Elaborar las políticas de seguridad de la información para la alcaldía de Tamalameque, Cesar, de acuerdo con los lineamientos del mintic, con el propósito de establecer un marco normativo que mejore la gestión y el manejo de la información institucional

José Luis Robles Machuca

Informe final de prácticas para optar por el título de ingeniero de sistemas

Mag. Erney Alberto Ramírez Camargo

Director

Universidad Popular del Cesar Seccional Aguachica

Facultad Ingenierías y Tecnologías

Ingeniería De Sistemas

2026

Resumen

La finalidad de este trabajo final de grado es desarrollar las políticas informativas para la Alcaldía de Tamalameque, Cesar, siguiendo las directrices del Ministerio de Tecnologías de la Información y las Comunicaciones (MINTIC, 2020). El objetivo principal es crear un marco normativo que potencie la administración y el manejo de la información dentro de la institución, asegurando la transparencia, la eficacia y la seguridad en los procesos administrativos. Este trabajo se lleva a cabo en un entorno donde las instituciones públicas afrontan el desafío de ajustarse a la digitalización y de salvaguardar la información que gestionan de manera apropiada.

Se llevó a cabo la investigación utilizando una metodología mixta que integró el análisis normativo, la revisión de documentos y la realización de encuestas a los empleados de la entidad. Los hallazgos mostraron que hay limitaciones tecnológicas, insuficiencias en la clasificación y protección de datos y falta de políticas institucionales consolidadas, lo cual dificulta la gestión documental. Se establecieron políticas de seguridad de la información con el objetivo de optimizar la gestión documental, aumentar la seguridad de los datos y promover la interoperabilidad entre los sistemas institucionales, a partir del diagnóstico. Asimismo, se propuso una estrategia de socialización con el fin de garantizar que los funcionarios públicos comprendan y asimilen estas políticas. Para concluir, la monografía brinda un marco guía que ayuda a modernizar la administración municipal, en línea con los principios del (MINTIC, 2020) y con las demandas contemporáneas de la gestión pública digital.

***Palabras clave*:** Políticas de seguridad de la información, gestión documental, Gobierno Digital, MinTIC, transparencia, Administración Pública.

Abstract

The purpose of this final degree project is to develop information policies for the Mayor's Office of Tamalameque, Cesar, in accordance with the guidelines established by the Ministry of Information and Communication Technologies (MINTIC, 2020). The main objective is to create a regulatory framework that strengthens the administration and management of institutional information, ensuring transparency, efficiency, and security in administrative processes. This study takes place in a context where public institutions face the challenge of adapting to digital transformation while safeguarding the information they manage appropriately.

A mixed methodology was used, integrating regulatory analysis, document review, and surveys conducted with the institution's employees. The findings revealed technological limitations, weaknesses in data classification and protection, and the absence of consolidated institutional policies, which hinder effective document management. Based on the diagnosis, information policies were established to optimize document management, enhance data security, and promote interoperability among institutional systems. Likewise, a socialization strategy was proposed to ensure that public officials understand and adopt these policies. In conclusion, this monograph provides a guiding framework that contributes to the modernization of municipal administration, in alignment with the principles of (MINTIC, 2020)) and the contemporary demands of digital public management.

Keywords: Information policies, document management, Digital Government, MINTIC, transparency, Public Administration.

Contenido

Pág.

Lista de figuras

Lista de tablas

Pág.

Introducción

Los continuos avances tecnológicos desde la Tercera Revolución Industrial, impulsados por los avances en las tecnologías de la información y las comunicaciones, han hecho fundamental que las instituciones y empresas adapten sus procesos a los requisitos del entorno digital. Este contexto es especialmente relevante en el sector público, donde la gestión eficaz de la información es clave para la transparencia, la eficiencia y el servicio al público.

La Alcaldía de Tamalameque César está dando un paso importante hacia la modernización de su gestión mediante el desarrollo de una política de información en línea con el Ministerio de Tecnologías de la Información y las Comunicaciones (MINTIC, 2020). Estos esfuerzos apuntan no sólo a mejorar la calidad y seguridad de la información mantenida por a la Alcaldía de Tamalameque Cesar, sino también a facilitar el acceso y uso de esta información por parte de los ciudadanos y el personal.

Las instituciones de educación superior, que forman a futuros profesionales en ingeniería y otros campos relacionados, juegan un papel importante en este proceso. A través de programas de pasantías empresariales, como los que se llevan a cabo en la Alcaldía de Tamalameque, los estudiantes tienen la oportunidad de aplicar sus conocimientos en entornos del mundo real, contribuyendo así al desarrollo de proyectos que tienen un impacto tangible en la comunidad local.

El proyecto no solo ayudará a la Alcaldía de Tamalameque a modernizarse y cumplir con las leyes, sino que también brindará a los estudiantes una experiencia valiosa que mejorará su formación académica y profesional. Por lo tanto, la colaboración entre los sectores público y académico es esencial para el crecimiento mutuo y para afrontar los desafíos de la transformación digital en la administración pública.

Justificación

En la actual era digital, la gestión adecuada y eficiente de la información se ha convertido en un pilar fundamental para el correcto funcionamiento de las entidades públicas y privadas (Cueto, 2023). La Alcaldía de Tamalameque, César, no está exenta de ello, debido a que la adopción de políticas de seguridad de la información como la Seguridad de la Información, la Arquitectura Empresarial y los Servicios Ciudadanos Digitales, alineadas con los lineamientos del Ministerio de Tecnologías de la Información y las Comunicaciones (MINTIC, 2020) es esencial para garantizar la transparencia, accesibilidad y seguridad de la información (Simões, 2023). Estas políticas optimizan los procesos internos y mejoran la toma de decisiones y la comunicación con los ciudadanos, aumentando la confianza en las instituciones locales.

Para cumplir con las regulaciones legales vigentes, también es esencial establecer políticas de seguridad de la información adecuadas, como la Ley de Transparencia y Acceso a la Información Pública (Ley 1712, 2014) . Garantizar que la información generada y custodiada por la Alcaldía se maneje de manera segura, eficiente y accesible no solo es un requisito legal, sino que también es esencial para la modernización administrativa y la integración con las estrategias nacionales de gobierno digital (Superservicios , 2023).

Además, la implementación de estas políticas tendrá un impacto directo en la calidad y eficacia de los servicios que la Alcaldía brinda a la comunidad. La gestión adecuada de la información permitirá satisfacer las necesidades de los ciudadanos de manera más rápida y precisa, mejorando la calidad del servicio público (Gestio documental, 2023).Para los trabajadores de la Alcaldía, esto implicaría que tendrían que aprender más acerca del manejo de las tecnologías de la información y adquirir nuevas herramientas que les ayuden a realizar sus tareas diarias.

Esta tarea es una gran oportunidad para los estudiantes de ingeniería de sistemas para aplicar sus conocimientos técnicos en el mundo real y desarrollar competencias en gestión de sistemas de información, seguridad informática y gobernanza de datos. (Jain, 2020).

Además, una mayor eficiencia administrativa y una mejor relación entre el gobierno local y la ciudadanía reflejarán el impacto social de esta labor. El estudiante contribuye directamente al desarrollo de un entorno más transparente, eficiente y centrado en el ciudadano al participar en este proyecto, lo que representa un importante aporte tanto para su formación profesional como para la comunidad en general.

Identificación de la problemática

La Alcaldía de Tamalameque, César, enfrenta desafíos significativos en la gestión de su información institucional. Actualmente, se presentan ineficiencias que dificultan el acceso oportuno a la información, la trazabilidad de documentos y la protección de datos sensibles. Estas deficiencias se deben a la ausencia de políticas claras y formalizadas que estén alineadas con los lineamientos del Ministerio de Tecnologías de la Información y las Comunicaciones (MINTIC, 2020). Esta situación limita la capacidad de la Alcaldía para atender las demandas ciudadanas de manera transparente y eficiente, generando incertidumbre entre la población del municipio.

Si bien la gestión de la información presenta avances en aspectos como la digitalización parcial de archivos, el uso de correos institucionales y la existencia de formatos internos para trámites administrativos, estos esfuerzos carecen de una estructura normativa que los articule con las prácticas nacionales establecidas en la (Ley 1712, 2014). La falta de estandarización y documentación formal impide consolidar una política institucional robusta. La administración

podrá cumplir con las exigencias legales y aumentar la eficiencia interna y la confianza del público al implementar políticas de seguridad de la información que formalicen los procesos, definan responsabilidades y garanticen la trazabilidad documental (ciberlinea, 2024)

La falta de capacitación del personal en tecnología de la información y la ausencia de un sistema integral que permita una gestión eficiente de los datos agrava este problema. (Mariana, 2024). La implementación de políticas de seguridad de la información adecuadas es crucial para superar estos desafíos (Políticas Técnicas de Seguridad de la Información , 2020), asegurando que la Alcaldía no solo cumpla con las normas legales, sino que también mejore sus procesos internos y brinde un mejor servicio a la comunidad.

Teniendo en cuenta lo anterior, es necesario desarrollar e implementar políticas de seguridad de la información que garanticen la integridad, y disponibilidad de los datos, así como la capacitación continua del personal (Ciberseguridad, 2021). Es importante que estas políticas se ajusten a los lineamientos del (MINTIC, 2020) y se adapten a las necesidades particulares de la Alcaldía de Tamalameque, lo que permitirá una gestión de la información más efectiva, clara y enfocada en el bienestar del ciudadano. La solución a estos problemas aumentará el desempeño administrativo de la Alcaldía y aumentará la confianza de la ciudadanía en las instituciones locales.

Metodología

Para abordar la elaboración de políticas de seguridad de la información para la Alcaldía de Tamalameque, César, se empleará un enfoque metodológico mixto, que integra técnicas de investigación cualitativa y cuantitativa.

La investigación cualitativa se centrará en comprender las percepciones, experiencias y necesidades del personal administrativo respecto a la gestión de la información institucional. Para ello, se realizarán entrevistas en profundidad con empleados clave, grupos focales con áreas estratégicas, y análisis documental de normativas vigentes, manuales internos y registros administrativos. Estos métodos permitirán identificar las barreras, fortalezas y oportunidades desde una perspectiva interpretativa.

Por su parte, la investigación cuantitativa se enfocará en la recolección de datos estadísticos mediante encuestas estructuradas aplicadas al personal de la Alcaldía. Estas encuestas medirán variables como el nivel de conocimiento sobre políticas de seguridad de la información, el grado de cumplimiento de procesos documentales, y la percepción general sobre la eficiencia institucional. Además, se analizarán indicadores internos de desempeño para establecer una línea base que permita evaluar el impacto de las políticas propuestas.

La combinación de ambos enfoques permitirá construir un diagnóstico integral que sirva como fundamento para el diseño de políticas de seguridad de la información alineadas con los lineamientos del (MINTIC, 2020)

Con base en los hallazgos, se diseñarán y formalizarán las políticas de seguridad de la información alineadas con los lineamientos del (MINTIC, 2020), desarrollando un marco normativo que mejore la gestión institucional. La metodología también incluirá la implementación de programas de capacitación para el personal y un sistema de monitoreo para

evaluar y ajustar las políticas según sea necesario. Este enfoque integral busca optimizar la gestión de la información, mejorar la transparencia y eficacia administrativa, y fortalecer la confianza ciudadana en la Alcaldía.

Objetivos

Objetivo general

Elaborar las políticas de seguridad de la información para la Alcaldía de Tamalameque, Cesar, de acuerdo con los lineamientos del (MINTIC, 2020) con el propósito de establecer un marco normativo que mejore la gestión y el manejo de la información institucional.

Objetivos específicos

Realizar un diagnóstico del estado actual de la gestión de la información en la Alcaldía de Tamalameque, Cesar, para identificar fortalezas, debilidades y necesidades de mejora en relación con los lineamientos del MINTIC.

Diseñar las políticas de seguridad de la información necesarias para la Alcaldía de Tamalameque, Cesar, que se ajusten a los lineamientos establecidos por el MINTIC y respondan a las necesidades identificadas en el diagnóstico.

Socializar las políticas de seguridad de la información desarrolladas para la Alcaldía de Tamalameque, Cesar, asegurando que todas las partes interesadas comprendan y apoyen las políticas y el marco normativo propuestos.

Marco referencial

Antecedentes

En la era de la transformación digital, las organizaciones públicas enfrentan el reto de garantizar la gestión eficiente, segura y transparente de la información. En Colombia, los lineamientos establecidos por el Ministerio de Tecnologías de la Información y las Comunicaciones (MINTIC, 2020) proporcionan un marco normativo para orientar a las entidades en la adopción de políticas que promuevan el uso adecuado de los recursos tecnológicos y la protección de los datos.

La Alcaldía de Tamalameque, Cesar, como entidad pública encargada de coordinar y ejecutar políticas y proyectos en beneficio de la comunidad, se encuentra en un contexto en el que la gestión de la información es esencial para la toma de decisiones, la prestación de servicios y la rendición de cuentas. Sin embargo, la ausencia de políticas claras de información podría generar riesgos como la pérdida de datos, el acceso no autorizado y la falta de control en el manejo de recursos tecnológicos, a continuación, se presentan proyectos relacionados:

Internacionales

Se investigó a nivel internacional y se encontró que en la Universidad Internacional Sek (Ecuador), (Pilla, 2019), presentó un proyecto titulado “Diseño de una política de seguridad de la información para el área de tecnología de la información de la cooperativa de ahorro y crédito chibuleo ltda., basado en la norma iso/iec 27002:2013” cuyo objetivo es el diseño de una política de seguridad de la información para el área de Tecnología de la Información (TI) de la Cooperativa de Ahorro y Crédito Chibuleo Ltda., basado en la norma ISO/IEC 27002:2013. Esta propuesta tiene con la finalidad mitigar posibles vulnerabilidades en los sistemas de información, estableciendo dominios, objetivos y controles para la gestión de la seguridad de la información.

Previo al desarrollo de la misma, se realizó un análisis inicial del estado de la seguridad de la información del área de TI, a través de reuniones con distintos involucrados del departamento. Posteriormente, los resultados se sintetizaron en una matriz de riesgos de Deloitte (2015) y del Banco de España (2012), donde se detallan los activos de información y los riesgos a evaluar.

Por otra parte, (Bustamante García et al., 2021) en (Perú), presentaron un proyecto titulado "Políticas basadas en la iso 27001:2013 y su influencia en la gestión de seguridad de la información en municipalidades de Perú" cuyo objetivo principal fue mejorar la gestión de seguridad de la información en una municipalidad distrital peruana, mediante la implantación de un modelo de políticas basado en la ISO 27001:2013. Para ello, se hizo una investigación preexperimental con una muestra de 30 trabajadores a quienes se les aplicó un cuestionario para medir el grado de satisfacción con el modelo implantado. En promedio, más del 90 % de los encuestados reconoció mejoras en la municipalidad, lo que marca una gran diferencia entre el pre y postest, de 49 % a 96 %. Se concluye que el modelo de políticas de seguridad basado en tres pilares fundamentales: confidencialidad, integridad y disponibilidad mejoró la gestión de seguridad de la información, garantizando un adecuado resguardo de los datos.

También, (Sepúlveda & Cravero, 2021) en Chile, presentaron un proyecto titulado "Diseño de una política de seguridad de la información" donde el objetivo principal fue presentar una propuesta para el diseño de políticas de seguridad de la información (SI), en el departamento de TIC de una empresa regional. La metodología usada se basa en la obtención de información de los dominios asociados a la norma ISO 27002 dentro de la empresa. Los resultados muestran una mejora en la SI de la empresa, considerando la elaboración de procedimientos y controles para restringir el acceso a los datos y ciertas dependencias de la empresa, principalmente del departamento TIC.

Además, en la Universidad Cesar Vallejo en Perú, (Giap & Villarreal, 2021), elaboraron un proyecto titulado “Sistema de gestión para la seguridad de la información basado en la Norma ISO/IEC 27001:2013 en la Empresa Constructora Pérez & Pérez SAC, Moyobamba, San Martín,2021”, tuvo como objetivo principal determinar la influencia de un sistema de gestión para la seguridad de la información basado en la norma 270001:2013 en la Empresa Constructora Pérez & Pérez SAC, ya que presenta vulnerabilidades en todos los procesos de todas las áreas y peligra los activos de información de la organización, la metodología fue cuantitativa aplicada, se trabajó con el diseño de investigación experimental del tipo preexperimental. Además, se conformó la muestra de 20 registros en cada indicador con la finalidad de obtener un resultado favorable en las dimensiones de seguridad de la información, la confidencialidad de la información de un 68,85% de vulnerabilidad disminuyó a un 15,40% para la integridad de la información tuvo una disminución de vulnerabilidad de un 52,60% a 11,40% y por último la disponibilidad de la información se logró disminuir la vulnerabilidad de un 47,15% a 11,95% en los tres dimensiones se logró aumentar la seguridad de la información a un 80% a 90% de efectividad. Finalmente se acierta que el sistema de gestión para la seguridad de la información basado en la norma iso27001 influye favorablemente en la constructora Pérez & Pérez SAC

Nacionales

A nivel nacional se encontró que (Marin, 2017), en la Universidad Nacional Abierta y a Distancia realizo un trabajo de grado titulado “Diseño e implementación de una política de seguridad de información, en el grupo de trabajo cuentas por pagar del ministerio de transporte”, cuyo objetivo fue diseñar e implementar una política de seguridad informática, dirigida a la información digital que se maneja en el Grupo de Cuentas por Pagar; hacer seguimiento y actualización a esta política y la debida socialización; no solo a nivel de grupo, sino a nivel

Subdirección Administrativa y Financiera; pues en cada grupo se maneja información digital diferente; pero en las que se puede implementar esta política de seguridad informática

También, Grupo ACS (2022) elaboró sus "Política de seguridad de la información", cuyo objetivo principal fue establecer los requisitos para proteger la información, los equipos y servicios tecnológicos que sirven de soporte para la mayoría de los procesos de negocio de ACS, Actividades de Construcción y Servicios, S.A. (en adelante, ACS) y las sociedades que componen su grupo de empresas (en adelante, Grupo ACS). Esta Política de Seguridad de la Información es la pieza angular por la que se rige el Cuerpo Normativo de Seguridad del Grupo ACS. El Cuerpo Normativo de Seguridad (en adelante, CNS) es un conjunto de documentos a diferentes niveles que conforman los requerimientos, directrices y protocolos que debe seguir el Grupo ACS en materia de seguridad. El CNS deberá ser desarrollado por cada sociedad del Grupo ACS mediante un conjunto de documentos (normas de uso, estándares normativos, procedimientos, manuales, guías, buenas prácticas, etc.) de tal manera que cubran todos los aspectos que se presentan en la Política, llegando a nivel de proceso operativo.

Además, en la Universidad Católica De Colombia, (Ortiz, 2021), se realizó un trabajo de grado titulado "Diseño De Las Políticas De Seguridad De La Información En La Compañía De Seguros S.A", cuyo objetivo fue el diseño de las Políticas de Seguridad de la Información para la Compañía de Seguros S.A. tomando como referencia el estándar ISO27001:2013 que apoye el fortalecimiento del SGSI, fomente el desarrollo de la cultura de seguridad de la información en la compañía y principalmente al cumplimiento de los requerimientos regulatorios de la Superintendencia Financiera de Colombia (SFC) en materia de seguridad.

Por otra parte, (Cuesta, 2022) realizó un "Análisis de la seguridad de la información en entidades públicas de Colombia" cuyo objetivo fue analizar las medidas adoptadas por el

Departamento Administrativo de la Presidencia de la República, de acuerdo con el modelo de Seguridad y Privacidad de la Información (MSPI) durante los años 2020-2022.

Locales

En la alcaldía de Bosconia – Cesar, el alcalde (Patiño, 2024), Elaboró el "Plan tratamiento de riesgo de seguridad y privacidad de la información" cuyo objetivo principal fue conocer la situación actual de la entidad territorial, así como sus activos y amenazas, luego se efectuar la medición de riesgos existentes y hacer las sugerencias necesarias para garantizar la protección de la información. Con este documento se busca mejorar la prestación de los servicios de tecnologías de la información que presta la Alcaldía Municipal de Bosconia, en el marco del cumplimiento de la Política de Gobierno Digital.

A demás, la empresa: corporación autónoma regional del cesar (CORPOCESAR), elaboró sus "Políticas de seguridad informática" cuyo objetivo fue brindar a los usuarios los recursos informáticos con la cantidad y calidad que demandan, esto es, que tengamos continuidad en el servicio los 365 días del año confiable. Así, la cantidad de recursos de cómputo y de telecomunicaciones con que cuenta el Centro son de consideración y se requiere que se protejan para garantizar su buen funcionamiento.

La seguridad de las instituciones en muchos de los países se ha convertido en cuestión de seguridad nacional, por ello contar con un documento de políticas de seguridad es imprescindible, y se debe plasmar mecanismos que con base en la política institucional proteja los activos del Centro.

Así pues, ante este panorama surge el siguiente proyecto de políticas rectoras que harán que la Dirección de Telemática pueda disponer de los ejes de proyección que en materia de seguridad la Institución requiere.

Marco Teórico

Este marco teórico apoya la elaboración de políticas de seguridad de la información para la Alcaldía de Tamalameque, César, al incorporar principios técnicos, conceptuales y normativos que guían el acceso ciudadano, la seguridad informacional y la gestión documental.

Protección de la información (ISO/IEC 27001)

La norma ISO/IEC 27001 define un sistema de gestión de la seguridad de la información apoyado en tres principios esenciales:

- Confidencialidad: Protección de datos contra accesos no permitidos.
- Integridad: Aseguramiento de que la información no se modifique sin permiso.
- Disponibilidad: Acceso oportuno a la información cuando sea necesario.

Asimismo, fomenta una perspectiva fundamentada en riesgos, que posibilita detectar amenazas, implementar controles y ajustar las políticas de seguridad a lo que la institución requiere.

Transparencia y acceso a la información pública (Ley 1712 de 2014)

La (Ley 1712, 2014) reconoce la información pública como un bien colectivo. Sus principios clave son:

- Publicidad y máxima divulgación
- Accesibilidad
- Rendición de cuentas
- No discriminación

Este marco legal exige que las entidades públicas garanticen el acceso libre, oportuno y comprensible a la información, fortaleciendo la democracia y el control social.

Protección de datos personales (Solove, 2006)

(Solove, 2006) sugiere un enfoque integral para enfrentar los retos que supone la privacidad en la época digital. Su modelo sobresale:

- La interrelación de problemas como la vigilancia, la explotación de datos y la discriminación.
- La exigencia de políticas institucionales transparentes y marcos normativos robustos.
- La relevancia de promover una ética de protección de datos.

Gestión de riesgos informáticos (ISO 31000)

La norma ISO 31000 ofrece un marco estructurado para reconocer, analizar y manejar los riesgos que ponen en peligro la seguridad, la disponibilidad y la integridad de los datos. Esta perspectiva permite:

- Disminuir los efectos adversos.
- Ampliar posibilidades en ambientes digitales.
- Robustecer la gobernanza informativa.

Marco Conceptual

Políticas de seguridad de la información

Las políticas de seguridad de la información son un conjunto de normas, directrices y procedimientos orientados a proteger la confidencialidad, integridad y disponibilidad de la información dentro de una organización. Estas establecen controles sobre el acceso, uso, almacenamiento y transmisión de los datos, con el fin de prevenir riesgos, minimizar vulnerabilidades y garantizar el cumplimiento de requisitos legales y normativos. Su objetivo es salvaguardar los activos de información, fortalecer la gestión de la seguridad y promover una cultura organizacional basada en la protección de los datos (Bustamante García et al., 2021).

Manejo de la información

La administración de la información incluye el ciclo organizativo de adquisición, resguardo, procesamiento, distribución y eliminación de datos, con el objetivo de respaldar la decisión y operación institucional. Incluye herramientas de tecnología, regulaciones y tácticas que garantizan la calidad, la utilidad y el acceso a la información (Cueto, 2023)

Directrices del MINTIC

Los lineamientos de la Política de Gobierno Digital son determinados por el Ministerio de Tecnologías de la Información y las Comunicaciones (MINTIC). Estos lineamientos engloban habilitadores como los servicios ciudadanos digitales, la seguridad informativa y la arquitectura empresarial (MINTIC, 2020)

Gobierno digital

El gobierno digital es una táctica de modernización administrativa que emplea tecnologías informáticas para perfeccionar la eficacia, la transparencia y el acceso a los servicios públicos. Su implementación posibilita que las entidades intercambien información, divulguen datos abiertos y participen digitalmente los ciudadanos (MINTIC, 2020)

Seguridad de la información

Los principios de confidencialidad, integridad y disponibilidad, definidos por la norma ISO/IEC 27001, son la base de la seguridad de la información. Para salvaguardar los activos informacionales de accesos no autorizados, cambios o pérdidas, esta norma establece controles organizacionales, físicos y tecnológicos (Ciberseguridad, 2021)

Protección de datos personales

La Ley Estatutaria 1581 de 2012 es la que regula en Colombia la protección de los datos personales, y esta ley determina derechos para aquellos que tienen la información y deberes para

quienes la administran. Esta ley requiere que se implementen medidas de seguridad para proteger la privacidad, que se establezca una finalidad legítima del tratamiento y que se obtenga el consentimiento informado (Superservicios., 2023)

Disponibilidad

Un principio de la seguridad informática es la disponibilidad, que garantiza a los usuarios autorizados el acceso fiable y en el momento adecuado a los datos. Conforme a normas como la ENS y la ISO 27000, este acceso debe fundamentarse en el principio de "necesidad de conocer", restringiendo el empleo de la información únicamente a aquellos que la necesiten para llevar a cabo sus funciones (Grupo ACS, 2022)

Interoperabilidad

La interoperabilidad hace referencia a la habilidad de los sistemas de información para intercambiar datos de forma eficaz y segura. En el ámbito público, posibilita que los organismos gubernamentales optimicen procesos, integren sus plataformas y tomen decisiones fundadas en datos actualizados (Patiño, 2024)

Marco Legal

Constitución Política de Colombia: La Constitución de 1991 es el fundamento jurídico más importante del país, estableciendo los derechos y deberes fundamentales de los ciudadanos y las entidades públicas. En particular, los artículos relacionados con la libertad de información y la transparencia en el manejo de los recursos públicos son esenciales para la Alcaldía de Tamalameque.

La (Ley 1712, 2014), que se desprende de la Constitución, refuerza el derecho de acceso a la información pública, asegurando que las entidades públicas, como la Alcaldía, deben facilitar el acceso a los documentos e información administrativa en sus diferentes modalidades.

Además, establece los mecanismos para garantizar que dicha información sea clara, accesible y esté debidamente organizada.

(Ley 1581 de 2012, s.f.)– Protección de Datos Personales: Esta ley tiene como objetivo establecer disposiciones para garantizar la protección de los datos personales en Colombia, regulando la recolección, almacenamiento, tratamiento y circulación de la información. En el contexto de la Alcaldía de Tamalameque, es fundamental cumplir con estos principios, especialmente al gestionar la información de los ciudadanos y empleados públicos. Las políticas de seguridad de la información deben incluir prácticas que aseguren el cumplimiento de esta ley, como la obtención de autorizaciones explícitas para el tratamiento de datos personales, la implementación de mecanismos de seguridad para prevenir su acceso no autorizado y la creación de protocolos para el manejo de solicitudes de los ciudadanos sobre sus datos personales.

(Ley 1266 de 2008, s.f.) **–** Hábeas Data: establece el régimen jurídico para el manejo de la información financiera, crediticia, comercial y de servicios de los ciudadanos, asegurando el derecho a la intimidad y el control sobre los datos personales. Aunque la Ley 1266 está más centrada en la protección de datos en el ámbito financiero, tiene implicaciones importantes para la Alcaldía de Tamalameque al tratar con la información de los habitantes en relación con servicios públicos, impuestos y otros trámites administrativos. Las políticas de seguridad de la información deben prever mecanismos para garantizar que los ciudadanos puedan acceder, corregir y eliminar sus datos personales en poder de la administración, además de proteger la información frente a riesgos de uso indebido.

Norma ISO 27001 – Sistema de Gestión de Seguridad de la Información: Aunque no es una ley nacional, la ISO 27001 es una norma internacional clave en la gestión de la seguridad de la información. Esta norma establece los requisitos para un sistema de gestión que proteja la

información, con el fin de garantizar su confidencialidad, integridad y disponibilidad. En el contexto de la Alcaldía de Tamalameque, implementar la ISO 27001 permitirá establecer procedimientos y controles para proteger la información sensible que maneja la institución, como datos personales de los ciudadanos y documentos administrativos. Además, contribuirá a asegurar que la gestión de la información cumpla con los estándares internacionales de seguridad, reduciendo los riesgos de ciberamenazas y mejorando la confianza de la ciudadanía en la administración pública.

Política de Gobierno Digital (MINTIC): La Política de Gobierno Digital del MINTIC busca promover la transformación digital en el sector público, con el fin de mejorar la eficiencia de la gestión pública y el acceso de los ciudadanos a los servicios. Esta política establece principios y estrategias para la modernización de la administración pública, incluyendo la digitalización de la información, la mejora de la infraestructura tecnológica y la implementación de sistemas interoperables entre entidades. Para la Alcaldía de Tamalameque, esta política debe ser un referente al diseñar sus propias políticas de la información, orientadas a promover el acceso abierto a la información pública, la utilización de plataformas digitales para trámites y servicios, y el fortalecimiento de la infraestructura tecnológica para garantizar la eficiencia en el manejo de los datos institucionales.

(Ley 1341 de 2009, s.f.)– Ley TIC: regula las políticas públicas relacionadas con las tecnologías de la información y las comunicaciones en Colombia, promoviendo su uso para el desarrollo social y económico. Esta ley tiene un impacto directo en cómo las entidades públicas, incluida la Alcaldía de Tamalameque, deben gestionar la información mediante el uso de las TIC. Las políticas de seguridad de la información deben alinearse con los principios establecidos en la ley, promoviendo la apropiación de las TIC por parte de los ciudadanos y empleados

públicos, garantizando el acceso a la información y fomentando el uso eficiente de las tecnologías para mejorar la gestión pública y los servicios ofrecidos a la comunidad.

Normativa del (MINTIC, 2020) sobre Políticas de seguridad de la Información: El MINTIC establece normativas específicas para el manejo de la información dentro de las entidades públicas, en línea con los principios de transparencia, eficiencia y seguridad. A través de la Guía para la Gestión de la Información Pública y otros documentos, el MINTIC define lineamientos claros sobre cómo deben organizarse y protegerse los datos y documentos en las entidades del Estado. La Alcaldía de Tamalameque debe incorporar estos lineamientos al desarrollar sus políticas de seguridad de la información, lo que incluye la gestión eficiente de los archivos electrónicos, la digitalización de los procesos administrativos, y el establecimiento de protocolos claros para la conservación, acceso y disposición de la información pública.

Plan de trabajo (6 meses):

Tabla 1.

Plan de trabajo

Objetivos	Mes 1/semana				Mes 2/semana				Mes 3/semana				Mes 4/semana				Mes 5/semana				Mes 6/semana			
	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4
Realizar un diagnóstico del estado actual de la gestión de la información en la Alcaldía de Tamalameque, Cesar, para identificar fortalezas, debilidades y necesidades de mejora en relación con los lineamientos del MINTIC.																								
Diseñar las políticas de la información necesarias para la Alcaldía de Tamalameque, Cesar, que se ajusten a los lineamientos establecidos por el MINTIC y respondan a las necesidades identificadas en el diagnóstico.																								
Socializar las políticas de la información desarrolladas para la Alcaldía de Tamalameque, Cesar, asegurando que todas las partes interesadas comprendan y apoyen las políticas y el marco normativo propuestos.																								

Nota: Fuente Autor

Resultados

Cumplimiento del objetivo 1

Realizar un diagnóstico del estado actual de la gestión de la información en la Alcaldía de Tamalameque, Cesar, para identificar fortalezas, debilidades y necesidades de mejora en relación con los lineamientos del (MINTIC, 2020).

Para llevar a cabo la elaboración del objetivo específico, se realizó un diagnóstico detallado del estado actual de la gestión de la información en la Alcaldía de Tamalameque, Cesar. Este diagnóstico fue fundamental, ya que permitió obtener una visión clara sobre cómo se gestionan actualmente los procesos de información dentro de la Alcaldía. A través de este análisis, se identificaron las fortalezas, debilidades y necesidades de mejora en relación con los lineamientos establecidos por el Ministerio de Tecnologías de la Información y las Comunicaciones (MINTIC, 2020).

La fase inicial de diagnóstico y planeación se llevó a cabo durante el primer mes del proyecto y se dividió en varias actividades clave que contribuyeron a cumplir el objetivo principal de este primer objetivo específico. En las primeras semanas, se enfocó en la revisión de los documentos internos de la Alcaldía, específicamente en la recopilación y análisis de los documentos actuales de gestión de la información.

Se hizo una solicitud de documentos referentes a la Seguridad de la Información al departamento de Secretaría Administrativa y del Interior

Figura 1.

Solicitud de Documentos

Señores

Secretaría Administrativa y del Interior

Asunto: Solicitud de documentos referentes a la Seguridad de la Información

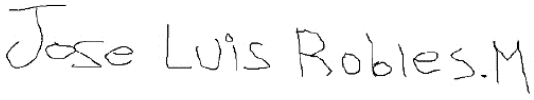
Estimados señores:

Por medio de la presente, me permito solicitarles de la manera más atenta que me proporcionen los documentos y políticas referentes a la Seguridad de la Información vigentes en su institución.

Como practicante universitario, Solicito acceder a esta información para poder llevar a cabo la elaboración de mi monografía. Los documentos que solicito incluyen, pero no se limitan a:

- Política de Seguridad de la Información
- Procedimientos y protocolos de seguridad de los sistemas de información
- Lineamientos para la clasificación y manejo de la información confidencial
- Plan de continuidad del negocio y recuperación ante desastres
- Cualquier otra documentación relevante al tema de seguridad informática y protección de datos

Agradeceré que puedan atender esta solicitud a la brevedad posible. Quedo a su disposición para cualquier aclaración o información adicional que requieran.



Atentamente,

José Luis Robles Machuca

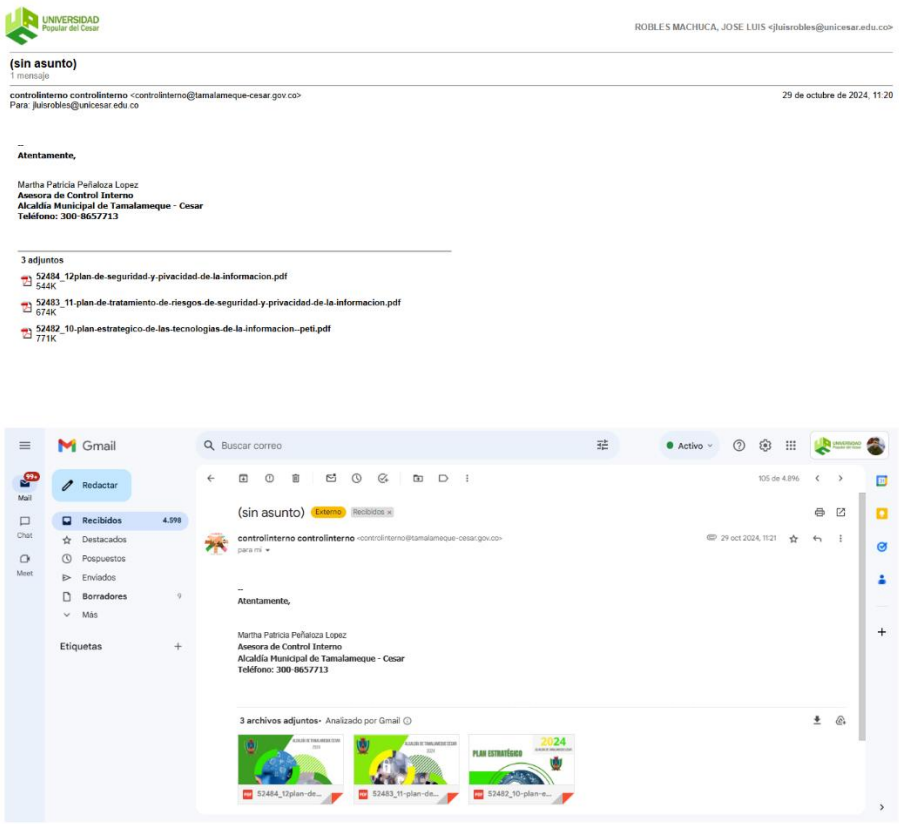
CC. 1003334592

Nota: Autoría propia

La solicitud fue atendida por el equipo de Control Interno de la Alcaldía Municipal de Tamalameque - Cesar, quienes enviaron una respuesta detallada vía correo electrónico. En esta comunicación, se adjuntaron tres documentos técnicos de gran relevancia: un plan de seguridad y privacidad de la información, un plan de tratamiento de riesgos asociados a la seguridad y privacidad de la información, y un plan estratégico para las tecnologías de la información. Estos documentos brindan un panorama completo de las medidas de seguridad y protección de datos implementadas por la entidad.

Figura 2.

Documentos técnicos



Nota: Autoría propia

Uno de los hallazgos más preocupantes fue la antigüedad de los documentos rectores. Por ejemplo, los manuales disponibles en el sitio web oficial de la Alcaldía (http://www.tamalameque-cesar.gov.co/) datan de 2017 y 2018, lo que significa que no incorporan las actualizaciones normativas ni las mejores prácticas en (Ciberseguridad, 2021) de los últimos años. Esta obsolescencia representa un riesgo jurídico y operativo, ya que las regulaciones en materia de protección de datos (como la (Ley 1581 de 2012, s.f.) y el (Decreto 1377 de 2013, s.f.) han evolucionado, exigiendo protocolos más rigurosos. Además, la falta de documentos digitalizados y accesibles dificulta su consulta y aplicación por parte de los funcionarios, generando inconsistencias en la implementación de las políticas.

Figura 3.

Sitio web oficial de la Alcaldía

Nota: Fuente (http://www.tamalameque-cesar.gov.co/)

Asimismo, la revisión de los documentos físicos asociados al Modelo Estándar de Control Interno (MECI) permitió identificar que, aunque existen políticas de seguridad digital, estas no han sido socializadas ni actualizadas en los últimos años. Esto ha generado que los funcionarios desconozcan los procedimientos establecidos o recurran a prácticas informales para el manejo de datos, aumentando la exposición a filtraciones, pérdida de información o ciberataques. La carencia de un marco normativo unificado y actualizado se convierte así en una barrera para la modernización de la gestión pública y en un obstáculo para garantizar la transparencia y rendición de cuentas.

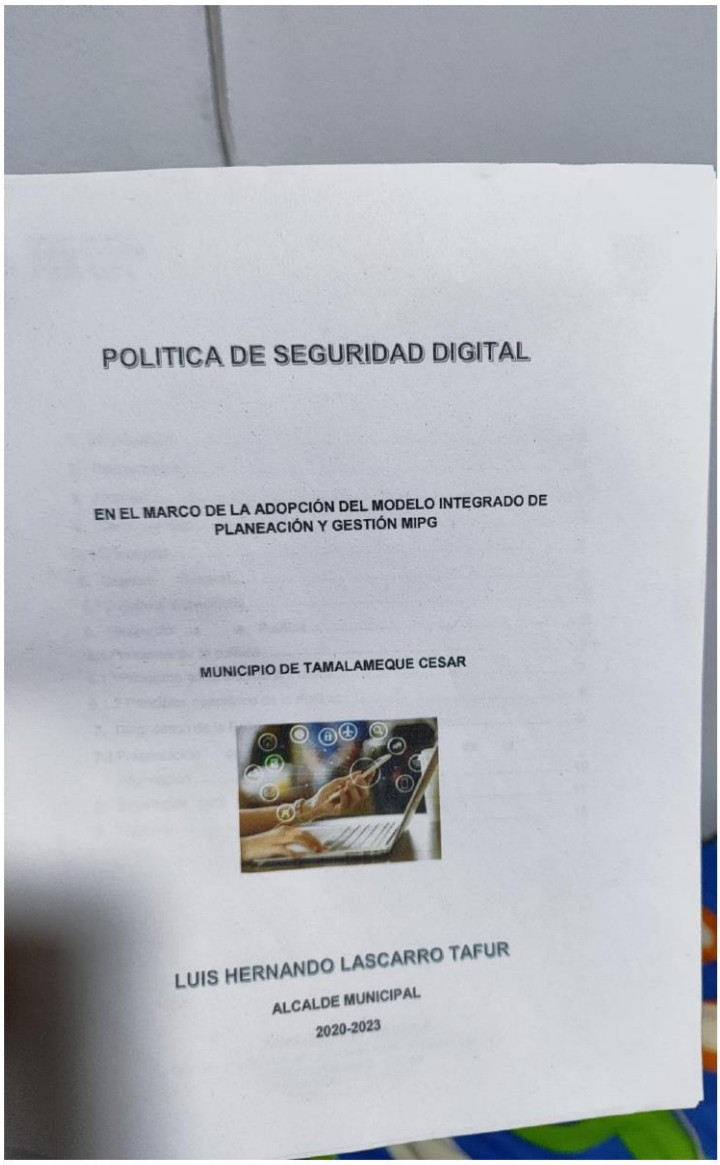
Figura 4.

Revisión de los documentos físicos

Nota: Encargada de los trámites de la seguridad de información y políticas de protección de datos

Figura 5.

Documentos de tratamiento de datos



Nota: Documentos en físico de tratamiento de datos

Tabla 2.

Clasificación de documentos

Tipo	Fecha de creación	Fecha de actualización	Descripción
Plan estratégico Tecnologías de la información y las comunicaciones	2024	2024	El presente documento tiene como finalidad llevar a cabo la actualización del PETI (Plan Estratégico de Tecnologías de la Información) de la Alcaldía Municipal de Tamalameque para la vigencia 2024. En este Plan Estratégico se presentarán un análisis extenso de las brechas, y la justificación de las necesidades identificadas
Plan de tratamiento de riesgos de seguridad y privacidad de la información	2024	2024	El siguiente "Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información" se rige como una herramienta integral para la identificación, evaluación y mitigación de los riesgos asociados con la información sensible y los datos personales gestionados por la Alcaldía Municipal de Tamalameque. Este plan se propone fortalecer la resiliencia de la entidad ante posibles amenazas, asegurando la integridad, confidencialidad y disponibilidad de la información
Plan de seguridad y privacidad de la información	2024	2024	El objetivo del Plan de Seguridad y Privacidad de la Información del Municipio de Tamalameque Cesar es garantizar la confidencialidad, integridad y disponibilidad de los datos e información manejados por la administración municipal. Se busca establecer mecanismos de protección eficaces contra posibles amenazas y vulnerabilidades, asegurando la privacidad de la información sensible de los ciudadanos. Este plan tiene como propósito principal fortalecer la infraestructura tecnológica y promover buenas prácticas en el manejo de la información, así como establecer protocolos de respuesta ante incidentes de seguridad
(MECI) Comunicación interna y externa	2017/08/24	2018/04/26	Gestionar la correspondencia entre dependencias y la enviada por la Alcaldía Municipal de Tamalameque al Municipio, Departamento o Nación (personas naturales y/o jurídicas), mediante el ingreso y registro de la información de los documentos por medio del libro radicador, o la base radicadora, con el fin de ejercer un control sobre ésta.
(MECI) Procedimientos de salud Procedimiento priorización base de datos de potenciales	2017/08/24	2018/04/26	Aplicar a la base de datos de potenciales beneficiarios (BDPB) los criterios de priorización definidos en las normas, para que las personas en situación de mayor pobreza y/o vulnerabilidad sean susceptibles de recibir los subsidios de salud, de acuerdo con la

Tipo	Fecha de creación	Fecha de actualización	Descripción
beneficiarios del régimen subsidiado en salud			disponibilidad de recursos del Sistema General de Seguridad Social en Salud
(MECI) Procedimientos gestión documental procedimientos para las comunicaciones recibidas por la administración central municipal	2017/08/24	2018/04/26	Gestionar toda la correspondencia recibida por la Alcaldía de Tamalameque, mediante el ingreso y registro de la información de los documentos en el libro radicador o un archivo magnético con el fin de ejercer un control y seguimiento.
Plan estratégico Tecnologías de la información (PETI)	2018/07/17	2019/11/20	Plan Estratégico de Tecnología de la Alcaldía Municipal de Tamalameque Cesar, surge con el propósito de lograr que las tecnologías de la información generen valor a la estrategia tanto de los sectores como de las entidades del sector público y que la gestión de la tecnología de la información sea coordinada y eficiente, tomando como base para ello el proceso de Gestión TIC. EL Plan se enmarca cumplimiento de los objetivos a nivel institucional, el cual debe ser en un alto estratégico, aportando valor y brindando tranquilidad a sus aliados en los procesos misionales estratégicos, de apoyo y evaluación.
Manual de normas y políticas de seguridad y privacidad de la información y protección de datos de la alcaldía municipal de Tamalameque cesar	10/10/2017	2018/12/26	La Alcaldía Municipal de Tamalameque Cesar, es consciente de la importancia de mantener la información en condiciones adecuadas de seguridad garantizando su integridad, confidencialidad y disponibilidad. La estrategia Gobierno en Línea del MINTIC incluye el eje de seguridad y privacidad de la información el cual es muy importante ya que funciona de manera transversal con los ejes de TIC para gobierno abierto, TIC para la gestión y TIC para servicios con el objetivo primordial de mantener en óptimos niveles de seguridad los datos manejados en el municipio a través de sus funcionarios y contratistas y los datos de trámites y servicios por parte de los ciudadanos.

Nota: Autoría propia

Inventario de equipos de la alcaldía entregado por la oficina de "Almacén y archivo".

Tras un exhaustivo proceso de búsqueda, recolección y clasificación de documentos relacionados con el tratamiento de datos personales y la seguridad de la información dentro de la Alcaldía de Tamalameque, Cesar, se evidenció la necesidad de complementar la información documental con un inventario actualizado de los recursos tecnológicos disponibles. Esta tarea es esencial, dado que la gestión eficiente de los activos informáticos constituye un pilar fundamental para garantizar la integridad, disponibilidad y confidencialidad de la información institucional (Bustamante García et al., 2021).

Se hizo una petición formal a la Oficina de Almacén y Archivo con el fin de conseguir un inventario detallado del hardware y software en uso, para poder tener una visión completa de la situación actual de los activos tecnológicos. Este registro posibilita no solo la identificación de la infraestructura tecnológica actual, sino también el análisis de los niveles de seguridad, la detección de vulnerabilidades y la creación de mecanismos de control más eficientes. La falta de control estricto sobre los activos tecnológicos, de acuerdo con (Cuesta, 2022), puede aumentar la posibilidad de que se pierdan datos, ocurran accesos no permitidos o haya ineficiencias en las operaciones. Esto es particularmente cierto en instituciones públicas, donde la trazabilidad de la información es obligatoria por ley.

Finalmente, los datos proporcionados por la oficina de Archivo y Almacén facilitarán que la Alcaldía de Tamalameque no solo evalúe la situación actual de sus recursos tecnológicos, sino que además establezca planes para acciones de mejora, renovación de equipos y robustecimiento de la seguridad digital. Esto resulta en una administración que es más moderna, transparente y que sigue las directrices del (MINTIC, 2020) (Ministerio de Tecnologías de la Información y las

Comunicaciones) dentro del modelo de Gobierno Digital y las políticas estatales colombianas sobre privacidad e seguridad de la información.

Figura 6.

Carta de información

ALCALDÍA MUNICIPAL DE TAMALAMEQUE CESAR
NIT 800.096.626-4
SECRETARÍA ADMINISTRATIVA Y DEL INTERIOR

Gobierno Municipal
TAMALAMEQUE
OFICINA DE ARCHIVO Y ALMACÉN

Tamalameque Cesar, 08 de mayo de 2025

Señor:
JOSE LUIS ROBLES MACHUCA
Practicante
Alcaldía Municipio de Tamalameque

Ref.: Envió información inventario de hardware y software para fines educativos.

En mi calidad de Técnico Administrativo de Archivo y Almacén de la Alcaldía Municipal de Tamalameque del Cesar, envío información solicitada de hardware y software con los que cuenta la entidad.

Es de anotar que la información suministrada por esta dependencia, solo podrá ser utilizada para fines educativos.

Atentamente,

JOSE LUIS PERALES VEGA
Técnico Administrativo Archivo y Almacén.
Alcaldía de Tamalameque

Palacio Municipal
Calle 3 # 3-14, Plaza Principal
Tamalameque Cesar
alcaldia@tamalameque-cesar.gov.co

Nota: Respuesta entregada por la oficina de almacén y archivo

Figura 7.

Inventario hardware

ALCALDÍA MUNICIPAL DE TAMALAMEQUE CESAR
NIT 800.096.626-4

Gobierno Municipal
TAMALAMEQUE

SECRETARIA ADMINISTRATIVA Y DEL INTERIOR / ARCHIVO Y ALMACEN

INVENTARIO HARDWARE

DESPACHO U OFICINA: ALCALDIA MUNICIPAL DE TAMALAMEQUE
FECHA DE INVENTARIO: 31/12/2024

CANTIDAD	DETALLE	COD. DEL DETALLE INVENTARIADO	ESTADO Y OBSERVACIONES
1	computador hp	0035	ACTIVO
1	Impresora Epson L5190	0021	ACTIVO
1	Monitor pc (COMPAQ)	0008	ACTIVO
1	CPU (133CR117026UB)	0007	ACTIVO
1	Impresora laser HP 137fmw	0058	ACTIVO
1	Impresora Epson L3250	0059	ACTIVO
1	computador Samsung	0062	ACTIVO
1	CPU(compumax)	0063	ACTIVO
1	impresora Epson L3110	0072	ACTIVO
1	computador samsung(ZUGTH9LBC05458W)	0009	ACTIVO
1	CPU	0010	ACTIVO
1	impresora epson l5190	0016	ACTIVO
1	computador hp (completo)	0074	ACTIVO
1	Impresora Epson L3210	0090	ACTIVO
1	Aire acondicionado panasonic de 24000 BTU	0162	ACTIVO
1	impresora epson L380	0163	ACTIVO
1	computador lennovo (6500778B109	0193	ACTIVO
1	Impresora Epson L5190	0196	ACTIVO
1	Computador portatil acer	0199	ACTIVO
1	Proyector (videobeni) Epson EMP-S4	0200	ACTIVO
1	computador LG(serial 303)	0.091	ACTIVO
1	computador lenovo(pf0kv7224LL03(	0.089	ACTIVO
1	impresora epson	0.395	ACTIVO
1	computador hp (SNKB501145002)	0133	ACTIVO
1	CPU	0134	ACTIVO
6	dispositivos movil de capturas y sus accesorios	0140-0145	ACTIVO
1	Impresora Epson L3250	0146	ACTIVO
1	plotter hp designjet T120	0181	ACTIVO
1	Impresora Epson L3250	0109	ACTIVO
1	computador portatil ASUS SN: N1NOCXO7B84101F	0154	ACTIVO
1	escaner marca canon R40	0157	ACTIVO
1	computador HP todo en uno (completo)	0112	ACTIVO
1	impresora epson L5190	0117	ACTIVO
1	computador hp blanco (completo)	0123	ACTIVO
1	impresora Hp laser MFP 137	0125	ACTIVO
1	Computador janus (completo)	0126	ACTIVO
1	Computador Negro HP (completo)	0128	ACTIVO
1	Computador Marca Lenovo (completo)	0093	ACTIVO
1	Impresora Marca Epson L5190	0095	ACTIVO
1	Escaner Canon R40	0098	ACTIVO

JOSE LUIS PERALES VEGA
Técnico Administrativo de Archivo y Almacén
Alcaldía Municipal de Tamalameque del Cesar

Nota: Respuesta entregada por la oficina de almacén y archivo

Tabla 3.

Inventario hardware

Cantidad	Detalle	Cod. Del detalle inventariado	Estado y observaciones
1	computador hp	0001	ACTIVO
1	impresora Epson L5190	0021	ACTIVO
1	Monitor hp (COMPAQ)	0008	ACTIVO
1	CPU (13)K,110(110)USB	0007	ACTIVO
1	Impresora láser hp m100a	0004	ACTIVO
1	Impresora Epson L3150	0059	ACTIVO
1	computador Samsung	0062	ACTIVO
1	CPU computador	0063	ACTIVO
1	Impresora Epson L3110	0064	ACTIVO
1	computador ASUS (I3,4G,1TVB,BC054SF)W	0009	ACTIVO
1	CPU	0010	ACTIVO
1	impresora epson l5190	0096	ACTIVO
1	impresora epson l3110	0091	ACTIVO
1	impresora Epson L3110	0090	ACTIVO
1	Aire acondicionado Panasonic de 24000 BTU	0082	ACTIVO
1	impresora epson L380	0083	ACTIVO
1	computador lenovo E/007786329	0100	ACTIVO
1	impresora Epson L5190	0099	ACTIVO
1	Computador portátil acer	0200	ACTIVO
1	Proyector (video Ben) Epson EMP S4	0200	ACTIVO
1	computador hp (escritorio)	0092	ACTIVO
1	computador Lenovo(I7,8g,1T,224)UJK	0089	ACTIVO
1	impresora Epson	0095	ACTIVO
1	Computador HP (SNX001145002)	0181	ACTIVO
1	CPU	0192	ACTIVO
8	Objetivos móvil de capturas y sus accesorios	0540-0545	ACTIVO
1	Impresora Epson L3250	0546	ACTIVO
1	plotter hp designjet T120	0181	ACTIVO
1	Impresora Epson L3250	0182	ACTIVO

Cantidad	Detalle	Cod. Del detalle inventariado	Estado y observaciones
1	computador portátil ASUS SN: NSID90CHO78430JJF	0154	ACTIVO
1	escáner marca canon R40	0157	ACTIVO
1	computador HP todo en uno (completo)	0114	ACTIVO
1	Impresora Epson L3250	0122	ACTIVO
1	Computador HP blanco (completo)	0123	ACTIVO
1	Impresora HP laser Mfp 137	0125	ACTIVO
1	Computador Dell (completo)	0128	ACTIVO
1	computador lenovo (completo)	0128	ACTIVO
1	Computador Marca Lenovo (completo)	0093	ACTIVO
1	Impresora Marca Epson L5330	0095	ACTIVO
1	Escáner Canon R40	0096	ACTIVO

Nota: Autoría propia

Tabla 4.

Plataformas Utilizadas por empleados de la alcaldía

ID	Detalle	Usuario	Cargo
0001	Siaobserva	Dairo Daza González	Apoyo plataformas institucionales
0002	Síacontraloría	Dairo Daza González	Apoyo plataformas institucionales
0003	Sigepii	Dairo Daza González	Apoyo plataformas institucionales
0004	Sireci	Dairo Daza González	Apoyo plataformas institucionales
0005	SGR	Carlos Torres Covilla	Secretario/a de Planeación
0006	Hotmail	Carlos Alberto Romero Gaona	Umata
0007	Gmail	Carlos Alberto Romero Gaona	Umata
0008	SIMÓ 4.0 - EDL	María Fernanda Molina Valle	Secretario/a de Gobierno
0009	Furag	Martha Patricia Peñaloza López	Asesor/a Jurídico/a
0010	Secop 1	Dixie Luz Pino Chávez	Asesor/a Jurídico/a
0011	Plataforma Renta Joven	Juana Mishell Robles Avila	Enlace renta joven
0012	CGN Saldos y Movimientos y Deudores Moroso	Gleiner Lobo	Contador/a

ID	Detalle	Usuario	Cargo
0013	SISPRO	Mayecsi Andrea Maestre Lobo	Profesional especializado salud pública
0014	Hércules	Ernesto José Estrada Mejía	Coordinador de deportes
0015	MGA y PIIP	Jonathan Torres Hernández	Banco de Proyectos
0016	Software Universo on line	Lebis Meza B	Líder de Presupuesto
0017	SIMIT	Yenis Paola Paniza Atencio	Coordinador renta ciudadana
0018	RIT	Yenis Paola Paniza Atencio	Coordinador renta ciudadana
0019	Devolución del IVA	Yenis Paola Paniza Atencio	Coordinador renta ciudadana
0020	SIFA IV	Yenis Paola Paniza Atencio	Coordinador renta ciudadana
0021	Ministerio de Hacienda	Joel Alberto Guerra	Secretario/a de Hacienda
0022	Plataforma de la Registraduría para elecciones de Consejos de Juventud	Juan José Villarreal Tovar	Registraduria para elecciones de consejos de Juventud
0023	Sistema CETIL	Ketty Luz Guerra	Apoyo profesional depuración pasivos pensionales
0024	Sistema Bonos Pensionales	Ketty Luz Guerra	Apoyo profesional depuración pasivos pensionales
0025	Pasivocol	Ketty Luz Guerra	Apoyo profesional depuración pasivos pensionales
0026	SAC	Yalimar Castro Muñoz	Auxiliar de Salud
0027	Sivigila	Luz Dany Ramirez Hernandez	Coord VSP
0028	Correo Institucional	Luz Mary Vanegas Jiménez	Ventanilla Unica
0029	PAIWEB	Zulay Liévano Valle	Apoyo PAI

Nota: Autoría propia

Cumplimiento del objetivo 2

Diseñar las políticas de seguridad de la información necesarias para la Alcaldía de Tamalameque, Cesar, que se ajusten a los lineamientos establecidos por el MINTIC y respondan a las necesidades identificadas en el diagnóstico

Diagnóstico de seguridad de los documentos obtenidos

Este diagnóstico tiene como objetivo analizar el estado actual de la seguridad de la información en la Alcaldía de Tamalameque, Cesar, con base en la documentación institucional recopilada y los lineamientos del (MINTIC, 2020). El propósito es identificar fortalezas, debilidades y riesgos que permitan diseñar políticas efectivas y alineadas con la normativa vigente.

Marco de Referencia

Normatividad y lineamientos considerados para el análisis:

- (Ley 1581 de 2012, s.f.): Protección de datos personales.
- (Ley 1712, 2014) Acceso a la información pública.
- Política de Gobierno Digital – (MINTIC, 2020)
- Modelo de Seguridad y Privacidad de la Información (MSPI).
- Norma ISO/IEC 27001 (referencia internacional).
- Finalidad: construir un marco regulador que asegure la confidencialidad, integridad, disponibilidad y trazabilidad de la información institucional.

Análisis Documental

A continuación, se presenta el análisis de los documentos revisados:

Tabla 5.

Análisis de documentos revisados

Documento	Año	Contenido clave	Observaciones
Plan estratégico tecnología de la información y telecomunicaciones	2024	El Plan Estratégico de Tecnologías de la Información (PETI) de la Alcaldía Municipal de Tamalameque 2024 presenta un diagnóstico detallado del estado actual de las TIC en la entidad, incluyendo una matriz DOFA, necesidades institucionales y una hoja de ruta clara. Se identifican aspectos clave como la necesidad de fortalecer la conectividad, la gestión documental, la seguridad de la información y la transformación digital. Además, el plan incorpora un marco normativo completo que incluye las leyes 1581 de 2012 (protección de datos personales) y 1712 de 2014 (acceso a la información pública), así como múltiples decretos y políticas nacionales relacionadas con gobierno digital y seguridad de la información.	A pesar de la amplitud normativa considerada, se identifican vacíos en la implementación práctica de las leyes mencionadas. En cuanto a la Ley 1581, no se evidencia un Manual de Políticas de Tratamiento de Datos Personales, ni la designación de un responsable de protección de datos. Por su parte, respecto a la Ley 1712, no se desarrollan mecanismos claros de clasificación de la información, ni procedimientos de respuesta a derechos de petición por medios electrónicos. También se observa la falta de políticas consolidadas en seguridad digital, uso y apropiación de TIC, e interoperabilidad de sistemas.
Plan de tratamiento de riesgos de seguridad y privacidad de la información	2024	Establece un marco integral para gestionar los riesgos asociados a la seguridad y privacidad de la información, alineado con normas como la Ley 1581 de 2012, Ley 1712 de 2014 e ISO/IEC 27001:2013. Incluye fases del ciclo PHVA (Planear, Hacer, Verificar, Actuar), definición de responsables, cronograma semestral de actividades y un enfoque metodológico basado en lineamientos del MinTIC. El plan abarca todos los activos y procesos informacionales de la entidad, con énfasis en identificación de riesgos, elaboración de mapas de calor, capacitación a funcionarios y seguimiento técnico. El objetivo general es preservar la confidencialidad, integridad y disponibilidad de los datos, así como garantizar el cumplimiento normativo y generar confianza en la ciudadanía.	**Fortalezas**: El plan tiene una estructura robusta, un enfoque metodológico claro, y contempla todos los niveles de la entidad. Se evidencia el compromiso con la protección de datos personales, transparencia y ciberseguridad. **Limitaciones:** • Aunque se menciona la Ley 1581, no se evidencia un procedimiento específico de atención a titulares ni mecanismos de autorización y consentimiento explícito. • No se incluye un inventario de bases de datos personales ni su registro ante la SIC, como lo exige el Decreto 1377 de 2013. • Falta detallar cómo se garantiza el acceso ciudadano a la información (Ley 1712) y qué medidas específicas se implementan para garantizar la transparencia activa. • La cultura organizacional y el cambio de comportamiento frente a la seguridad digital se

Documento	Año	Contenido clave	Observaciones
			menciona, pero sin indicadores de impacto o resultados medibles. • No se hace alusión a auditorías internas ni externas como mecanismo de verificación independiente.
Plan de seguridad y privacidad de la información	2024	Este plan tiene como propósito garantizar la confidencialidad, integridad y disponibilidad de la información administrada por la Alcaldía de Tamalameque. Está enmarcado en un Sistema de Gestión de Seguridad de la Información (SGSI) conforme a la norma ISO/IEC 27001 y las directrices del Modelo Integrado de Planeación y Gestión (MIPG). Cubre desde la gestión de riesgos hasta la implementación de controles, la vigilancia de software, la capacitación al personal y el cumplimiento normativo. El marco legal referenciado incluye la Ley 1581 de 2012 (protección de datos personales) y la Ley 1712 de 2014 (acceso a la información pública), así como su respectiva reglamentación. Se establece una política de seguridad institucional obligatoria para todos los funcionarios, acompañada de un cronograma anual de actividades de monitoreo, evaluación y cultura de seguridad.	**Aspectos positivos:** • El plan incorpora principios fundamentales de un SGSI bajo estándares internacionales y leyes colombianas clave. • Se articula con un comité institucional responsable de la seguridad de la información y contempla medidas para sensibilización, vigilancia y mejora continua. • Se establece una política explícita de seguridad de la información con compromisos claros sobre confidencialidad, integridad, disponibilidad y cumplimiento legal. **Aspectos críticos o mejorables:** • No se evidencia el procedimiento detallado para la atención de solicitudes de los titulares de datos personales, como exige el artículo 8 de la Ley 1581. • Falta incluir un registro formal de bases de datos personales o su inscripción ante la SIC, lo cual es obligatorio según el Decreto 1377 de 2013. • En cuanto a la Ley 1712, no se especifica cómo se garantiza el acceso a la información pública más allá del cumplimiento genérico. • No se desarrollan indicadores de desempeño para medir la eficacia de la política de seguridad ni los impactos del plan. • La responsabilidad de cumplimiento parece generalizada a “todas las secretarías”, sin roles diferenciados o responsables designados con funciones específicas.
Modelo estándar de control interno MECI.	2017	Establecer los lineamientos para la gestión de la comunicación institucional, tanto interna como	**Puntos positivos:**

Documento	Año	Contenido clave	Observaciones
(Comunicación interna y externa)		externa, en la Alcaldía de Tamalameque. Aunque la información es limitada se reconoce la intención de estructurar y formalizar los procesos de comunicación como parte integral del funcionamiento organizacional y del cumplimiento del PETI y otros planes estratégicos. Este documento busca garantizar la transparencia, mejorar la interacción con la ciudadanía y fortalecer la coordinación entre áreas.	• Se vislumbra la intención de profesionalizar la comunicación institucional. • En el contexto del PETI, este documento cumple una función complementaria importante para socializar avances, políticas y actividades de transformación digital. **Aspectos por mejorar:** • El documento no desarrolla contenidos concretos como objetivos específicos, medios de comunicación, tipos de mensajes, flujos de información o canales oficiales. • No hay mención de protocolos de comunicación en situaciones críticas o de seguridad (lo cual es clave para el componente de privacidad de la información). • Falta vinculación explícita con la Ley 1581 de 2012 (protección de datos personales) y Ley 1712 de 2014 (acceso a la información pública). • No se identifican roles ni responsables institucionales de la comunicación, ni se contemplan estrategias de capacitación o evaluación de impacto.
Manual de normas y políticas de seguridad y privacidad de la información y protección de datos de la alcaldía municipal de Tamalameque Cesar	2017	Establece un marco normativo y operativo para la gestión de la seguridad y privacidad de la información en la Alcaldía de Tamalameque. Su objetivo es preservar la integridad, confidencialidad y disponibilidad de los activos informáticos institucionales. Define conceptos fundamentales como datos personales, datos sensibles, amenazas, vulnerabilidades y riesgos, y describe recursos como antivirus, firewalls y prácticas organizativas. El manual incluye definiciones detalladas, responsabilidades de los funcionarios y contratistas, y establece la importancia del factor humano en la seguridad informacional. Se enfoca en concientizar al personal sobre el manejo responsable de la	El manual está alineado con la Ley 1581 de 2012, abordando adecuadamente los principios de tratamiento de datos personales, incluyendo la distinción entre datos públicos, sensibles y privados. Reconoce la existencia de políticas institucionales de privacidad y garantiza los derechos de los titulares. También articula el derecho de acceso a la información pública conforme a la Ley 1712 de 2014, aunque de forma general. Se evidencia correspondencia con la Política de Gobierno Digital del MinTIC, al enmarcarse en el eje transversal de seguridad y privacidad. El documento adopta términos y conceptos de la norma ISO/IEC 27001, incluyendo la gestión de riesgos, amenazas y controles, aunque sin declarar explícitamente una conformidad con dicha norma ni proponer auditorías

Documento	Año	Contenido clave	Observaciones
		información y promueve buenas prácticas alineadas con el MSPI (Modelo de Seguridad y Privacidad de la Información).	internas que verifiquen su cumplimiento.
Plan estratégico de tecnologías de la información PETI	2018	Está orientado a que la gestión de las TIC aporte valor a los objetivos institucionales y facilite una administración pública más eficiente, coordinada y estratégica. El plan se basa en el proceso de Gestión TIC y busca articular las tecnologías de la información con los procesos misionales, de apoyo y evaluación, asegurando alineación con la estrategia general del municipio. Se enfoca en lograr que las TIC no solo apoyen la operación, sino que también impulsen la transformación digital, mejoren la toma de decisiones, fortalezcan la gobernanza y promuevan una cultura institucional innovadora.	Aunque el PETI tiene una intención estratégica clara y reconoce el rol transversal de las TIC, no se evidencia una mención explícita a elementos clave como la protección de datos personales (Ley 1581 de 2012) ni al acceso a la información pública (Ley 1712 de 2014). De igual forma, el plan se alinea conceptualmente con la Política de Gobierno Digital del MinTIC, al priorizar la eficiencia y la articulación institucional, pero sería recomendable reforzar su integración mediante indicadores de interoperabilidad, servicios ciudadanos digitales y gobernanza de la información. En cuanto a la ISO/IEC 27001, no se indica si el PETI incorpora procesos de gestión de la seguridad de la información, lo cual es fundamental si se busca generar confianza y sostenibilidad en los sistemas tecnológicos.
Modelo estándar de control interno MECI. (Procedimiento priorización base de datos de potenciales beneficiarios del régimen subsidiado en salud)	2017	Este procedimiento tiene como objetivo establecer los lineamientos para la priorización de personas en la base de datos del régimen subsidiado en salud, de acuerdo con los criterios definidos por el Gobierno Nacional y las entidades territoriales. El documento aborda aspectos clave como el manejo de información sensible, criterios de inclusión, jerarquización de beneficiarios y el uso de herramientas técnicas para garantizar equidad en el acceso. Aunque el contenido completo no es legible por la calidad del escaneo, el propósito es técnico, administrativo y legal, enmarcado en procesos de atención a población vulnerable.	**Fortalezas:** • La naturaleza del documento implica el manejo de datos personales sensibles, lo que lo hace directamente relacionado con la Ley 1581 de 2012 (protección de datos personales). • Promueve una metodología estandarizada para garantizar la equidad en el acceso al sistema de salud, lo cual está alineado con los principios constitucionales y de política pública. **Debilidades y vacíos:** • No se observa una mención expresa a la Ley 1581 de 2012 ni a mecanismos de autorización, consentimiento o atención de derechos de los titulares de datos. • No se evidencia una ruta de tratamiento de datos ni designación de un responsable de protección de datos, pese al uso de información sensible. • No se hace alusión a la Ley 1712 de 2014 (transparencia y acceso a

Documento	Año	Contenido clave	Observaciones
			la información), pese a que se trata de una base pública de datos. • No incluye medidas claras de seguridad de la información, ni protocolos en caso de incidentes, errores o fugas. • Tampoco se evidencian procedimientos para revisión, actualización o eliminación de datos personales, derechos clave bajo el habeas data.
Modelo estándar de control interno MECI. (Procedimiento de gestión documental)	2017	El documento tiene como propósito establecer los lineamientos para la correcta administración, organización, conservación y disposición final de los documentos institucionales de la Alcaldía de Tamalameque. Se enfoca en regular las fases del ciclo de vida documental (producción, recepción, distribución, uso, organización, consulta, conservación y eliminación). Estos procedimientos son fundamentales para garantizar la trazabilidad de la información pública y privada, facilitar el acceso oportuno a los datos y cumplir con principios de eficiencia administrativa, transparencia y protección de la información.	**Fortalezas:** • El enfoque está alineado con políticas de gobierno digital y gestión archivística. • Establece una base necesaria para soportar otros sistemas como el SGSI (Sistema de Gestión de Seguridad de la Información) y el cumplimiento de la Ley 1712 de 2014 (transparencia). • Permite el control y preservación de la memoria institucional y garantiza la recuperación documental ante auditorías o litigios. **Aspectos críticos:** • El procedimiento no hace una mención explícita a la Ley 1581 de 2012, pese a que muchas de las series documentales podrían contener datos personales o sensibles. • No se observa un protocolo para el manejo de documentos confidenciales o reservados, ni medidas para restringir el acceso a terceros no autorizados. • Falta vinculación con el concepto de acceso diferenciado a la información (pública, clasificada y reservada), exigido por la Ley 1712. • No se evidencia la existencia de responsables documentales formales, ni un sistema claro de roles, autorizaciones o trazabilidad de accesos. • No se desarrollan mecanismos de digitalización segura, ni medidas específicas para la protección de archivos digitales y físicos contra

Documento	Año	Contenido clave	Observaciones
			pérdida, manipulación o divulgación no autorizada.

Nota: Autoría propia

Identificación de Brechas o Riesgos

Tabla 6.

Comparación entre la situación actual y las exigencias normativas

Tema	Situación actual	Exigencia normativa	Brecha identificada
Control de accesos a sistemas	No se evidencian políticas formales ni autenticación individual en los planes	ISO 27001 y MSPI: autenticación segura, control de accesos individual	Riesgo de acceso no autorizado a información sensible
Tratamiento de datos personales	No hay políticas específicas ni procedimiento de atención a titulares	Ley 1581: autorización, derechos del titular, atención de consultas y reclamos	Incumplimiento de derechos de habeas data
Clasificación de la información	No se segmenta la información por niveles de acceso o sensibilidad	Ley 1712: obligación de clasificar información como pública, reservada o confidencial	Posibilidad de divulgación indebida
Capacitación del personal	No hay programas estructurados o frecuentes de sensibilización	MinTIC, ISO 27001: capacitación periódica en seguridad y protección de datos	Bajo nivel de conciencia en seguridad y privacidad
Transparencia activa	No se detalla cómo se garantiza el acceso ciudadano a la información	Ley 1712: publicación de datos en portales oficiales, atención a solicitudes	Riesgo de incumplimiento de principios de transparencia
Responsables de seguridad y datos	No se identifican roles formales en ninguno de los documentos	Ley 1581 y ISO 27001: deben existir responsables definidos (DPO, Comité de Seguridad, etc.)	Ausencia de responsables institucionales formales
Respaldo y continuidad de información	Solo se mencionan respaldos generales, no se especifica frecuencia ni ubicación	ISO 27001: respaldos regulares, externos, con verificación y plan de recuperación	Riesgo de pérdida total o parcial de datos
Gestión documental	No se incluyen controles específicos para documentos con datos personales	Ley 1581 y Archivo General: medidas especiales para protección y acceso restringido	Riesgo de exposición de información personal
Auditorías y seguimiento	No se incluyen procesos de auditoría interna ni evaluación de cumplimiento	ISO 27001 y MIPG: auditorías internas periódicas para evaluar eficacia del SGSI	Falta de mecanismos de control y mejora continua
Digitalización segura	No se contemplan medidas de seguridad en escaneo,	Ley 1581 y MinTIC: almacenamiento	Riesgo de fuga de información en soportes digitales

Tema	Situación actual	Exigencia normativa	Brecha identificada
	almacenamiento o eliminación	seguro, cifrado, destrucción controlada	
Interacción con ciudadanos	No se establecen canales oficiales ni protocolos de respuesta de información pública	Ley 1712: tiempos de respuesta, canales accesibles, trazabilidad de solicitudes	Riesgo de vulnerar derecho a acceso a la información
Base de datos del régimen subsidiado	No se menciona registro ante la SIC ni controles de seguridad sobre datos sensibles	Decreto 1377/2013 y Ley 1581: registro obligatorio, medidas de seguridad reforzadas	Exposición de información sensible sin controles formales

Nota: Autoría propia

Conclusiones y Recomendaciones

Con base en el análisis anterior, se concluye que:

Plan estratégico tecnología de la información y telecomunicaciones

El plan estratégico tecnología de la información y telecomunicaciones es una herramienta estratégica ambiciosa y bien estructurada que busca transformar digitalmente la gestión pública local mediante un enfoque planificado y participativo. Su contenido refleja compromiso institucional con la modernización y la transparencia, aunque existen brechas importantes en cuanto a la aplicación práctica de normas técnicas internacionales y mecanismos de aseguramiento de la calidad. La articulación entre diagnóstico, necesidades y soluciones es clara, pero el éxito del plan dependerá de la voluntad política, la asignación adecuada de recursos y la formación continua del personal. Es crucial que la ejecución esté acompañada de seguimiento riguroso, integración interinstitucional y una cultura organizacional que valore el cambio digital. Se recomienda:

- Incorporar formalmente el estándar ISO/IEC 27001 como marco guía para gestionar la seguridad de la información, desarrollando un Sistema de Gestión de Seguridad de la Información (SGSI) documentado y auditable.

- Diseñar protocolos específicos para garantizar el cumplimiento efectivo de la (Ley 1581 de 2012, s.f.) y la (Ley 1712, 2014) , incluyendo indicadores de acceso, protección y uso responsable de datos personales y públicos.
- Establecer un catálogo de servicios digitales interoperables, con criterios de calidad, accesibilidad y usabilidad, conforme a la NTC 5854 y los lineamientos del (MINTIC, 2020)
- Aumentar la inversión en formación técnica y cultural del personal y la ciudadanía, en áreas como gestión de servicios TI, analítica de datos y apropiación de las TIC.
- Fortalecer la evaluación del PETI con auditorías internas y externas, incorporando revisiones periódicas que garanticen su adaptación a nuevas tecnologías y necesidades emergentes.

Plan de tratamiento de riesgos de seguridad y privacidad de la información

Este plan representa un representa una herramienta operativa y estratégica robusta que refuerza la cultura institucional de seguridad de la información en la administración pública local. Sus fundamentos normativos y metodológicos lo convierten en un instrumento confiable para la gestión preventiva de riesgos digitales. La claridad en las fases de implementación, los recursos asignados, la participación transversal de las áreas y el compromiso con el seguimiento sistemático permiten prever un impacto positivo en la protección de los datos personales y en la resiliencia organizacional. Sin embargo, su efectividad dependerá de la rigurosidad en su ejecución y la actualización constante frente a nuevas amenazas. Se recomienda:

- Integrar un procedimiento formal de atención de solicitudes de titulares de datos, conforme al Artículo 8 de la (Ley 1581 de 2012, s.f.)
- Incluir el registro y clasificación de bases de datos personales y la correspondiente inscripción ante la Superintendencia de Industria y Comercio.

- Formalizar la política de gestión de riesgos como documento institucional de obligatorio cumplimiento, alineado con las directrices nacionales del (MINTIC, 2020) y el Modelo Integrado de Planeación y Gestión (MIPG).
- Desarrollar un plan específico de cumplimiento de la (Ley 1712, 2014), que contemple acciones de transparencia proactiva, canales de acceso a la información pública y publicación de datos abiertos.
- Fortalecer la formación del personal mediante programas continuos de capacitación en ciberseguridad, privacidad de datos y gestión de incidentes, priorizando a quienes manejan información sensible.
- Implementar auditorías de cumplimiento de seguridad de la información, tanto internas como externas, y garantizar la trazabilidad de los controles aplicados.

Plan de seguridad y privacidad de la información

El plan constituye un esfuerzo sólido y estructurado por institucionalizar la gestión de la seguridad de la información en la administración pública local. Articula adecuadamente normativas legales y técnicas, promueve la cultura de seguridad y propone acciones calendarizadas para su implementación. Sin embargo, su impacto podría verse limitado si no se acompaña de mecanismos de auditoría, medición de resultados e interoperabilidad con otras entidades del Estado. La ausencia de un compromiso formal con estándares internacionales como la ISO/IEC 27001, más allá de su mención, representa una oportunidad de mejora en términos de madurez organizacional y gobernanza digital. Se recomienda:

- Adoptar formalmente la norma ISO/IEC 27001, estableciendo como meta la implementación plena de su sistema de gestión y la eventual certificación.

- Fortalecer los mecanismos de monitoreo y auditoría sobre el cumplimiento de la (Ley 1712, 2014), garantizando el acceso real y eficaz a la información pública.
- Desarrollar indicadores de gestión y seguridad para medir el impacto del plan y facilitar la toma de decisiones basada en datos.
- Ampliar las acciones de formación y sensibilización en seguridad digital, enfocadas especialmente en funcionarios con acceso privilegiado a la información.
- Actualizar periódicamente el plan y su cronograma conforme a los avances tecnológicos, amenazas emergentes y cambios regulatorios.

Manual de normas y políticas de seguridad y privacidad de la información y protección de datos de la alcaldía municipal de Tamalameque Cesar

El manual es un instrumento normativo clave para institucionalizar la seguridad digital en el municipio. Su estructura y contenido evidencian una comprensión adecuada de los riesgos informáticos y la necesidad de establecer lineamientos claros para el manejo seguro de la información. También contribuye a la cultura organizacional en seguridad y privacidad, con énfasis en la capacitación y concienciación del personal. Sin embargo, su alcance práctico puede mejorarse mediante la implementación de mecanismos de evaluación y seguimiento continuo, así como con la formalización de políticas bajo estándares internacionales. Se recomienda:

- Desarrollar e implementar una política de auditoría interna para verificar el cumplimiento del manual y su alineación con los estándares de la norma ISO/IEC 27001.
- Formalizar procesos de actualización periódica del manual, especialmente en respuesta a nuevas amenazas tecnológicas o cambios en la legislación.
- Diseñar rutas de atención y gestión de incidentes de seguridad, que incluyan canales de reporte, trazabilidad y tiempos de respuesta establecidos.

- Fortalecer la formación continua del personal en temas de ciberseguridad, manejo ético de datos personales y uso responsable de tecnologías de la información.
- Complementar este manual con políticas específicas sobre protección de datos personales, gestión documental digital y seguridad física de los activos tecnológicos.

Plan estratégico de tecnologías de la información (PETI)

Es una herramienta útil para consolidar el papel de las TIC como eje estratégico del desarrollo municipal. Contribuye a orientar la inversión tecnológica, coordinar las iniciativas digitales y asegurar que los recursos tecnológicos respalden de forma efectiva las metas institucionales. Sin embargo, la ausencia de componentes específicos en torno a seguridad, privacidad, normatividad y gestión de riesgos puede limitar su impacto si no se complementa con políticas y planes técnicos específicos. Para ser completamente funcional, debe integrarse con otros instrumentos como el Plan de Seguridad Informática, los lineamientos del MSPI y las normas ISO. Se recomienda.

- Incorporar explícitamente referencias normativas a la (Ley 1581 de 2012, s.f.) y (Ley 1712, 2014), con medidas para garantizar la protección de datos personales y la transparencia en el acceso a la información.
- Alinear el PETI con el Modelo de Seguridad y Privacidad de la Información (MSPI) y la norma ISO/IEC 27001, incluyendo aspectos de riesgo, controles, incidentes y mejora continua.
- Establecer métricas de impacto TIC, no solo en términos operativos, sino también en cómo estas tecnologías contribuyen al valor público, la eficiencia y la participación ciudadana.
- Fortalecer los mecanismos de seguimiento mediante auditorías, reportes de cumplimiento y revisión continua del plan, asegurando su actualización anual.

- Conectar el PETI con otras estrategias institucionales, como el Plan de Desarrollo Municipal, el Plan Anticorrupción y el de Servicio al Ciudadano, para garantizar una visión integral del ecosistema digital del municipio.

Modelo estándar de control interno MECI. (Comunicación interna y externa)

Cumple una función descriptiva útil en cuanto a la identificación de actores y canales de comunicación, pero presenta vacíos significativos en la integración de marcos normativos y técnicos fundamentales. La falta de mención específica de normas y estándares limita su aplicabilidad como política institucional o directriz formal. Para que el sistema de comunicación aporte a la gobernanza, la transparencia y la seguridad informacional, es necesario que se articule de manera directa con las exigencias legales y con estándares internacionales como la ISO/IEC 27001, que aseguran confidencialidad, integridad y disponibilidad de la información. Se recomienda:

- Incorporar una sección específica sobre protección de datos personales, detallando las medidas de seguridad, tratamiento, autorización y derechos de los titulares conforme a la (Ley 1581 de 2012, s.f.).
- Designar formalmente un responsable de protección de datos, como exige la ley, e incluir canales de atención a peticiones de ciudadanos sobre su información.
- Establecer medidas que garanticen la integridad, confidencialidad y disponibilidad de la información priorizada, incorporando controles técnicos y administrativos.
- Alinear la estrategia comunicacional con la Política de Gobierno Digital, promoviendo el uso de medios digitales accesibles, seguros e interoperables.
- Desarrollar un mecanismo de actualización periódica de la base de datos y validación de la información con los ciudadanos, para prevenir exclusiones o errores.

- Integrar este procedimiento con el Sistema de Gestión de Seguridad de la Información (SGSI) de la entidad.
- Establecer protocolos formales de retroalimentación y monitoreo, que permitan evaluar la efectividad de los canales de comunicación y realizar ajustes conforme a las necesidades de la organización y la ciudadanía.

Modelo estándar de control interno MECI. (Procedimiento de gestión documental)

Este documento es un pilar esencial de la gestión institucional y aporta al orden, trazabilidad y legalidad en la administración pública. Sin embargo, su alineación con la normativa de seguridad y privacidad aún es débil. Se recomienda:

- Incluir lineamientos específicos para el tratamiento de documentos que contengan datos personales, conforme a la (Ley 1581 de 2012, s.f.) y su decreto reglamentario.
- Establecer una clasificación documental según la naturaleza de la información: pública, reservada, clasificada, personal y sensible.
- Designar formalmente responsables del manejo documental con funciones diferenciadas y acceso controlado.
- Integrar medidas de seguridad física y digital, incluyendo control de acceso, respaldo, cifrado y destrucción segura.
- Desarrollar políticas para la digitalización segura, gestión de archivos electrónicos y respaldo de la documentación crítica.
- Articular este procedimiento con los planes de seguridad de la información, riesgos y comunicación, y con el cumplimiento de las (Ley 1581 de 2012, s.f.) y (Ley 1712, 2014).

Fases de implementación

Planeación y aprobación: elaboración del documento normativo, validación por el Comité de Gobierno Digital.

Socialización y capacitación: jornadas de formación dirigidas a funcionarios y contratistas.

Implementación operativa: ejecución por fases en dependencias clave.

Evaluación y seguimiento: auditorías internas, indicadores de desempeño y mejora continua.

Actualización periódica: revisión anual de políticas y adecuación a nuevas normativas.

Indicadores de evaluación

- % de funcionarios capacitados en protección de datos.
- % de información clasificada correctamente.
- N.º de incidentes de seguridad reportados.
- Tiempo promedio de respuesta a solicitudes ciudadanas.
- Nivel de cumplimiento del MINTIC y la Ley 1712.

Impactos esperados

- Modernización administrativa y tecnológica.
- Reducción de riesgos informáticos y de seguridad.
- Cumplimiento de normas nacionales e internacionales.
- Mayor transparencia y participación ciudadana.
- Creación de una cultura institucional de gestión informacional eficiente.

Conclusión

De acuerdo con los resultados obtenidos en el diagnóstico institucional, la Alcaldía enfrenta debilidades estructurales en la gestión de la información. Los funcionarios manifiestan un conocimiento parcial de los lineamientos del (MINTIC, 2020) y de las políticas de protección de datos personales. Aproximadamente el 65 % del personal no ha recibido capacitación formal sobre el tema, lo que evidencia la necesidad de establecer mecanismos formales de formación y estandarización. Asimismo, la información se maneja mediante criterios individuales, sin protocolos unificados de clasificación ni sistemas tecnológicos integrados.

Estas limitaciones obstaculizan la trazabilidad, la seguridad y la transparencia informacional. Por ello, el diseño de las políticas propuestas se fundamenta en un enfoque integral que articula el marco legal vigente, las necesidades identificadas y los principios de transformación digital del Estado colombiano.

En este sentido, el proceso de diseño se rige por las disposiciones establecidas en la (Ley 1581 de 2012, s.f.) , que regula la protección de datos personales; la (Ley 1712, 2014), sobre transparencia y acceso a la información pública; el Decreto 1008 de 2018, que reglamenta la política de Gobierno Digital; y las directrices del Modelo de Seguridad y Privacidad de la Información (MSPI). Además, se consideran las buenas prácticas internacionales definidas por la Norma ISO/IEC 27001, orientadas a la creación de Sistemas de Gestión de Seguridad de la Información (SGSI).

Cumplimiento del Objetivo 3

Socializar las políticas de seguridad de la información desarrolladas para la Alcaldía de Tamalameque, Cesar, asegurando que todas las partes interesadas comprendan y apoyen las políticas y el marco normativo propuestos.

Introducción

Después de haber elaborado las políticas de seguridad de la información siguiendo las directrices del Ministerio de Tecnologías de la Información y las Comunicaciones (MINTIC, 2020) es necesario promover su difusión en la Alcaldía de Tamalameque, Cesar. Este procedimiento es un avance estratégico para asegurar que las políticas no solo estén presentes en el ámbito normativo, sino que todos los funcionarios públicos y todas las dependencias de la institución que manejan información en su trabajo diario las entiendan, se apropien de ellas y las implementen.

Para establecer una cultura organizacional fundamentada en la transparencia, la eficiencia y la protección de datos, principios básicos del Gobierno Digital, es esencial la socialización. La implementación de las políticas mencionadas en el capítulo previo, que incluyen la clasificación y protección de datos, la gestión documental, el acceso a la información, la capacitación institucional y la infraestructura tecnológica, solo se podrá lograr mediante el compromiso activo de los actores institucionales.

Fundamentación del proceso de socialización

La necesidad de robustecer las capacidades institucionales que fueron identificadas en el diagnóstico inicial es lo que motiva el proceso de socialización de las políticas de seguridad de la información. Los resultados de este diagnóstico se ilustraron por medio de los gráficos examinados en el segundo capítulo. Las gráficas mostraron que los funcionarios poseen un nivel

medio-bajo de conocimiento acerca de las directrices del (MINTIC, 2020), que existe una gestión limitada de los procesos relacionados con la seguridad informativa y que no se han establecido procedimientos estandarizados para el manejo documental.

Por ejemplo, los gráficos que muestran la opinión de los servidores acerca del acceso y control de la información institucional revelaron que más del 60 % de los encuestados no conocía las reglas internas vinculadas con la protección de datos. Asimismo, se evidenció que el 50 % de los funcionarios no ha recibido capacitación reciente en temas de seguridad digital o gobierno abierto, lo que confirma la necesidad de un plan de socialización estructurado y permanente.

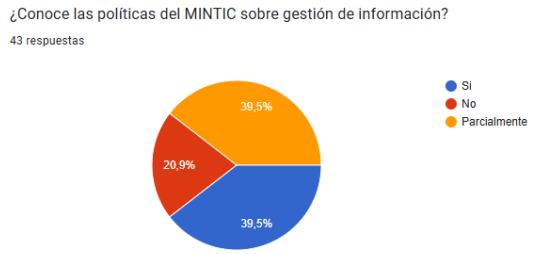
Estos resultados respaldan de manera total la ejecución del tercer objetivo del proyecto, que persigue asegurar el respaldo institucional y la apropiación de las políticas diseñadas. La socialización no solo hará posible la divulgación de su contenido, sino que también fomentará el compromiso y el sentido de pertenencia con respecto a la implementación del marco normativo que se ha propuesto.

Conoce las políticas del MINTIC sobe gestión de información

Los resultados del diagnóstico institucional efectuado en los empleados de la Alcaldía de Tamalameque, Cesar, son la base para el proceso de socialización de las políticas informativas. El diagnóstico mencionado reveló importantes diferencias en el entendimiento, manejo y ejecución de las directrices del (MINTIC, 2020) y de las políticas de administración de la información, lo que evidencia la urgencia de robustecer la cultura informacional dentro de la organización.

Grafica 1.

Conoce las políticas del MINTIC sobe gestión de información



Nota: Autoría propia

Análisis de resultados

La gráfica indica que solo el 39,5 % de los funcionarios asegura estar al tanto de las políticas del (MINTIC, 2020) en lo que respecta a la gestión de la información; un 39,5 % adicional admite tener un conocimiento parcial y el 20,9 % restante manifiesta no conocerlas para nada. Este escenario muestra que hay una distribución equitativa entre aquellos que tienen un conocimiento completo y los que lo tienen de manera escasa o nula, lo cual pone de manifiesto la ausencia de uniformidad y apropiación institucional en relación con las pautas nacionales.

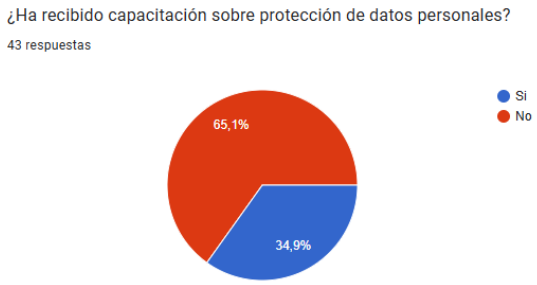
La falta de un conocimiento uniforme obstaculiza la aplicación adecuada de las normas de transparencia informativa, clasificación y seguridad definidas por el (MINTIC, 2020)Por tanto, este resultado tiene efectos directos en la administración pública local.

Capacitación sobre protección de datos personales

La siguiente gráfica presenta los resultados obtenidos respecto a la capacitación del personal en temas de protección de datos personales. Este aspecto resulta clave para evaluar el nivel de preparación institucional en el manejo responsable de la información y el cumplimiento de las políticas del MINTIC.

Grafica 2.

Ha recibido capacitación sobre protección de datos personales



Nota: Autoría propia

La Gráfica 2 revela que el 65,1% de los funcionarios no ha recibido capacitación formal en protección de datos personales, lo cual demuestra una brecha significativa en la formación del personal. Esta situación representa una debilidad crítica, ya que limita la correcta aplicación de los lineamientos del (MINTIC, 2020) y compromete la seguridad de la información institucional.

Por tanto, la socialización de las políticas de información, planteada en el objetivo 3, debe incluir no solo la divulgación de los lineamientos normativos, sino también espacios de capacitación y sensibilización que fortalezcan las competencias del personal en materia de protección de datos personales, clasificación documental y uso ético de la información pública. De esta manera, se garantiza que los funcionarios comprendan la importancia de aplicar criterios homogéneos, contribuyendo a la transparencia, eficiencia y confianza institucional.

Clasificación y Protección de la Información

La gráfica evidencia un manejo heterogéneo en la clasificación y protección de la información dentro de la Alcaldía de Tamalameque, Cesar. Mientras algunos funcionarios aplican parcialmente políticas institucionales, una proporción significativa aún recurre a criterios informales o personales para determinar la naturaleza de los documentos que manejan. Esta situación refleja una baja estandarización en los procesos y un conocimiento limitado de los lineamientos del MINTIC sobre gestión informacional. En consecuencia, se identifica la

necesidad de establecer protocolos unificados que fortalezcan la seguridad, confidencialidad y trazabilidad de los datos institucionales, garantizando así un cumplimiento efectivo del marco normativo vigente.

Cómo clasifica la información que maneja (pública, reservada, confidencial)

Los funcionarios de la Alcaldía han utilizado criterios de clasificación dispares, tal como se puede apreciar en la figura 3. Los resultados del diagnóstico indican que entre el 43 y el 49 % (según la consolidación definitiva) implementa una política institucional de clasificación; cerca del 37 % emplea criterios no formales (decisiones individuales o en equipo); mientras que el 7 % no lleva a cabo ninguna clasificación formal. Estos porcentajes muestran que, aunque hay un grupo considerable que aplica criterios institucionales, una parte significativa depende de prácticas ad hoc, lo cual provoca incoherencias en la gestión de documentos.

Las consecuencias prácticas de esta circunstancia son importantes: la ausencia de un criterio uniforme para clasificar información —en particular en documentos que contienen datos personales o información confidencial— incrementa el peligro de accesos no autorizados, pérdida del seguimiento y problemas para responder a peticiones de información dentro de los plazos y formatos requeridos por la (Ley 1712, 2014) y la (Ley 1581 de 2012, s.f.) Asimismo, la heterogeneidad de clasificación complica que los sistemas documentales sean interoperables y automatizados (por ejemplo, el etiquetado en los gestores documentales o el control de accesos por rol).

Grafica 3.

Cómo clasifica la información que maneja (pública, reservada, confidencial)

Nota: Autoria propia

Análisis de resultado

Los resultados evidencian una gestión heterogénea en los procesos de clasificación y resguardo de la información dentro de la entidad. Aunque algunos funcionarios aplican criterios institucionales formales, una parte considerable continúa utilizando métodos informales o personales, lo que genera inconsistencias en la protección de los datos. Esta falta de estandarización puede comprometer la confidencialidad de los documentos sensibles y aumentar los riesgos de pérdida o filtración de información. Asimismo, la baja claridad sobre la existencia de protocolos específicos sugiere una débil cultura organizacional en torno a la seguridad de la información. Por tanto, se hace necesario implementar políticas claras de clasificación, acompañadas de procesos de capacitación continua y mecanismos de control que garanticen el cumplimiento de las normas de protección de datos institucionales.

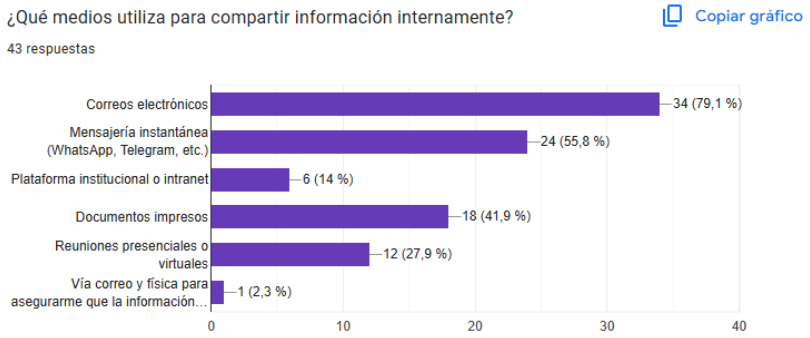
Qué medios utiliza para compartir información internamente

La siguiente gráfica presenta los principales medios que utilizan los funcionarios de la Alcaldía de Tamalameque, Cesar, para compartir información de manera interna. Este aspecto es fundamental para comprender cómo fluye la comunicación institucional y qué tan alineados

están los procesos con las políticas de gestión de la información promovidas por el (MINTIC, 2020)

Grafica 4.

Qué medios utiliza para compartir información internamente



Nota: Autoría propia

Análisis de resultado

La gráfica muestra los canales más empleados por los funcionarios de la Alcaldía de Tamalameque, Cesar, para el intercambio de información institucional. Se observa que el correo electrónico (79,1 %) y la mensajería instantánea (55,8 %) son los medios predominantes, mientras que el uso de herramientas institucionales o plataformas de intranet apenas alcanza un 14 %, lo que evidencia una baja consolidación de sistemas formales de gestión documental. Este comportamiento sugiere la ausencia de una estructura tecnológica robusta que garantice trazabilidad y seguridad en los flujos informacionales.

Asimismo, la falta de mecanismos institucionalizados para la rendición de cuentas y la comunicación con entes de control limita la transparencia y dificulta la supervisión de los procesos administrativos. Esta situación subraya la necesidad de fortalecer las políticas de información mediante la implementación de plataformas digitales seguras, interoperables y

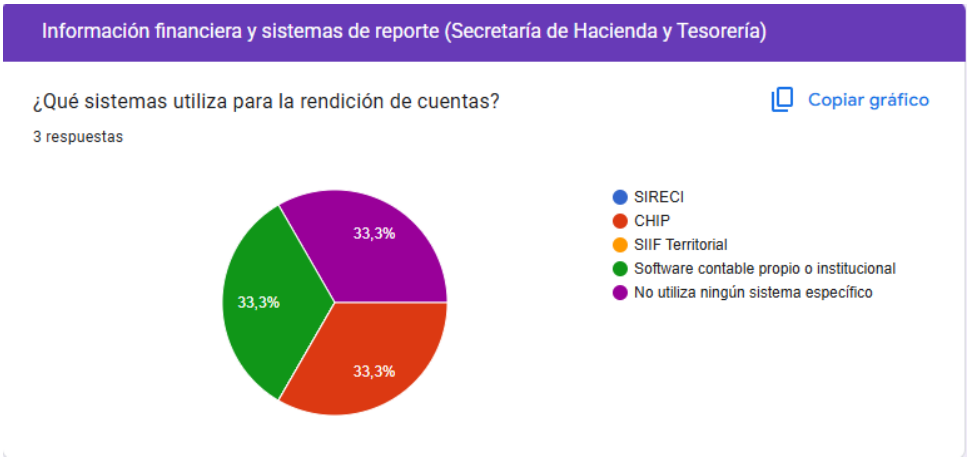
alineadas con los principios del Gobierno Abierto, promoviendo una gestión más eficiente y responsable.

Que sistemas utiliza para la rendición de cuentas

La siguiente gráfica evidencia los sistemas utilizados por las dependencias financieras y administrativas de la Alcaldía de Tamalameque, Cesar, para la rendición de cuentas. Este indicador permite evaluar el grado de institucionalización y estandarización en los procesos de reporte, así como el cumplimiento de los principios de transparencia y responsabilidad pública.

Grafica 5.

Que sistemas utiliza para la rendición de cuentas



Nota: Autoría propia

Análisis de resultado

De acuerdo con los datos obtenidos, se observa que la rendición de cuentas dentro de la Alcaldía de Tamalameque, Cesar, se realiza mediante distintos sistemas: el SIRECI, el CHIP y el SIIF Territorial, cada uno con una participación del 33,3 %. Esta distribución refleja una fragmentación en los mecanismos de reporte, ya que no existe una plataforma unificada que concentre la información financiera, presupuestal y de gestión.

Esta situación genera duplicidad de esfuerzos y limita la trazabilidad de la información, dificultando el seguimiento y la verificación de los resultados institucionales por parte de los entes de control y la ciudadanía. A su vez, el hecho de que no se evidencie un sistema propio o institucional para la rendición de cuentas muestra una dependencia de plataformas externas y una débil articulación con las políticas de Gobierno Digital del (MINTIC, 2020) que promueven la interoperabilidad y la gestión integrada de la información pública.

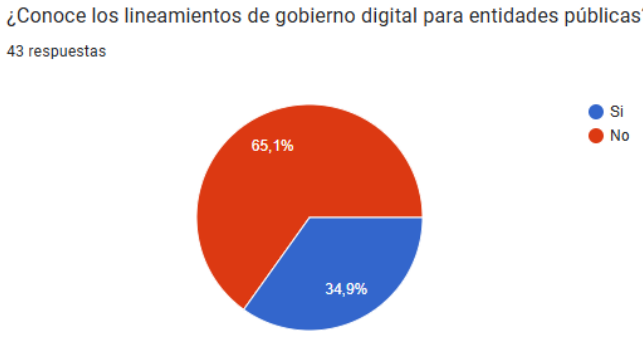
En este sentido, la falta de un sistema centralizado impide consolidar una cultura de transparencia activa, afectando el cumplimiento de la (Ley 1712, 2014) sobre acceso a la información pública. Es necesario avanzar hacia la adopción de una plataforma institucional interoperable, que permita la publicación de informes, datos abiertos y resultados de gestión en tiempo real, fortaleciendo la confianza ciudadana y la eficiencia administrativa.

Conoce los lineamientos de gobierno digital para entidades públicas

La siguiente gráfica muestra el nivel de conocimiento que poseen los funcionarios de la Alcaldía de Tamalameque, Cesar, sobre los lineamientos de Gobierno Digital establecidos por el (MINTIC, 2020). Este indicador es clave para comprender el grado de apropiación institucional de las políticas nacionales orientadas a la transformación digital del sector público.

Grafica 6.

Conoce los lineamientos de gobierno digital para entidades públicas



Nota: Autoría propia

Análisis de resultados

Los hallazgos indican que sólo el 34,9 % de los encuestados dice estar informado acerca de las pautas de Gobierno Digital, mientras que el 65,1 % restante no lo sabe. Esta cifra muestra una gran brecha en la comprensión y aplicación de las políticas nacionales vinculadas con la modernización del Estado y el manejo tecnológico.

La falta de conocimiento generalizado sobre estas directrices supone que las instituciones tienen una capacidad reducida para llevar a cabo estrategias de interoperabilidad, seguridad de la información y digitalización, elementos esenciales del modelo de Gobierno Digital. Asimismo, evidencia que no existen programas de capacitación o difusión interna que aseguren que los funcionarios entiendan cuán relevantes son estas políticas para la transparencia y eficacia en la administración.

Esta falencia representa un obstáculo para el cumplimiento de los objetivos establecidos por el (MINTIC, 2020), particularmente aquellos relacionados con la transformación digital, la innovación pública y la confianza ciudadana. En consecuencia, se recomienda desarrollar estrategias de formación continua, jornadas de socialización y talleres prácticos, orientados a fortalecer las competencias digitales del personal y asegurar la correcta implementación del marco normativo vigente.

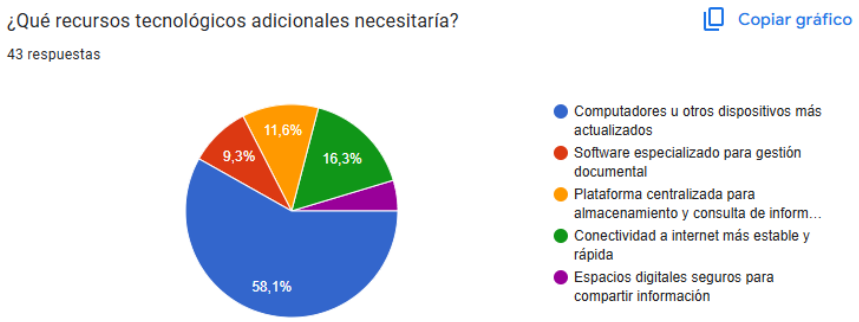
En suma, la gráfica permite concluir que el éxito de la transformación digital en la Alcaldía de Tamalameque depende en gran medida de la apropiación interna del modelo de Gobierno Digital, lo cual exige una intervención inmediata en materia de sensibilización y fortalecimiento de capacidades institucionales

Que recursos tecnológicos adicionales necesitaría

La siguiente gráfica presenta los recursos tecnológicos adicionales que el personal de la Alcaldía de Tamalameque considera necesarios para fortalecer los procesos de gestión y avanzar hacia un modelo institucional más digital. Este aspecto resulta esencial para identificar las principales brechas tecnológicas que limitan la eficiencia administrativa y la implementación de estrategias de Gobierno Digital.

Grafica 7.

Que recursos tecnológicos adicionales necesitaría



Nota: Autoría propia

Análisis de resultados

Los hallazgos indican que el 58,1 % de los encuestados reconoce la necesidad de tener computadoras o dispositivos más modernos, lo cual demuestra que el parque tecnológico actual está obsoleto y supone un impedimento para llevar a cabo tareas digitales y administrativas. En segundo lugar, el 16,3 % destaca la conectividad a internet como una prioridad, subrayando que es crucial tener una red más estable y veloz para que las plataformas y los sistemas de información puedan operar correctamente.

Además, el 11,6 % de los encuestados cree que es esencial la creación de una plataforma única para almacenar y consultar información, lo que simplificaría la comunicación entre

dependencias e integraría datos. El 9,3 % de los encuestados indica que no tienen software especializado para la gestión de documentos, lo cual es una herramienta esencial para automatizar procesos. Por último, el 4,7 % menciona la ausencia de espacios digitales seguros para intercambiar información, lo que refleja una inquietud por la seguridad y privacidad de los datos de la institución.

En términos generales, los hallazgos muestran que la actualización de equipos y el aumento de la conectividad son las necesidades tecnológicas primordiales del organismo. La falta de estas capacidades limita la habilidad operativa y el uso de herramientas digitales, lo que repercute negativamente en la productividad y en la calidad del servicio público. Por lo tanto, se sugiere elaborar un plan de inversión en infraestructura tecnológica que dé prioridad a la actualización de los equipos, al incremento del acceso a internet y a la implementación de sistemas integrados que hagan más robusta la gestión institucional.

Conclusión

Realizar este trabajo final de grado, posibilitó entender la importancia que tienen las políticas de seguridad de la información para el fortalecimiento institucional y para la modernización de la administración pública a nivel local. La investigación realizada en la Alcaldía de Tamalameque, Cesar, mostró que la institución afronta desafíos importantes con respecto a la gestión de datos, a la protección de los mismos y al uso de las tecnologías de información y comunicación (TIC). La falta de políticas formales y unificadas, a pesar de que algunas dependencias individuales están intentando mejorar, obstaculiza la trazabilidad de los procedimientos, la transparencia y la eficacia administrativa.

Además, se comprobó que era necesario establecer un marco normativo interno que guíe el tratamiento, la difusión y el almacenamiento de datos públicos, siguiendo las directrices del Ministerio de Tecnologías de la Información y las Comunicaciones (MINTIC, 2020) La ausencia de un liderazgo claro en este tema pone en peligro la confianza de los ciudadanos en la administración pública y la seguridad de los datos institucionales.

Por otra parte, se detectó una actitud favorable por parte de los funcionarios respecto de la implementación de métodos actuales de gestión y el uso de herramientas digitales. Este descubrimiento es crucial porque evidencia que hay una intención institucional de avanzar hacia un modelo de gestión de información más completo, transparente y eficaz, así como hacia la aplicación del Gobierno Digital. Por lo tanto, formular políticas de seguridad de la información no es únicamente un requerimiento normativo, sino también una oportunidad para cambiar la gestión pública a nivel local y reforzar su habilidad para responder a las exigencias tecnológicas y ciudadanas del contexto presente.

Recomendaciones

Conforme a las directrices del (MINTIC, 2020), la (Ley 1712, 2014) sobre Transparencia y la (Ley 1581 de 2012, s.f.) sobre protección de datos personales, desarrollar e implementar una política institucional para gestionar información que defina procesos oficiales para clasificar, resguardar, almacenar y divulgar datos.

Con la implementación de una plataforma tecnológica que centralice toda la información financiera, administrativa y documental, es posible unificar los sistemas de rendición de cuentas. Esto asegura que los trámites sean transparentes, eficaces y trazables ante el público y las entidades reguladoras.

Optimizar la gestión institucional y hacer más accesible la información pública mediante el fortalecimiento de la infraestructura tecnológica de la entidad, lo cual se logra con la modernización de los equipos informáticos, el perfeccionamiento de la conectividad y el establecimiento de soluciones digitales interoperables.

Con el objetivo de robustecer las habilidades de los servidores públicos en cuanto a la gestión de TIC, la seguridad de datos y las regulaciones actuales sobre Gobierno Digital, se deben establecer programas continuos de capacitación y alfabetización digital.

Fomentar una cultura organizacional que esté enfocada en la innovación y en el empleo responsable de la información, en la cual los datos se vean como un recurso estratégico para decidir, ser transparentes y permitir la participación ciudadana.

Implementar un monitoreo y una evaluación periódica de la política de información, definiendo indicadores de cumplimiento y procedimientos para mejorar constantemente que garanticen su efectividad, sostenibilidad y congruencia con las metas institucionales.

Referencias bibliográficas

Bustamante García et al., 2. (Junio de 2021). *Políticas basadas en la ISO 27001:2013 y su influencia en la gestión de seguridad de la información en municipalidades de Perú.* Obtenido de https://doi.org/10.29019/enfoqueute.743

Chiyana, S. (13 de Octubre de 2023). *ITDO*. Obtenido de https://www.itdo.com/blog/como-garantizar-el-cumplimiento-y-la-privacidad-de-datos-en-la-era-de-la-analitica/

ciberlinea. (25 de agosto de 2024). Obtenido de La organización de la información: Claves para una gestión eficiente en tu empresa. : https://ciberlinea.net/la-organizacion-de-la-informacion/

Ciberseguridad. (2021). *ciberseguridad*. Obtenido de https://ciberseguridad.com/herramientas/politica-seguridad-informacion/

Cuesta, D. (2022). *repository.unimilitar.* Obtenido de https://repository.unimilitar.edu.co/server/api/core/bitstreams/cab4bdf3-1a54-4977-af3e-0c39997457de/content

Cueto, H. (13 de Abril de 2023). *Business Insider Mexico*. Obtenido de https://businessinsider.mx/gestion-datos-clave-para-exito-empresas-era-digital_tecnologia/

Decreto 1377 de 2013. (s.f.). Obtenido de https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=53646

Gestio documental. (14 de Agosto de 2023). Obtenido de Beneficios de la gestión documental para empresas en la era digital.: https://www.gestiodocumental.net/beneficios-de-la-gestion-documental-para-empresas-en-la-era-digital/

Giap, E., & Villarreal, R. (2021). *Sistema de gestión para la seguridad de la información basado en la Norma ISO/IEC 27001:2013 en la Empresa Constructora Pérez & Pérez SAC, Moyobamba.* Obtenido de Universidad César Vallejo: https://repositorio.ucv.edu.pe/handle/20.500.12692/63424

Grupo ACS. (8 de Julio de 2022). Obtenido de https://www.grupoacs.com/ficheros_editor/File/05_Compliance/Pol%C3%ADticas/31_Pol%C3%ADtica%20de%20Seguridad%20de%20la%20Informaci%C3%B3n.pdf

Jain, A. (2020). *Visure Solutions, Inc.* Obtenido de ¿Qué es la ingeniería de sistemas?: https://visuresolutions.com/es/blog/Ingenier%C3%ADa-de-Sistemas/

Ley 1266 de 2008. (s.f.). Obtenido de https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=34488

Ley 1341 de 2009. (s.f.). Obtenido de https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=36913

Ley 1581 de 2012. (s.f.). Obtenido de Función publica: https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=49981

Ley 1712. (6 de mayo de 2014). *Gestor Normativo. (s/f.* Obtenido de https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=56882

Mariana. (20 de Enero de 2024). *ciberlinea.* Obtenido de https://ciberlinea.net/riesgos-y-consecuencias-de-la-falta-de-capacitacion-laboral/

Marin, M. (2017). *Diseño e implementacion de una politica* . Obtenido de https://repository.unad.edu.co/bitstream/handle/10596/14261/51820281.pdf?sequence=1

MINTIC. (31 de Diciembre de 2020). Obtenido de https://mintic.gov.co/portal/inicio/Sala-de-prensa/Noticias/161311:MinTIC-establece-lineamientos-para-que-las-entidades-publicas-estandaricen-la-oferta-de-informacion-y-servicios

Ortiz, V. (2021). *repository.ucatolica.* Obtenido de https://repository.ucatolica.edu.co/server/api/core/bitstreams/671c379e-57cf-4b0b-93d1-eccb021944e5/content

Patiño, J. (Enero de 2024). *bosconia-cesar.* Obtenido de https://www.bosconia-cesar.gov.co/Transparencia/PlaneacionGestionyControl/PLAN%20DE%20TRATAMIENTO%20DE%20RIESGOS%20DE%20SEGURIDAD%20Y%20PRIVACIDAD%20DE%20LA%20INFORMACI%C3%93N%20BOSCONIA%202024.pdf

Pilla Y, J. C. (2019). *repositorio.uisek.* Obtenido de https://repositorio.uisek.edu.ec/bitstream/123456789/3601/1/DISE%C3%91O%20DE%20UNA%20POL%C3%8DTICA%20DE%20SEGURIDAD%20DE%20LA%20INFORMACI%C3%93N%20PARA%20EL%20%C3%81REA%20DE%20TECNOLOG%C3%8DA%20DE%20LA%20INFORMACI%C3%93.pdf

Políticas Técnicas de Seguridad de la Información . (Septiembre de 2020). Obtenido de Función publica: https://www1.funcionpublica.gov.co/documents/418537/36701283/politicas-tecnicas-seguridad-informacion.pdf/8020b3e9-5d8e-6344-8884-400ca273483c?t=1600987972846

Sepúlveda, S., & Cravero, A. (Noviembre de 2021). *Diseño de una política de seguridad de la información: una propuesta*. Obtenido de Proquest.com: https://www.proquest.com/openview/3af57e779f875359ddf2c47da5b37225/1?pq-origsite=gscholar&cbl=1006393

Solove, D. (2006). *A taxonomy of privacy. University of Pennsylvania Law Review, 154(3), 477–560.* Obtenido de https://scholarship.law.upenn.edu/penn_law_review/vol154/iss3/1/

Superservicios . (Enero de 2023). Obtenido de Plan de seguridad y privacidad de la informacion : https://www.superservicios.gov.co/sites/default/files/inline-files/Plan-de-seguridad-y-privacidad-de-la-informacion-v1-2023.pdf

(enero de 2023). *Superservicios.* Obtenido de Plan de seguridad y privacidad de la información.: https://www.superservicios.gov.co/sites/default/files/inline-files/Plan-de-seguridad-y-privacidad-de-la-informacion-v1-2023.pdf