cambios tecnológicos y normativos, asegura que el SGSI se mantenga alineado con las mejores prácticas y estándares de seguridad, en el contexto de la investigación propuesta, este énfasis en la mejora continua proporciona un marco para el desarrollo y la optimización continuos de las prácticas de seguridad documental, asegurando la relevancia y efectividad a largo plazo del sistema.

En el ámbito de la seguridad documental en una institución gubernamental como el Archivo Central, la ISO 27001, al resaltar la mejora continua, orienta hacia la implementación de procesos dinámicos y la capacidad de adaptación a las cambiantes necesidades o desafíos en la gestión de la información, este enfoque fortalece la resiliencia del SGSI frente a amenazas potenciales, al garantizar que la seguridad documental evoluciona de manera concertada con los avances tecnológicos y los cambios en el entorno normativo.

La combinación de elementos clave de la norma ISO 27001 argumenta convincentemente su utilidad en la investigación propuesta para el Archivo Central de la Gobernación del Magdalena.

El objetivo principal de establecer un marco sistemático y proactivo para la gestión de la seguridad de la información destaca la importancia de abordar este tema de manera integral, el enfoque basado en el ciclo PHVA proporciona una estructura organizada para la implementación y mantenimiento del SGSI, al asegurar la continuidad y eficacia del sistema, la consideración del contexto organizacional y la evaluación de riesgos refuerzan la necesidad de adaptar las prácticas de seguridad a las circunstancias específicas o de anticiparse a posibles amenazas.

La norma exige la formulación de una política de seguridad documentada, la asignación de roles y responsabilidades claros, así como la planificación y control operativo, al asegurar una gestión coherente y estructurada de la seguridad de la información, la incorporación de auditorías internas y revisiones por la dirección garantiza la supervisión y mejora constantes del SGSI. Finalmente, la perspectiva de mejora continua subraya la necesidad de adaptarse y evolucionar a lo largo del tiempo, estos elementos, en conjunto, respaldan la aplicabilidad y eficacia de la ISO 27001 en el contexto de la seguridad documental, ofreciendo un marco integral y dinámico para abordar los desafíos y riesgos asociados con la gestión de la información en el Archivo Central.

4.2. Plan Institucional de Archivos (PINAR) Gobernación Magdalena 2020- 2023

4.2.1. Objetivos del PINAR

El Plan Institucional de Archivos (PINAR) de la Gobernación de Magdalena para el período 2020-2023 tiene como objetivo principal la mejora sustancial de la gestión documental en la entidad. En este sentido, el PINAR surge como una respuesta estratégica a las normativas gubernamentales, en particular, a la Ley General de Archivos (Ley 594 de 2000) y decretos asociados, el cumplimiento de estas normas garantiza la validez legal de los documentos producidos y recibidos por la Gobernación, al establecer una base sólida para la transparencia y la rendición de cuentas.

La eficiencia operativa también se encuentra en el núcleo del objetivo del PINAR, la optimización de procesos relacionados con la gestión documental busca reducir los tiempos dedicados a estas tareas, con la mejora de la precisión y la rapidez en la recuperación de la información, esto se traduce en una administración más efectiva de los recursos, para permitir que

la Gobernación atienda de manera más ágil las demandas y requerimientos relacionados con los documentos y archivos bajo su custodia.

Uno de los aspectos clave del PINAR es la mejora de la infraestructura, tanto física como tecnológica, la carencia de espacios adecuados y la ausencia de un Sistema de Gestión de Documentos Electrónicos (SGDEA) son desafíos identificados, los proyectos asociados buscan abordar estas limitaciones, se proporciona una base sólida para una gestión documental moderna y alineada con las demandas contemporáneas, donde los documentos electrónicos desempeñan un papel fundamental.

La transparencia y el acceso a la información son consecuencias directas de la implementación del PINAR, un sistema eficiente de gestión documental facilita el acceso a la información pública, fortaleciendo la transparencia gubernamental, esto es un requisito normativo y componente para construir o mantener la confianza de la ciudadanía en la administración pública.

Otro aspecto del PINAR es la convalidación y actualización de instrumentos archivísticos, como las Tablas de Valoración Documental, este proceso asegura la adecuada conservación y eliminación de documentos, porque logra contribuir a la organización eficiente del archivo, evita la acumulación innecesaria y facilita la identificación de información relevante.

Para concluir este apartado, el desarrollo de recursos humanos a través de la elaboración de políticas, manuales y programas de capacitación en gestión documental es básico, un equipo capacitado y comprometido ayuda al éxito del PINAR, ya que la implementación efectiva de estas estrategias requiere la colaboración y comprensión de todos los involucrados en los procesos documentales de la Gobernación.

En conjunto, el PINAR de la Gobernación de Magdalena se toma como un instrumento integral que, a través de una serie de acciones y proyectos asociados, busca modernizar y fortalecer la gestión documental, contribuyendo así a una administración pública más eficiente, transparente y confiable.

4.2.2. Enfoque en el Ciclo PHVA

El Plan Institucional de Archivos (PINAR) de la Gobernación de Magdalena para el periodo 2020-2023 también adopta un enfoque basado en el ciclo PHVA (Planear, Hacer, Verificar y Actuar), o conocido como ciclo de mejora continua. Este enfoque proporciona una metodología sistemática y cíclica que permite la planificación, implementación, evaluación y ajuste constante de las estrategias de gestión documental. A continuación, se argumenta sobre cómo se integra este enfoque en el PINAR:

Planear (Plan):

En la fase de “Planear”, el PINAR establece una visión estratégica y define los objetivos específicos que la Gobernación busca lograr en términos de gestión documental. El plan detalla acciones y proyectos asociados para abordar aspectos críticos identificados, como la falta de procesos definidos, la carencia de un Sistema de Gestión de Documentos Electrónicos (SGDEA) y la necesidad de convalidación de instrumentos archivísticos. Este proceso de planificación es esencial para establecer una dirección clara y alinear los esfuerzos con los objetivos institucionales.

En la fase de "Hacer", se implementan los planes y proyectos detallados en el PINAR. Esto implica llevar a cabo acciones concretas, como la creación de un SGDEA, el diseño e implementación de procesos de gestión documental, y la mejora de la infraestructura física y tecnológica. Esta etapa busca materializar las estrategias delineadas en la fase de planificación, con un énfasis en la ejecución eficiente de las actividades propuestas.

La fase de "Verificar" implica la evaluación y el monitoreo continuo de los resultados obtenidos durante la implementación. Aquí, se introducen herramientas de seguimiento y control, como indicadores clave de rendimiento (KPIs) y mediciones trimestrales, estos permiten evaluar el progreso de los proyectos asociados y su alineación con los objetivos establecidos. La verificación identifica posibles desviaciones y áreas de mejora, garantizando que la implementación se ajuste a las expectativas.

La fase "Actuar" es básica para cerrar el ciclo de mejora continua, basándose en los resultados y evaluaciones obtenidas en la fase de verificación, se toman medidas correctivas y se ajustan las estrategias según sea necesario. Este ciclo constante de planificación, implementación,

evaluación y ajuste asegura que el PINAR se adapte dinámicamente a cambios en el entorno, nuevas regulaciones o descubrimientos internos que puedan impactar la gestión documental.

El enfoque en el ciclo PHVA en el PINAR de la Gobernación de Magdalena refleja un compromiso con la mejora continua y la adaptabilidad. Proporciona un marco robusto para abordar los desafíos identificados y garantiza que la gestión documental evolucione de manera efectiva en respuesta a las dinámicas cambiantes del entorno institucional y normativo. Este enfoque busca resolver problemas actuales, al tiempo que sienta las bases para un proceso continuo de perfeccionamiento y eficiencia en la gestión documental a lo largo del tiempo.

4.2.3. Contexto Gobernación de Magdalena

La Gobernación de Magdalena, ubicada en un contexto regional único, se enfrenta a diversos desafíos y oportunidades en los ámbitos socioeconómico, cultural y ambiental, este contexto regional específico influye directamente en la formulación del Plan Institucional de Archivos (PINAR) para el periodo 2020-2023. El departamento se compromete a impulsar el desarrollo integral, y en este sentido, el PINAR se posiciona como una herramienta estratégica alineada con el Plan de Desarrollo "Magdalena Renace 2020-2023".

La misión y visión institucional de la Gobernación reflejan su compromiso con la gestión eficiente de la información y los documentos, son un elemento valioso en la ejecución de sus diversas áreas de acción gubernamental, en consonancia con el eje estratégico "Revolución del Gobierno Popular", el PINAR busca modernizar y optimizar los procesos internos, al focalizar sus esfuerzos en la gestión documental para mejorar la organización, acceso y conservación de la información gubernamental.

La entidad gubernamental se encuentra sujeta a normativas y directrices nacionales en materia de gestión documental, como la Ley 594 de 2000 y decretos reglamentarios, el PINAR adquiere un papel decisivo al ser concebido como una herramienta para asegurar el cumplimiento normativo, garantizando que los archivos y documentos gubernamentales cumplan con los requisitos establecidos por la legislación nacional.

4.2.4. *Los Riesgos de la Institución*

La evaluación de riesgos en el Plan Institucional de Archivos (PINAR) de la Gobernación de Magdalena desempeña un papel en la identificación, análisis y gestión de posibles amenazas y obstáculos que podrían afectar la implementación exitosa de la estrategia archivística, esta evaluación se realiza con el objetivo de anticipar y/o mitigar los impactos negativos, que garanticen la integridad, disponibilidad y confidencialidad de la información gubernamental.

En el contexto del PINAR, la evaluación de riesgos abarca diversos aspectos, desde los desafíos normativos hasta los obstáculos operativos, uno de los riesgos identificados es la falta de convalidación de los instrumentos archivísticos, lo que podría generar incongruencias con la normativa vigente y afectar la validez legal de los documentos. Además, la carencia de un Sistema de Gestión de Documentos Electrónicos (SGDEA) representa un riesgo potencial en términos de eficiencia operativa y seguridad de la información.

La evaluación de riesgos también considera aspectos relacionados con recursos humanos, tecnológicos y financieros, la insuficiencia de personal capacitado en gestión documental podría ser un riesgo que afecte la implementación efectiva de los procesos propuestos en el PINAR, como la falta de recursos tecnológicos y financieros podría limitar la adopción de soluciones tecnológicas necesarias para la gestión eficiente de documentos electrónicos.

Es necesario que la Gobernación de Magdalena, a través del PINAR, establezca un proceso continuo de evaluación de riesgos, esto implica la revisión periódica de los riesgos identificados, la actualización de la evaluación en función de cambios internos y externos, y la incorporación de medidas preventivas o correctivas. La evaluación de riesgos se concibe como una tarea puntual y un componente dinámico e integral que contribuye a la adaptabilidad o resiliencia del sistema de gestión documental ante un entorno en constante cambio.

4.2.5. Gestión en la Seguridad de la Información

La política de Gestión Documental de la Gobernación de Magdalena establece un compromiso claro con la misión y visión del departamento, centrado en la ejecución de competencias, garantía de condiciones de competitividad y el respeto a la legalidad, instituciones democráticas, derechos humanos y sostenibilidad ambiental, dentro de este marco, la Política de

Gestión Documental se erige como un pilar para la implementación efectiva de la Gestión Documental del departamento.

En sintonía con los principios delineados en el Decreto 2609 de 2012 del Ministerio de Cultura, la Gobernación de Magdalena se compromete a planificar adecuadamente la creación de documentos, al considerar la eficiencia de la Gestión Documental y el cuidado del medio ambiente, este enfoque destaca la necesidad de generar únicamente los documentos necesarios, para gestionar los costos asociados y promover prácticas sostenibles.

La política subraya la necesidad de control y seguimiento de la documentación, con la implementación de acciones correctivas y preventivas cuando sea necesario, lo que garantiza la oportuna consulta de documentos por parte de todas las partes interesadas y se presenta como un principio clave, se destacan la transparencia en la actuación de los funcionarios y su disposición para orientar adecuadamente a los ciudadanos.

Además, se compromete a aplicar los principios, normas y estándares establecidos por el Archivo General de la Nación, que aseguran la coherencia y la calidad en la gestión documental, la promoción de la cultura de la Gestión Documental dentro de la Gobernación de Magdalena se posiciona como un objetivo relevante, al reconocer la importancia y el valor de los archivos como activos estratégicos para la entidad.

Esta política establece un marco sólido para estandarizar y fortalecer los procesos de Gestión Documental en la Gobernación de Magdalena, abarca todas las etapas del ciclo de vida de los documentos y refleja un compromiso integral con la eficiencia, la transparencia y la sostenibilidad.

4.2.6. Roles Específicos

El Plan Institucional de Archivos (PINAR) de la Gobernación de Magdalena establece roles y responsabilidades clave para asegurar la implementación efectiva de las estrategias y acciones delineadas en el documento, estos roles son útiles para garantizar que la gestión documental se lleve a cabo de manera coordinada, eficiente y en cumplimiento con las normativas o políticas establecidas, algunos aspectos sobre los roles y responsabilidades expresados en el PINAR incluyen:

Tabla 2, Roles y Responsabilidades

Roles	Responsabilidades
Comité Institucional de Gestión y Desempeño (CIGD)	Como se menciona en el PINAR, el CIGD tiene la responsabilidad de aprobar las Tablas de Valoración Documental y brindar dirección estratégica para la gestión documental. Su papel es garantizar que las decisiones clave relacionadas con la conservación y disposición de documentos estén alineadas con los objetivos institucionales.
Personal Encargado de Gestión Documental	El PINAR asigna responsabilidades específicas a individuos o equipos encargados de la gestión documenta, estos roles pueden incluir la actualización y aplicación de instrumentos archivísticos, la implementación de procesos de gestión documental, y la supervisión del cumplimiento normativo. La claridad en estas responsabilidades aumenta la eficacia operativa.
Unidades Administrativas Específicas	Por la estructura organizativa, ciertas unidades administrativas tienen roles específicos en la gestión documental. Estos roles pueden incluir la generación y organización de documentos, el mantenimiento de registros, y la colaboración en la implementación de tecnologías documentales, como el Sistema de Gestión de Documentos Electrónicos (SGDEA).
Responsables de Proyectos Asociados	Dado que el PINAR identifica varios proyectos específicos, es crucial definir roles y responsabilidades para aquellos encargados de liderar y ejecutar dichos proyectos. Estos responsables deben garantizar que los proyectos se implementen dentro de plazos establecidos, con los recursos adecuados y según los estándares de calidad definidos.

Nota: La tabla detalla las responsabilidades expresadas en el PINAR de la Gobernación del Magdalena 2020- 2023, autoría propia.

La claridad en los roles y responsabilidades facilita la ejecución efectiva de la estrategia, al promover la rendición de cuentas y la colaboración entre diferentes partes interesadas, porque asegura que todos los aspectos de la gestión documental estén debidamente atendidos, desde la creación y clasificación hasta la disposición final de los documentos.

4.2.7. Controles Operativos

Dentro del Plan Institucional de Archivos (PINAR) de la Gobernación de Magdalena, se aborda de manera integral el control operativo como parte fundamental de la gestión documental, el PINAR establece directrices y estrategias específicas para asegurar un control efectivo en las operaciones relacionadas con la creación, manejo, custodia y disposición de documentos a lo largo de su ciclo de vida, en el contexto del control operativo, el PINAR se enfoca en varios aspectos clave:

Tabla 3, Control Operativo

Control	Alcance
Diseño e Implementación de Procesos	• Identifica la falta de diseño e implementación de los procesos establecidos en el Programa de Gestión Documental (PGD). • Propone proyectos específicos para diseñar e implementar estos procesos, lo que contribuirá directamente al control operativo al establecer procedimientos claros y eficientes.
Evaluación de Riesgos y Aspectos Críticos	• Reconoce la importancia de evaluar los riesgos normativos y los aspectos críticos en la gestión documental. • Propone la implementación de proyectos asociados para abordar estos riesgos, destacando la necesidad de convalidación y registro ante el Archivo General de la Nación (AGN).
Instrumentos Archivísticos y Reglamento de Archivo	• Identifica la carencia de instrumentos archivísticos, como el Modelo de requisitos para la gestión de documentos electrónicos, mapas de procesos y flujos documentales, así como la falta de un Reglamento de Archivo aprobado y aplicado.

	• Propone proyectos específicos para diseñar, elaborar e implementar estos instrumentos y reglamentos, lo que proporcionará directrices y normativas esenciales para el control operativo.
Seguimiento y Control	• Reconoce la importancia de contar con herramientas efectivas de seguimiento y control mediante indicadores clave de rendimiento (KPIs). • Propone la implementación de un sistema de seguimiento y control con mediciones trimestrales y tableros de control para evaluar el progreso de los proyectos asociados y la eficacia de las acciones implementadas.

Nota: La tabla muestra los aspectos clave en el control operativo del desempeño del PINAR de la Gobernación del Magdalena 2020- 2023, autoría propia.

El PINAR de la Gobernación de Magdalena aborda de manera integral el control operativo como parte esencial de la gestión documental, los proyectos propuestos buscan establecer procesos y normativas, para centrarse en evaluar o abordar los riesgos, promoviendo una cultura organizacional que prioriza la eficiencia y la mejora continua en todas las operaciones relacionadas con la documentación.

4.2.8. Control Interno

La Auditoría Interna y la Revisión por la Dirección son componentes básicos dentro del marco del Plan Institucional de Archivos (PINAR) de la Gobernación de Magdalena, ambos procesos se diseñan con el objetivo de evaluar y mejorar continuamente el desempeño de la gestión documental en la entidad.

Sobre la auditoría interna, en el contexto del PINAR se centra en realizar evaluaciones sistemáticas e independientes de los procesos, procedimientos y controles relacionados con la gestión documental de la institución. A través de la Auditoría Interna, se verifica el cumplimiento de los procedimientos establecidos en el PINAR, identificando posibles desviaciones, riesgos y

áreas de mejora, este proceso proporciona una evaluación objetiva de la eficacia de la implementación de los proyectos y acciones propuestas en el PINAR, y permite ajustes o correcciones según sea necesario.

Sobre la revisión de la dirección, esta implica la evaluación a un nivel más estratégico, donde los líderes y responsables del PINAR revisan y analizan el desempeño general del plan, durante esta revisión, se analizan los resultados obtenidos a través de indicadores clave de rendimiento (KPIs) y se evalúa el impacto de las acciones implementadas en la gestión documental.

La Revisión por la Dirección también proporciona una oportunidad para alinear el PINAR con los objetivos institucionales más amplios y realizar ajustes estratégicos si es necesario, el conjunto de la Auditoría Interna y la Revisión por la Dirección establece un proceso cíclico de mejora continua basado en el modelo PHVA (Planificar, Hacer, Verificar, Actuar)., este enfoque asegura que la gestión documental se adapte a las necesidades cambiantes de la entidad y cumpla con las normativas y estándares establecidos.

Además, estos procesos contribuyen a la transparencia y la rendición de cuentas al proporcionar una evaluación objetiva del desempeño del PINAR, permiten que la alta dirección tome decisiones informadas para fortalecer la eficacia de la gestión documental y su alineación con los objetivos estratégicos de la Gobernación de Magdalena.

4.2.9. Revisión y Actualización

En el marco del Plan Institucional de Archivos (PINAR) de la Gobernación de Magdalena, se aborda de manera integral el concepto de mejora continua como un pilar para el perfeccionamiento constante de los procesos de gestión documental, el enfoque adoptado sigue el modelo PHVA (Planificar, Hacer, Verificar, Actuar), que estructura la metodología de trabajo a lo largo del ciclo de vida de los documentos.

La implementación de auditorías internas y revisiones periódicas constituye un componente para evaluar la eficacia de los procesos establecidos en el PINAR, estas evaluaciones regulares identifican áreas de oportunidad, al igual que garantizan la conformidad con los estándares y normativas establecidos, contribuyendo así a la excelencia en la gestión documental.

Un aspecto para la mejora continua radica en la definición y seguimiento de Indicadores Clave de Rendimiento (KPIs), estos proporcionan métricas cuantificables que permiten evaluar el desempeño de la gestión documental, facilitando la toma de decisiones informadas y la identificación de áreas específicas que requieren mejoras.

La retroalimentación directa de los usuarios y la participación activa en la identificación de áreas de mejora son elementos en el proceso, la voz de los usuarios, expresada a través de encuestas y comentarios, proporciona una perspectiva valiosa que se incorpora en la revisión de procesos y en la implementación de mejoras concretas.

En complemento, la evaluación continua de riesgos en la gestión documental es una práctica anticipativa que permite identificar posibles desafíos y establecer medidas preventivas y correctivas. Esta visión proactiva contribuye a mantener la seguridad y confidencialidad de la información en todo momento.

Además, la capacitación y desarrollo continuo del personal en las últimas prácticas y tecnologías relacionadas con la gestión documental se considera un elemento clave para asegurar la adaptabilidad y la mejora constante en la ejecución de los procesos, la actualización regular de normativas y tecnologías garantiza que el PINAR esté siempre alineado con los requisitos más recientes y las mejores prácticas en la materia.

En concordancia, la revisión estratégica por parte de la dirección brinda una perspectiva global sobre el impacto del PINAR en la consecución de los objetivos institucionales, este nivel de revisión permite ajustes y mejoras a nivel estratégico, asegura que la mejora continua sea un proceso reactivo, y un principio que impulse la innovación con eficiencia en la gestión documental de la Gobernación de Magdalena.

4.3. Comparación

4.3.1. Tabla de Comparación

La tabla de comparación propuesta tiene como objetivo detallar y analizar de manera sistemática las similitudes y diferencias entre el Plan Institucional de Archivos (PINAR) de la Gobernación del Magdalena y los requisitos establecidos por la Norma ISO 27001 en materia de

seguridad de la información, esta herramienta proporciona una visión integral de la gestión documental y de seguridad en el Archivo Central, permitiendo identificar áreas de convergencia y posibles brechas.

La tabla se estructurará de manera organizada, abordando aspectos clave relacionados con el alcance y aplicabilidad, controles operativos y de seguridad, y otros elementos relevantes. A través de esta comparación detallada, se busca evaluar el grado de alineación entre las prácticas internas de la institución y los estándares internacionales en seguridad de la información, esta información sirve para informar la propuesta de implementación de la Norma ISO 27001 en el Archivo Central de la Gobernación del Magdalena, al proporcionar una base objetiva y fundamentada para el análisis o la toma de decisiones.

Aspectos de Comparación	**PINAR Gobernación del Magdalena (2020-2023)**	**Software INFODOC**	**Norma ISO 27001**
Objetivo Principal	Establecer un marco para la gestión de la seguridad de la información en archivos.	Administrar la información a través de la implementación de un sistema específico (INFODOC).	Establecer un marco sistemático para la gestión de la seguridad de la información en una organización.
Enfoque PDCA	Sigue el ciclo PDCA para implementar y mantener el SGSI específicamente en el ámbito archivístico.	INFODOC implementa funcionalidades que permiten el registro, radicación, seguimiento y control de la gestión documental, indicando un enfoque PDCA para sus procesos.	También sigue el ciclo PDCA, pero para la gestión de la seguridad de la información en general.
Contexto Organizacional	Considera factores internos y externos para alinear el SGSI con	INFODOC se implementa para eficiencia de procesos	Alínea la gestión de la seguridad de la información con la

	objetivos estratégicos en gestión documental.	y gestión documental, alineándose con la misión y visión del Departamento.	dirección estratégica de la organización.
Evaluación de Riesgos	Identifica y evalúa riesgos de seguridad de la información específicos para archivos.	No se proporciona información específica sobre la evaluación de riesgos en INFODOC, pero su implementación indica una consideración de la seguridad de la información.	Requiere una evaluación de riesgos para identificar amenazas, vulnerabilidades y evaluar impactos.
Política de Seguridad de la Información	Establece una política de seguridad de la información documentada.	No se proporciona información específica sobre políticas en INFODOC, pero su implementación indica un compromiso con la gestión documental.	Requiere una política de seguridad de la información que refleje el compromiso de la alta dirección.
Roles y Responsabilidades	Asigna roles y responsabilidades claros para la seguridad de la información en el ámbito archivístico.	No se proporciona información específica sobre roles y responsabilidades en INFODOC, pero su implementación implica asignación de funciones para el uso adecuado del software.	Requiere la designación de un responsable de seguridad de la información y participación activa de la alta dirección.
Planificación y Control Operativo	Establece controles operativos para gestionar la seguridad de	INFODOC implementa módulos que abarcan desde la planificación de	Requiere la implementación de controles operativos para garantizar la

	la información en archivos.	necesidades hasta el control operativo de procesos de gestión documental.	seguridad de la información.
Auditorías Internas y Revisión por la Dirección	Realiza auditorías internas y revisión por la dirección centradas en gestión documental.	No se proporciona información específica sobre auditorías internas y revisiones en INFODOC, pero su incorporación de un módulo de auditoría indica una posibilidad de seguimiento y evaluación.	Requiere auditorías internas y revisión por la dirección para evaluar la eficacia del SGSI.
Mejora Continua	Enfatiza la importancia de la mejora continua en el ámbito de la gestión documental.	INFODOC incluye módulos de reportes, expedientes virtuales y gestión y trámite, indicando una orientación hacia la mejora continua en la gestión documental.	Pone un fuerte énfasis en la mejora continua del SGSI.

4.3.2. Observaciones Adicionales

Las observaciones adicionales sobre INFODOC revelan valiosas consideraciones que afectan la implementación de controles operativos y de seguridad, así como la revisión continua del Plan Institucional de Archivos (PINAR), estas observaciones son útiles para comprender las limitaciones y áreas de mejora en la gestión de la seguridad de la información en el Archivo Central de la Gobernación del Magdalena.

En primer lugar, la observación relacionada con el alcance y aplicabilidad señala una brecha potencial en la cobertura de los requisitos generales de seguridad de la información establecidos por la ISO 27001, dado que el PINAR se centra específicamente en la gestión de

archivos, podría no abordar completamente aspectos críticos de seguridad de la información que son esenciales para cualquier tipo de organización, esta limitación podría comprometer la integridad, confidencialidad y disponibilidad de la información si no se consideran los requisitos más amplios de la ISO 27001.

En segundo lugar, la identificación de áreas donde el PINAR puede carecer de controles operativos y de seguridad específicos requeridos por la ISO 27001 destaca la necesidad de una evaluación detallada de los procedimientos actuales, garantizar la integridad, confidencialidad y disponibilidad de la información es valioso, y cualquier omisión en los controles puede representar un riesgo significativo, esta observación destaca la importancia de revisar y fortalecer los controles operativos en áreas específicas para cumplir con los estándares internacionales.

Para finalizar este apartado, la recomendación de revisar y actualizar periódicamente el PINAR es clave para asegurar su alineación con estándares internacionales y adaptarse a cambios en los requisitos normativos y organizativos, la sugerencia de prestar mayor atención a la preservación de la información como parte de la mejora continua resalta la importancia de no solo cumplir con los requisitos actuales, sino también de anticipar y adaptarse a las necesidades futuras de preservación de información, lo cual fortalece la sostenibilidad y la efectividad a largo plazo del sistema de gestión de la seguridad de la información.

5. Capítulo, Propuesta para la Implementación de la Norma ISO 27001 en el Archivo Central de la Gobernación del Departamento del Magdalena

Introducción

El archivo central de la gobernación del Magdalena abarca la producción documental transferida a lo largo de la historia de dicha institución. Por consiguiente, surge la necesidad de cumplir con las recomendaciones del estándar ISO 27001 de tal modo que se garantice la disponibilidad, integridad y confidencialidad de los documentos. Lo cual se estructura en la siguiente propuesta en la cual se presenta la implantación establecida por fases según el ciclo PHVA.

Es así como, sin dejar a un lado la normatividad archivística vigente y los lineamientos de gestión documental descritos en el PGD. De acuerdo con lo anterior, los sistemas de seguridad para la gestión documental deben contemplar: el análisis de riesgos, los controles de madurez según el nivel de cumplimiento y la aplicabilidad de cada instrumento archivístico de tal forma que estén documentados en procedimientos e implementación técnica.

Posibles Fases de Implementación

Para garantizar una implementación efectiva del estándar ISO 27001 en el Archivo Central de la Gobernación del Departamento del Magdalena, se propone seguir un enfoque basado en fases, estructurado según el ciclo PHVA (Planificar, Hacer, Verificar, Actuar), a continuación, se describe cada fase tentativa para una posible implementación:

Fase 1, Planificación

Objetivo, Establecer las bases para la implementación de ISO 27001, seguido se detallan posibles actividades:

1. **Revisión inicial y análisis de brechas**

- Realizar un diagnóstico inicial del estado actual de la seguridad de la información en el archivo central.
- Identificar brechas entre las prácticas actuales y los requisitos de ISO 27001.

2. **Definición del alcance del SGSI**

- Determinar las áreas y procesos que estarán cubiertos por el Sistema de Gestión de Seguridad de la Información (SGSI).

3. **Desarrollo de la política de seguridad de la información**

- Crear una política de seguridad alineada con ISO 27001, adaptada a las necesidades del archivo central.

4. **Identificación de riesgos y evaluación de impactos**

- Identificar amenazas y vulnerabilidades.
- Evaluar los impactos potenciales de estos riesgos en la información documental.

5. **Plan de gestión de riesgos**

- Establecer medidas para mitigar los riesgos identificados.
- Desarrollar planes de contingencia para riesgos residuales.

Fase 2, Implementación

Objetivo, poner en práctica las políticas, procedimientos y controles definidos en la fase de planificación, seguido se detallan posibles actividades:

1. **Desarrollo de procedimientos y controles**

- Documentar procedimientos operativos para la seguridad de la información.
- Implementar controles técnicos y administrativos.

2. **Capacitación y concienciación**

- Capacitar al personal del archivo central en políticas y procedimientos de seguridad de la información.
- Crear campañas de concienciación sobre la importancia de la seguridad de la información.

3. **Configuración y adaptación del sistema INFODOC**

- Integrar controles de seguridad en el sistema INFODOC.
- Asegurar que el sistema INFODOC cumpla con los requisitos de ISO 27001.

4. **Gestión de documentos y registros**

- Asegurar que todos los documentos y registros relacionados con el SGSI estén bien gestionados y disponibles.

Fase 3, Verificación

Objetivo, evaluar la efectividad de la implementación del SGSI y asegurar el cumplimiento continuo, a continuación, se detallan las posibles actividades

1. **Auditorías internas**

- Realizar auditorías internas periódicas para evaluar la conformidad con ISO 27001.
- Identificar áreas de mejora y no conformidades.

2. **Revisión por la dirección**

- Realizar revisiones periódicas del SGSI por parte de la alta dirección.
- Evaluar la efectividad y adecuación del SGSI.

3. **Monitoreo y medición**

- Implementar sistemas de monitoreo continuo para evaluar la efectividad de los controles de seguridad.
- Medir el desempeño del SGSI contra los objetivos establecidos.

Fase 4, Actuar

Objetivo, mejorar continuamente el SGSI basándose en los resultados de la fase de verificación, a continuación, se detallan sus posibles actividades:

1. **Acciones correctivas y preventivas**
    - Implementar acciones correctivas para abordar no conformidades y áreas de mejora identificadas.
    - Desarrollar acciones preventivas para evitar la ocurrencia de futuros problemas.
2. **Actualización de políticas y procedimientos**

- Revisar y actualizar las políticas y procedimientos de seguridad de la información según sea necesario.

3. **Mejora continua**

- Fomentar una cultura de mejora continua en la seguridad de la información.
- Promover la innovación y la adaptación a nuevos riesgos y tecnologías.

Fase de Evaluación Final

Objetivo, asegurar que el SGSI está completamente integrado y funcionando de manera efectiva, a continuación, se detallan sus posibles actividades:

1. **Evaluación integral del SGSI**

- Realizar una evaluación integral del SGSI para asegurar su efectividad.
- Documentar los logros y áreas de mejora.

2. **Certificación ISO 27001**

- Prepararse para la auditoría externa de certificación.
- Obtener la certificación ISO 27001 para el Archivo Central de la Gobernación del Magdalena.

Cronograma de Implementación

a) Primer Trimestre

- Realización de diagnósticos y análisis de brechas.
- Definición del alcance del SGSI y desarrollo de la política de seguridad.
- Identificación de riesgos y evaluación de impactos.

b) Segundo Trimestre

- Desarrollo e implementación de procedimientos y controles.
- Capacitación y concienciación del personal.
- Configuración del sistema INFODOC.

c) Tercer Trimestre

- Realización de auditorías internas.
- Revisión por la dirección.
- Monitoreo y medición continua.

d) Cuarto Trimestre

- Implementación de acciones correctivas y preventivas.
- Revisión y actualización de políticas y procedimientos.
- Preparación para la certificación ISO 27001.

Esta estructura secuencial y organizada permitirá una implementación efectiva y sostenible del estándar ISO 27001, asegurando la seguridad de la información en el Archivo Central de la Gobernación del Departamento del Magdalena.

Objetivo Propuesta

Garantizar la seguridad de la información que reposa en el archivo central de la gobernación del departamento del Magdalena a través de la implementación del estándar ISO 27001.

Alcance de Propuesta

La propuesta abarca las fases de implementación según el estándar ISO 27001 para el archivo central de la gobernación del Magdalena e incluye las capacitaciones necesarias en seguridad de la información de tal modo que los funcionarios de dicha unidad de información desde el ejercicio de sus funciones sean conscientes de la importancia que tienen los sistemas de seguridad de la información.

Referentes normativos

Al tener control sobre la información (SI) se aplican una serie de normas relacionadas con la gestión documental, razón por la cual a continuación se presentan las normas que están relacionadas con la seguridad de la información:

Tabla 4, Normas para la seguridad de la información.

Tipo de Norma	Número	Objeto	Relación con la SI
Ley	594/2000	Ley general de archivos	Menciona la seguridad de la información como un requisito para la conservación de los soportes documentales.
Decreto	2609/2012	Reglamenta el titulo V de la ley general de archivos	Brinda los lineamientos requeridos para los

			sistemas de gestión documental y su seguridad.
Ley	1712/2014	Ley de transparencia y acceso a la información.	Considera la seguridad como un elemento clave en la transparencia
Acuerdo	04 de 2019	Procedimiento de TRD y TVD	Establece la forma en que se dispone de los documentos.
Ley	1437/2011	Expide el código de procedimiento Administrativo	Considera la seguridad como un elemento clave en la transparencia de los procesos administrativos.

Nota: La tabla muestra las normas y acuerdos necesarios en el marco de la seguridad de la información, autoría propia.

Contexto Entidad

La Gobernación del Magdalena es una entidad del orden departamental que pertenece a la rama ejecutiva y fue creada mediante la ley 25 de 1967. En la actualidad cuenta con 46 dependencias las cuales han transferido al único deposito que posee el archivo central con un aproximado de 20.000 cajas entre referencias X-300 y X-200.

Metodología

La implementación de la norma ISO requiere de fases en las cuales se deben tener requisitos previos entre los cuales está: contar con el apoyo de la gerencia, aplicar la gestión por proyectos, aplicar el alcance del sistema de gestión de seguridad de la información (SGSI) de tal modo que se incluya una política de SI y evaluar los riesgos para así ofrecer un plan de contingencia para cada riesgo a través de las auditorías internas.

Fases del Sistema de Gestión de Seguridad de la Información

Fase de planificación: En esta fase se definen los objetivos con los cuales se tienen los controles requeridos para la seguridad de la información desde los siguientes elementos:

Confidencialidad: Establecer controles de confidencialidad de acuerdo con los tipos de información que contiene el archivo central de la gobernación del Magdalena.

Tabla 5, Tipología de la información

Tipos de información	**Aspectos para revisar**		
	Series documentales según dependencia de origen	**Firmas**	**Aspectos legales**
Pública	La información pública aplica para algunas series a la que todos pueden tener acceso.	Las firmas se deben realizar por los directores de dependencias o que se encuentren en modo de encargo por medio de acto administrativo.	Deben contemplar lo mencionado en los artículos 6 y 8 de la ley 1712 de 2014
Clasificada	La información clasificada aplica para algunas series a la que se pueden tener acceso mediante una solicitud de información.	Las firmas se deben realizar por los directores de dependencias o que se encuentren en modo de encargo por medio de acto administrativo.	Deben contemplar lo mencionado en artículo 18 de la ley 1212 de 2014

Reservada	La información reservada está contenida en aquellas series documentales que tienen información a la que solo los implicados pueden acceder o mediante orden judicial	Las firmas se deben realizar por los directores de dependencias o que se encuentren en modo de encargo por medio de acto administrativo y los implicados en cada documento.	Deben contemplar lo mencionado en artículo 19 de la ley 1212 de 2014

Nota: Tabla de tipologías de la información y sus distintas medidas de seguridad contempladas, autoría propia.

Integridad: Garantizar que la información esté completa y sin alteraciones por terceros no autorizados.

Tabla 6, Control y evaluación de la información

Tipos de información	**Aspectos para revisar**		
	Firmas	**Control de versiones**	**Políticas de acceso y cambios**
Pública	Las firmas no deben estar alteradas y completas de lo contrario no tendrá validez	El control de las versiones debe estar a cargo por cada dependencia productora de documentos	Revisar que no se realicen cambios por personal no autorizado
Clasificada			
Reservada			

Nota: Elementos de revisión de la información producida, autoría propia.

Disponibilidad del sistema: Garantizar que los tipos de información se encuentren disponibles en el sistema según los estipulado en las tablas de control y acceso (TCA).

Tabla 7, Campos para las TCA

Serie	Subserie	Tipo de acceso	Normatividad aplicable
Nombre de la serie documental	Nombre de la subserie documental	De acuerdo con los tipos de información que estén dentro de cada serie o subserie: • Clasificada. • Publica • Reservada	Normatividad que aplica según el tipo de información.

Nota: Elementos de los campos de las TCA, autoría propia.

Plan de Implementación

A continuación, se presenta la estructura de cómo se propone implementar la norma ISO 27001, cabe resaltar que contempla el sistema INFODOC, al tiempo que integra la infraestructura física y el formato papel como complemento a la propuesta.

Tabla 8, Estrategias de implementación ISO 27001 en INFODOC

Componentes	Norma ISO 27001	Implementación	Estrategias
Contexto Organizacional	Alínea la gestión de la seguridad de la información con la dirección estratégica de la organización.	Generar estrategias que permitan el adecuado funcionamiento del archivo central desde la gestión pública de la Gobernación del Magdalena.	Comprender el contexto de la organización. Tener en cuenta las necesidades de la organización.
Evaluación de Riesgos	Requiere una evaluación de riesgos para identificar amenazas, vulnerabilidades y evaluar impactos.	Realizar un diagnóstico integral de archivos y analizar los resultados desde la seguridad de la información.	Contemplar los riesgos encontrados en el diagnóstico integral de archivos.
Política de Seguridad de la Información	Requiere una política de seguridad de la información	Consignar las estrategias de seguridad basadas en el	Analizar si las políticas de seguridad actuales contemplan todos los aspectos requeridos.

	que refleje el compromiso de la alta dirección.	diagnostico integral de archivos.	Indagar sobre los terceros que poseen documentación en custodia.
Roles y Responsabilidades	Requiere la designación de un responsable de seguridad de la información y participación de la alta dirección.	Dividir las responsabilidades entre los encargados de custodiar el archivo central no solo desde la parte física sino también en el sistema INFODOC.	Generar políticas de uso para las herramientas tecnológicas que dispone el archivo central y asignar un responsable encargado del sistema.
Planificación y Control Operativo	Requiere la implementación de controles operativos para garantizar la seguridad de la información.	Garantizar el acceso y tratamiento de la información a personal autorizado, además de tener actualizados los inventarios documentales.	Crear capacitaciones sobre la importancia de la seguridad de la información de tal modo que se genere conciencia en todos los colaboradores del archivo central. Ejecutar controles y revisiones al momento de recibir una transferencia documental. Aplicar la correcta disposición final según las tablas de retención documental y de valoración.

			Revisión de las instalaciones según la normatividad vigente para depósitos de archivo.
Auditorías Internas y Revisión por la Dirección	Requiere auditorías internas y revisión por la dirección para evaluar la eficacia del SGSI.	Generar un cronograma de auditorías internas de manera periódica para revisar el estado de la implementación del SGSI.	Revisión del correcto diligenciamiento de los formatos de entrada y salida de personal. Controlar los activos de información. Realizar auditoria al funcionamiento del SGDA. Limitar permisos en el acceso a la información. Cifrar información confidencial.

Nota: Elementos de implementación ISO 27001 en INFODOC, autoría propia.

Plan de Evaluación

Revisar la aplicación del sistema de tal modo que se evalúen posibles fallas para lo cual se propone el siguiente instrumento, el cual compila

Tabla 9, Componentes y medición de cumplimiento

Componentes	**Escala de cumplimiento (1 mínimo - 100 máximo)**
Autenticación	50 %
Autorización	50 %
Cifrado	50 %
Firewalls	50 %
Detección de intrusiones	50 %
Gestión de vulnerabilidades	50 %
Control de acceso	50 %
Seguridad física	80 %

Nota: Componentes de evaluación del sistema, autoría propia.

Mejora continua: Realizar los cambios detectados en la fase de evaluación a cada una de las áreas competentes en el archivo central de la gobernación del Magdalena.

Tabla 10, Componentes detectados en evaluación

Aspectos susceptibles de mejora	**Componentes**	**Responsable**
Actualización de políticas y procedimientos	Revisar y actualizar las políticas planteadas en	Área administrativa

	la seguridad de la información. Facilitar el acceso y entendimiento de las políticas	
Auditorias de seguridad regulares	Generar oportunidades de mejora a partir de los hallazgos.	Área administrativa y Área técnica
Gestión de vulnerabilidades	Generar un macroproceso que permita subsanar las vulnerabilidades	Área técnica
Monitorización continua y detección de amenazas	Detectar amenazas no solo en las instalaciones sino en los sistemas.	Área de recursos físicos
Evaluación de riesgos y mejora del análisis del impacto en el negocio	Analizar el impacto que tienen los incidentes de seguridad.	Área administrativa
Revisión de mejora de controles, acceso y privacidad	Gestionar la privacidad de los datos a través de políticas que favorezcan la seguridad de estos.	Área administrativa y Área técnica

Nota: Cambios de la mejora continua, autoría propia.

Conclusiones

La investigación sobre la implementación de la Norma ISO 27001 en el Archivo Central de la Gobernación del Magdalena se ha centrado en tres objetivos específicos fundamentales; diagnosticar las debilidades y falencias del acceso a la información administrada por el software INFODOC, identificar las prácticas actuales de gestión de seguridad de la información en comparación con los requisitos de la Norma ISO 27001, y estructurar los elementos necesarios para una propuesta efectiva de implementación, se presentan las conclusiones derivadas de cada uno de estos objetivos.

Del diagnóstico de debilidades y falencias del acceso a la información administrada por INFODOC, este diagnóstico reveló varias áreas críticas que necesitan atención para mejorar la seguridad y la eficiencia del sistema de gestión documental; Accesos No Autorizados, uno de los problemas identificados fue la falta de controles robustos para gestionar los accesos al sistema INFODOC, se encontraron múltiples casos en los que el acceso a información sensible no estaba restringido adecuadamente, lo que aumenta el riesgo de exposición no autorizada, esta debilidad se relaciona directamente con la necesidad de establecer mecanismos de autenticación y autorización más estrictos.

Deficiencias en la Configuración del Software, el análisis también puso de manifiesto deficiencias en la configuración del software INFODOC, se identificaron configuraciones inapropiadas que permitían a usuarios no autorizados realizar cambios en los documentos o acceder a áreas restringidas del sistema, la falta de personalización en los permisos de usuario y la insuficiente segmentación de la información expusieron al sistema a riesgos de integridad y confidencialidad.

Carencia de Auditorías Internas, la ausencia de auditorías internas periódicas para monitorear y revisar los accesos y cambios en el sistema INFODOC es otra debilidad crítica, sin auditorías regulares, es difícil detectar actividades sospechosas o errores en la gestión de acceso, este aspecto subraya la necesidad de implementar un plan de auditorías internas que permita una revisión continua de los controles de acceso y de la gestión de la información.

Capacitación Insuficiente del Personal, la falta de capacitación adecuada del personal en el uso de INFODOC y en prácticas de seguridad de la información también emergió como una debilidad importante, muchos usuarios no están completamente informados sobre las mejores prácticas de seguridad y sobre cómo utilizar el software de manera segura, esto resalta la necesidad de desarrollar programas de formación específicos para asegurar que el personal entienda y siga los procedimientos de seguridad establecidos.

Sobre la *identificación y comparación de prácticas actuales con los requisitos de ISO 27001*, esta comparación permitió identificar varias discrepancias y áreas de mejora en la implementación de medidas de seguridad; Políticas y Procedimientos de Seguridad Inadecuados, se observó que las políticas y procedimientos actuales de seguridad de la información en el Archivo Central no están completamente alineados con los requisitos de la Norma ISO 27001. Aunque existen políticas básicas, carecen de detalle y especificidad en áreas clave como la gestión de incidentes, la clasificación de la información y el control de accesos, la norma ISO 27001 exige una documentación más rigurosa y exhaustiva para cubrir todos los aspectos de la seguridad de la información.

Evaluación de Riesgos No Sistemática, el proceso de evaluación de riesgos actual en el Archivo Central no sigue un enfoque sistemático ni estructurado, la Norma ISO 27001 requiere una evaluación de riesgos detallada y periódica para identificar amenazas y vulnerabilidades, y para establecer controles adecuados, el enfoque actual es ad hoc y no proporciona una visión integral de los riesgos potenciales, lo que limita la capacidad para implementar controles efectivos.

Falta de Formación Continua, la comparación también reveló una falta de formación continua y actualizada en seguridad de la información, según la Norma ISO 27001, la capacitación debe ser regular y adaptada a los cambios en las amenazas y en las políticas de seguridad, en el Archivo Central, la formación en seguridad de la información es esporádica y no siempre está alineada con las mejores prácticas internacionales.

Deficiencias en la Gestión de Controles de Acceso, la gestión de controles de acceso en el Archivo Central no cumple con los estándares de la Norma ISO 27001, se identificaron brechas en la implementación de controles de acceso y en la administración de permisos, la norma requiere

controles más estrictos y un sistema de gestión de acceso más detallado para garantizar que solo las personas autorizadas puedan acceder a la información sensible.

De la *Estructuración de la Propuesta para la Implementación de ISO 27001*, a partir de los diagnósticos y comparaciones realizadas, se ha desarrollado una propuesta integral que abarca los siguientes elementos clave:

Definición de Objetivos y Políticas, la propuesta incluye la definición clara de objetivos de seguridad de la información alineados con los requisitos de la Norma ISO 27001, se elaborarán políticas y procedimientos detallados que aborden aspectos como la clasificación de la información, el control de accesos, la gestión de incidentes y la evaluación de riesgos. Estas políticas serán fundamentales para establecer un marco sólido para la seguridad de la información en el Archivo Central.

Asignación de Responsabilidades, se ha diseñado una estructura organizativa para la gestión de la seguridad de la información que incluye la asignación de responsabilidades específicas, se designará un responsable de seguridad de la información y se definirá un equipo encargado de implementar y supervisar las políticas de seguridad. Esta estructura garantizará que haya una clara rendición de cuentas y que se mantenga la eficacia del sistema de gestión de seguridad de la información.

Desarrollo de un Sistema de Gestión de Seguridad de la Información (SGSI), la propuesta incluye la creación de un SGSI que sirva como marco de referencia para la implementación de la Norma ISO 27001, el SGSI permitirá gestionar los controles de seguridad, realizar evaluaciones de riesgos, y supervisar la eficacia de las medidas implementadas, este sistema será esencial para mantener la conformidad con la norma y para gestionar de manera efectiva la seguridad de la información.

Programa de Capacitación y Concienciación, se ha desarrollado un programa de capacitación integral para el personal del Archivo Central, este programa abordará desde conceptos básicos hasta aspectos técnicos de la Norma ISO 27001, asegurando que todos los empleados comprendan la importancia de la seguridad de la información y estén capacitados para seguir los procedimientos establecidos.

Implementación de Controles de Seguridad, la propuesta incluye la implementación de controles de seguridad específicos basados en la evaluación de riesgos, se establecerán medidas para proteger la confidencialidad, integridad y disponibilidad de la información, se desarrollarán planes de contingencia para manejar incidentes de seguridad y se implementarán auditorías internas para revisar la efectividad de los controles.

Evaluación y Mejora Continua, para finalizar la propuesta contempla la implementación de un proceso de evaluación y mejora continua, se establecerán mecanismos para realizar auditorías internas periódicas, revisar los controles de seguridad y actualizar las políticas y procedimientos en función de los resultados obtenidos y de los cambios en el entorno de seguridad.

En conclusión, la investigación ha demostrado que la implementación de la Norma ISO 27001 en el Archivo Central de la Gobernación del Magdalena es esencial para mejorar la seguridad de la información y para garantizar la integridad, confidencialidad y disponibilidad de los documentos, a través del diagnóstico de debilidades, la comparación con los requisitos de la norma y la estructuración de una propuesta detallada, se han establecido las bases para desarrollar un sistema de gestión de seguridad de la información sólido y eficaz. Este sistema permitirá al Archivo Central enfrentar los desafíos actuales y futuros en materia de seguridad de la información, asegurando que se mantenga alineado con las mejores prácticas y estándares internacionales.

Recomendaciones

La implementación de la Norma ISO 27001 en entidades gubernamentales, como el Archivo Central de la Gobernación del Departamento del Magdalena, es útil para garantizar la seguridad de la información y proteger los datos sensibles de los ciudadanos, a lo largo de esta investigación, se ha establecido un marco sólido para evaluar las prácticas de gestión de seguridad de la información, integrando tanto estándares internacionales como políticas internas específicas. A continuación, se presentan recomendaciones ampliadas basadas en los hallazgos de la investigación, con un enfoque en la implementación efectiva y la optimización continua del Sistema de Gestión de Seguridad de la Información (SGSI).

De la *Integración Estratégica de Normas y Políticas Internas*, la estrategia de implementación y sinergia entre normas, la combinación de la Norma ISO 27001 con el Plan Institucional de Archivos (PINAR) ofrece una perspectiva integral que abarca tanto estándares internacionales como políticas internas, esta integración asegura que el SGSI cumpla con requisitos globales, al tiempo que también se alinee con las necesidades y directrices locales del archivo. Es necesario desarrollar un marco de trabajo que unifique estos elementos, facilitando la implementación y asegurando que las políticas y procedimientos sean coherentes o complementarios, la integración debe incluir la revisión periódica de ambos documentos para asegurar que sigan siendo relevantes y efectivos.

Sobre la *Actualización Continua y Adaptación*, los documentos de políticas y procedimientos deben ser actualizados regularmente para reflejar cambios en la normativa, en la tecnología y en el entorno organizacional, implementar un proceso de revisión periódica para ajustar el PINAR y las políticas de seguridad de la información en función de los resultados de auditorías internas y cambios en la ISO 27001 garantiza la relevancia y efectividad continuas del SGSI.

De la *Aplicación del Ciclo PHVA en la Implementación y Mantenimiento del SGSI*, sobre la Planificación Detallada, durante la fase de planificación, se debe desarrollar un plan detallado que defina claramente los objetivos de seguridad, el alcance del SGSI, y los recursos necesarios para su implementación, este plan debe incluir un cronograma, un presupuesto estimado y una estrategia de comunicación para asegurar el compromiso de todas las partes interesadas.

Sobre la *Implementación Efectiva*, la fase de implementación debe ser cuidadosamente gestionada para garantizar que todas las políticas y procedimientos sean seguidos y que los controles de seguridad se apliquen de manera efectiva, la capacitación del personal es básica en esta etapa para asegurar que todos los empleados comprendan sus responsabilidades y las mejores prácticas en seguridad de la información.

Sobre la *Verificación y Auditoría*, la fase de verificación implica realizar auditorías internas y revisiones periódicas para evaluar la eficacia del SGSI, estas auditorías deben ser realizadas por personal calificado y deben evaluar todos los aspectos del sistema, incluyendo la gestión de riesgos, el cumplimiento de políticas, y la eficacia de los controles de seguridad.

Sobre la *Acción Correctiva y Mejora Continua*, en la fase de acción, se deben implementar medidas correctivas basadas en los hallazgos de las auditorías internas y en los resultados de la evaluación del desempeño del SGSI, es necesario establecer un proceso de mejora continua que permita ajustar y mejorar los controles y procedimientos en función de las lecciones aprendidas y las nuevas amenazas.

De la *Evaluación del Contexto Organizacional y de Riesgo*, sobre el *Contexto Organizacional*, es clave comprender el contexto organizacional para una implementación efectiva del SGSI, esto incluye identificar factores internos y externos que puedan afectar la seguridad de la información, como cambios en la legislación, en la estructura organizacional, o en la tecnología, un análisis exhaustivo del contexto permitirá adaptar el SGSI a las necesidades específicas de la Gobernación del Magdalena.

Sobre la *Evaluación de Riesgos Integral*, la evaluación de riesgos debe ser un proceso sistemático y continuo que identifique, analice y evalúe las amenazas y vulnerabilidades que afectan la seguridad de la información, la implementación de controles adecuados basados en esta evaluación ayudará a mitigar los riesgos identificados, es recomendable utilizar herramientas y metodologías probadas para garantizar una evaluación de riesgos precisa y efectiva.

De la *Recomendaciones para Futuras Investigaciones*, sobre los *Estudios Comparativos*, realizar estudios comparativos entre diferentes entidades gubernamentales que hayan implementado la Norma ISO 27001 permitirá identificar las mejores prácticas y los desafíos

comunes, estos estudios pueden proporcionar insights valiosos sobre cómo abordar problemas similares y optimizar el proceso de implementación en diferentes contextos, analizar casos de éxito y fracaso en la implementación puede ofrecer lecciones útiles y recomendaciones prácticas.

Sobre el *Impacto en la Eficiencia Operativa*, investigar el impacto de la implementación de la Norma ISO 27001 en la eficiencia operativa de las entidades gubernamentales puede ayudar a medir la efectividad de las inversiones en seguridad de la información, evaluar cómo la implementación de la norma contribuye a la mejora de procesos, la reducción de costos y el aumento de la productividad puede proporcionar evidencia tangible de los beneficios y justificar la inversión en el SGSI.

Sobre la *Participación de las Partes Interesadas*, analizar la participación de las partes interesadas en el proceso de implementación es crucial para entender cómo la alta dirección, los empleados, los proveedores y los ciudadanos pueden influir en el éxito del SGSI, investigar cómo la participación activa de estas partes contribuye al éxito de la implementación y cómo puede mejorarse puede proporcionar estrategias efectivas para involucrar a todos los stakeholders.

Sobre el *Desarrollo de Indicadores de Desempeño*, desarrollar indicadores específicos para medir el impacto de la implementación de la Norma ISO 27001 en la seguridad de la información es fundamental para evaluar la efectividad del SGSI, estos indicadores deben incluir medidas de seguridad, satisfacción del usuario y eficiencia operativa. Establecer un sistema de métricas ayudará a realizar un seguimiento del desempeño del SGSI y a realizar ajustes según sea necesario.

La implementación de la Norma ISO 27001 en entidades gubernamentales como el Archivo Central de la Gobernación del Departamento del Magdalena es un proceso complejo que requiere una planificación cuidadosa, una ejecución efectiva y una evaluación continua, la integración de la norma con el PINAR proporciona una base sólida para la gestión de la seguridad de la información, mientras que el enfoque basado en el ciclo PHVA asegura la adaptabilidad y la mejora continua del SGSI.

La evaluación del contexto organizacional y de riesgos, junto con las recomendaciones para futuras investigaciones, ofrece una guía para optimizar la implementación y fortalecer la seguridad de la información en el sector público, las investigaciones futuras pueden contribuir a

mejorar las prácticas de seguridad de la información y a fortalecer la confianza de los ciudadanos en las instituciones gubernamentales, promoviendo un entorno más seguro y eficiente para la gestión de datos sensibles.

Referencias bibliográficas

Arévalo Ascanio, J. G., Bayona Trillos, R. A., & Rico Bautista, D. W. (2015). Implantación de un sistema de gestión de seguridad de información bajo la ISO 27001: Análisis del riesgo de la información. *Tecnura*, *19*(46), 123-134. https://doi.org/10.14483/udistrital.jour.tecnura.2015.4.a10

Estrada-Esponda, R. D., Unás-Gómez, J. L., Flórez-Rincón, O. E., Estrada-Esponda, R. D., Unás-Gómez, J. L., & Flórez-Rincón, O. E. (2021). Prácticas de seguridad de la información en tiempos de pandemia. Caso Universidad del Valle, sede Tuluá. *Revista Logos Ciencia & Tecnología*, *13*(3), 98-110. https://doi.org/10.22335/rlct.v13i3.1446

Martelo, R. J., Madera, J. E., & Betín, A. D. (2015). Software para Gestión Documental, un Componente Modular del Sistema de Gestión de Seguridad de la Información (SGSI). *Información tecnológica*, *26*(2), 129-134. https://doi.org/10.4067/S0718-07642015000200015

Ramos, Y., Urrutia, O., Bravo, A., & Ordoñez, D. (2017). Adoptar una política de seguridad de la información basados en un dominio del estándar NTC ISO/IEC 27002:2013 para la Cooperativa Codelcauca. *Memorias de Congresos UTP*, 88-95.

Rodriguez Baca, L. S., Cruzado Puente de la Vega, C. F., Mejía Corredor, C., & Diaz, M. A. A. (2020). Aplicación de ISO 27001 y su influencia en la seguridad de la información de una empresa privada peruana. *Propósitos y Representaciones*, *8*(3), 11. https://doi.org/10.20511/pyr2020.v8n3.786

Terán Terranova, Y. J. (2021). *Seguridad en la Gestión de la información para las organizaciones públicas desde el enfoque ISO/IEC 2700: Un Mapeo Sistemático* [bachelorThesis]. http://dspace.ups.edu.ec/handle/123456789/20333

Valencia Duque, F., & Orozco-Alzate, M. (2017). Metodología para la implementación de un Sistema de Gestión de Seguridad de la Información basado en la familia de normas ISO/IEC 27000. *RISTI - Revista Ibérica de Sistemas e Tecnologias de Informacao*, 73-88.

Antonow, A. A. (2021). Archivos del silencio. Estado, indígenas y violencia en Patagonia central 1878-1941. *Trabajos y Comunicaciones*, *no. 54*, 3. https://doi.org/10.24215/23468971e156

Arévalo Ascanio, J. G., Bayona Trillos, R. A., & Rico Bautista, D. W. (2015). Implantación de un sistema de gestión de seguridad de información bajo la ISO 27001: Análisis del riesgo de la información. *Tecnura, 19*(46), 123-134. https://doi.org/10.14483/udistrital.jour.tecnura.2015.4.a10

Argüezo Ramirez, E. D. (2019). Propuesta de un Sistema De Gestión De Seguridad de Información para la Protección de Activos de Información Basado en la Norma ISO 27001 en el Área de Informática de la Municipalidad Provincial de Huánuco. *Universidad de Huánuco*, 141.

Barrón de Olivares, V., & D'Aquino, M. (2020). *Proyectos y metodologías de la investigación*. Editorial Maipue. https://elibro.net/es/ereader/uniminuto/160000?page=1

Bautista, V., & Denys, A. (2021). *Análisis de los riesgos de seguridad de la información del sistema de gestión documental de la Alcaldía Municipal de Ibagué*. http://repository.unad.edu.co/handle/10596/51504

Benites Durand, C. A. (2019). Implementación de un sistema de gestión de seguridad de la información—Norma ISO 27001 para la fábrica Radiadores Fortaleza. *Universidad Tecnológica del Perú*, 274.

Bernal Ibarra, G. (2018). *Análisis documental de las metodologías de enseñanza*. 16. http://ciinsev.com/web/revistas/2017-2018/primeraEdicion/REVISTA4/03.pdf

Bernal Torres, C. A. (2016). *Metodología de la investigación: Administración, economía, humanidades y ciencias sociales*. Universidad de La Sabana. http://www.ebooks7-24.com.ezproxy.uniminuto.edu/stage.aspx?il=4326&pg=&ed=

Binda, N. U., & Balbastre-Benavent, F. (2013). Investigación cuantitativa e investigación cualitativa: Buscando las ventajas de las diferentes metodologías de investigación. *Revista de Ciencias Económicas*, *31*(2), Article 2.

Briones, G. (2022). *Metodología de la investigación cuantitativa en las ciencias sociales*. 219.

Buitrago Rojas, D. S., & Alvarado Romero, E. L. (2018). *Sistema de gestión de seguridad de la información (SGSI) aplicada al área de operaciones de una Empresa de Telecomunicaciones.* 89.

Cardona Fernández, J. I., & Restrepo Granada, R. A. (2020). *Evaluación de la implementación de la norma ISO 27001 en empresas del sector privado, bajo un enfoque cultural*. 13.

Chávarry Bonilla, S. N. F. (2021). Implementación de ISO 27001 y 27002 adaptadas para gestión de seguridad de información en Secretaría Ejecutiva de Policía Nacional del Perú. *Repositorio Institucional - UCV*, 132.

Congreso de la Republica. (1995). *Decreto Ley 2150 de 1995*. https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=1208

Congreso de la Republica. (2011). *Decreto 3573 de 2011*. https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=64920

Congreso de la Republica. (2014). *Ley 1712 de 2014*. https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=56882

Pulido-Daza, N. J., & Pérez, E. P. (2019). Buenas prácticas para la administración: Caso de estudio gobernación del valle del cauca. *Revista CODICES*, *15*(I y II), Article I y II.

Dominguez, J. A. P., Caipo, Y. G. L., & Santos, A. M. D. los. (2022). Efectos de la implementación de un SGSI basado en la norma ISO 27001 para las organizaciones. *Perfiles de Ingeniería*, *18*(18), Article 18. https://doi.org/10.31381/perfilesingenieria.v18i18.5399

Egea Sossa, J. A., & López Rodríguez, C. (2021). *Desarrollo de aplicación web para la gestión de la documentación en ISO 27001 haciendo uso de herramientas de software libre*. http://repositorio.uts.edu.co:8080/xmlui/handle/123456789/7567

Estrada-Esponda, R. D., Unás-Gómez, J. L., Flórez-Rincón, O. E., Estrada-Esponda, R. D., Unás-Gómez, J. L., & Flórez-Rincón, O. E. (2021). Prácticas de seguridad de la información en tiempos de pandemia. Caso Universidad del Valle, sede Tuluá. *Revista Logos Ciencia & Tecnología*, *13*(3), 98-110. https://doi.org/10.22335/rlct.v13i3.1446

Ferreiro Gravié, R. (2017). *¿Cómo ser maestro investigador? – El Método Javi*. Corporación Universitaria Minuto de Dios. https://repository.uniminuto.edu/bitstream/10656/10167/1/Libro_Como%20ser%20maestro%20investigador_2017.pdf

Garcia Cruz, R. A. (2021). Propuesta de un sistema de gestión de seguridad de la información basado en la norma ISO 27001 para la oficina de Tecnologías de Información del gobierno regional Piura; 2020. *Universidad Católica Los Ángeles de Chimbote*, 102.

Garzón Barón, J. L. (2018). *Guía de seguridad de la información basada en la norma ISO 27001 y el estándar NIST-IR 7621 revisión 1 del National Institute Of Standards And Technology para pymes, con diseño de políticas para la empresa profesionales Asociados Ltda.* 105.

Giraldo Bedoya, N. M., & Arias Vanegas, C. (2020). *Razones de la falta de certificación de las organizaciones colombianas en la norma ISO/IEC 27001:2013*. 17.

Gobernación del Magdalena. (2023). *Gobernación del Magdalena*. Gobernación del Magdalena. https://www.gobernaciondelmagdalena.gov.co/

Hernández Sampieri, R., & Mendoza Torres, C. P. (2018). *Metodología de la investigación: Las rutas: cuantitativa ,cualitativa y mixta*. Mc Graw Hill educación. http://repositorio.uasb.edu.bo/handle/54000/1292

Lema Vinlasaca, R. C. (2018). *Implementación de un sistema de gestión de seguridad de información basado en la Norma ISO 27001:2013 para el control físico y digital de documentos aplicado a la empresa LOCKERS S.A.*

Macedonio, M. N. L. (2018). El archivo de la Dirección Federal de Seguridad: Una fuente para escribir la historia de la segunda mitad del siglo XX mexicano. *Boletín del Archivo General de la Nación*, *8*(15), Article 15. https://doi.org/10.31911/bagn.2018.8.15.29

Martelo, R. J., Madera, J. E., & Betín, A. D. (2015). Software para Gestión Documental, un Componente Modular del Sistema de Gestión de Seguridad de la Información (SGSI).

Información tecnológica, *26*(2), 129-134. https://doi.org/10.4067/S0718-07642015000200015

Martín, T. de la R. (2021). Automatización de un sistema de gestión de seguridad de la información basado en la Norma ISO/IEC 27001. *Revista Universidad y Sociedad*, *13*(5), 495-506.

Montalbán, E. A. R., Gómez, R. J. M., & Borré, D. A. F. (2020). Diseño de un sistema de gestión de seguridad de la información para el proceso administrativo de la infraestructura tecnológica de instituciones académicas basado en Magerit. *Aglala*, *11*(1), Article 1.

Montalvo Cisneros, O. A. (2021). *Efectos de la implementación de una auditoría informática a las empresas de seguros a través de la ISO 27001 :2013 ubicadas en el Norte del DMQ.* [bachelorThesis]. http://dspace.ups.edu.ec/handle/123456789/19918

Mori, L. Y. (2021). Especificaciones ambientales y técnicas de seguridad para el diseño de la infraestructura física de un archivo central. *Revista del Archivo General de la Nación*, *36*(1), Article 1. https://doi.org/10.37840/ragn.v36i1.126

Moscaiza Moncada, O. I. (2018). *Diseño de un sistema de gestión de la seguridad de la información (SGSI) para la Cooperativa de Ahorro y Crédito ABC, basado en la norma ISO 27001:2013*.

Muñoz, P. (2015). *Metodología de la investigación científica*. 41.

Navarro Martínez, J. (2018). *Creación de una guía de auditoría para el cumplimiento de la norma UNE-ISO 27001* [Proyecto/Trabajo fin de carrera/grado, Universitat Politècnica de València]. https://riunet.upv.es/handle/10251/111385

Preciado Cortez, Y. Y. (2022). *Análisis de un sistema de información basado en la norma de seguridad informática ISO 27001 para la reducción de las posibles vulnerabilidades en*

la empresa privada Atimasa S.A. de la ciudad de Guayaquil. [Universidad de Guayaquil. Facultad de Ingeniería Industrial. Carrera de Licenciatura en Sistemas de Información.]. http://repositorio.ug.edu.ec/handle/redug/64646

Ramos, Y., Urrutia, O., Bravo, A., & Ordoñez, D. (2017). Adoptar una política de seguridad de la información basados en un dominio del estándar NTC ISO/IEC 27002:2013 para la Cooperativa Codelcauca. *Memorias de Congresos UTP*, 88-95.

Rodriguez Baca, L. S., Cruzado Puente de la Vega, C. F., Mejía Corredor, C., & Diaz, M. A. A. (2020). Aplicación de ISO 27001 y su influencia en la seguridad de la información de una empresa privada peruana. *Propósitos y Representaciones*, *8*(3), 11. https://doi.org/10.20511/pyr2020.v8n3.786

Rodríguez Bustos, A. L. (2019). *Nivel de madurez de seguridad en el área de redes de la Universidad Pedagógica y Tecnológica de Colombia (U.P.T.C) Tunja, basado en Norma ISO 27001*. 97.

Rodríguez, G. R. D. L. C., Fernández, R. A. M., & Santos, A. C. M. D. L. (2023). Seguridad de la información en el comercio electrónico basado en ISO 27001: Una revisión sistemática. *Innovación y Software*, *4*(1), Article 1. https://doi.org/10.48168/innosoft.s11.a79

Rodriguez Zapata, Y. A. (2021). *El papel fundamental de las nuevas tecnologías de la información y comunicación para la gestión de la seguridad en las organizaciones*. 17.

Rosales Montalban, E. A. (2019). *Diseño de un sistema de gestión de seguridad de la información para el proceso de gestión de la infraestructura tecnológica del Colegio Salesiano basado en Magerit*. 67. https://doi.org/10.57799/11227/8399

Sepúlveda, A. B., & Jaramillo, C. B. (2018). Modelo sistema de gestión de seguridad de la información para instituciones educativas de nivel básico. *Scientia Et Technica*, *23*(1), 85-92.

Terán Terranova, Y. J. (2021). *Seguridad en la Gestión de la información para las organizaciones públicas desde el enfoque ISO/IEC 2700: Un Mapeo Sistemático* [bachelorThesis]. http://dspace.ups.edu.ec/handle/123456789/20333

Torres Chango, C. D. (2020). *Plan de seguridad informática basado en la norma iso 27001, para proteger la información y activos de la empresa privada Megaprofer S.A.* [bachelorThesis, Universidad Técnica de Ambato. Facultad de Ingeniería en Sistemas, Electrónica e Industrial. Carrera de Ingeniería en Sistemas Computacionales e Informáticos]. https://repositorio.uta.edu.ec:8443/jspui/handle/123456789/30690

Valencia Duque, F. J. (2021). *Sistema de gestión de seguridad de la información basado en la familia de normas ISO/IEC 27000*. Centro Editorial de la Facultad de Administración. https://repositorio.unal.edu.co/handle/unal/80158

Valencia Duque, F., & Orozco-Alzate, M. (2017). Metodología para la implementación de un Sistema de Gestión de Seguridad de la Información basado en la familia de normas ISO/IEC 27000. *RISTI - Revista Iberica de Sistemas e Tecnologias de Informacao*, 73-88.

Yungán Cazar, J. C., & Narváez Contero, C. V. (2022). Aplicación de la Norma ISO 27001 para la seguridad de los Sistemas de Información. *Dominio de las Ciencias*, *8*(3), 14.