Desarrollar Guía de Buenas Prácticas para el Mejoramiento de los Servicios en la Nube de la Alcaldía de Fusagasugá

Alcaldía de Fusagasugá

Karen Vanessa Escalante Cubillos

Universidad de Cundinamarca

Facultad de ingeniería

Ingeniería de sistemas y computación

Fusagasugá

2025

Desarrollar Guía de Buenas Prácticas para el Mejoramiento de los Servicios en la Nube de la Alcaldía de Fusagasugá

Pasantía

Karen Vanessa Escalante Cubillos

German Mauricio Rodríguez Fernández

Director Interno

Javier Mauricio Rodríguez Ruiz

Director externo

Universidad de Cundinamarca

Facultad de ingeniería

Ingeniería de sistemas y computación

Fusagasugá

2025

Tabla de contenido

Lista de Figuras

Lista de apéndice

Resumen

El presente proyecto se realizó con el objetivo de desarrollar una guía de buenas prácticas para el mejoramiento de los servicios en la nube de la alcaldía de Fusagasugá en la oficina TIC y transformación digital, de esta manera se busca fortalecer la seguridad de la infraestructura tecnológica de la entidad. Para lograr los resultados esperados, se aplicó el ciclo PHVA (Planear – Hacer – Verificar – Actuar) como guía metodológica, lo cual permitió estructurar el trabajo en fases consecutivas para ajustar las soluciones propuestas al contexto institucional.

Durante la fase de planificación, se realizó un diagnóstico del estado en el que se encontraba la infraestructura en la nube de la entidad, lo que permitió identificar fortalezas en la segmentación de subredes y la escalabilidad de los servicios. Igualmente, se identificaron puntos críticos que requieren ser tratados de manera oportuna. A partir de estos hallazgos, se determinó cual sería el proceso por seguir en las siguientes fases.

Con ello, en la fase de ejecución se realizó un análisis para identificar vulnerabilidades en una instancia representativa de la plataforma en la nube por medio de Nmap, esta evaluación evidenció la importancia de aplicar mecanismos preventivos que permitan anticiparse a escenarios de riesgo sin comprometer la estabilidad operativa de los servicios de la entidad.

Para la fase de verificación se diseñó una matriz de riesgos y se representó visualmente mediante un mapa de calor, lo cual facilitó la clasificación y priorización de amenazas de acuerdo con la probabilidad e impacto. Con esta información se formularon controles de seguridad alineados con la norma ISO/IEC 27001:2022 y se estimó el riesgo residual asociado a cada escenario. Se validó la viabilidad técnica ya que los resultados proyectados presentaron una disminución significativa en el nivel de exposición.

En la fase final, actuar, se documentaron procedimientos para la instalación de certificados SSL y la configuración de copias de seguridad, acciones que están orientadas a mejorar la disponibilidad y la protección de los datos institucionales. Además, para integrar el trabajo realizado en las fases anteriores se diseñó una guía de buenas prácticas ajustada a las necesidades de la entidad, la cual recopila recomendaciones normativas y operativas que fortalecen la gestión segura de los servicios en la nube y es un insumo importante en la toma de decisiones a futuro para la protección de la información de la entidad.

Los resultados del proyecto aportan valor estratégico a la alcaldía de Fusagasugá, al brindar herramientas para mejorar la infraestructura digital de manera preventiva y de acuerdo a los lineamientos normativos a nivel nacional e internacional para reducir la brecha y fortalecer la seguridad de la información de la entidad.

Palabras claves: Seguridad de la información, nube, gestión del riesgo, vulnerabilidades, infraestructura tecnológica, buenas prácticas.

Abstract

This project was carried out with the objective of developing a guide of good practices for the improvement of cloud services of the Mayor's Office of Fusagasugá in the TIC and digital transformation office, thus seeking to strengthen the security of the technological infrastructure of the entity. To achieve the expected results, the PHVA cycle (Plan - Do - Verify - Act) was applied as a methodological guide, which allowed structuring the work in consecutive phases to adjust the proposed solutions to the institutional context.

During the planning phase, a diagnosis was made of the state of the entity's cloud infrastructure, which made it possible to identify strengths in the segmentation of sub-networks and the scalability of services. Critical points that need to be addressed in a timely manner were also identified. Based on these findings, the process to be followed in the following phases was determined.

With this, in the execution phase, an analysis was carried out to identify vulnerabilities in a representative instance of the cloud platform by means of Nmap. This evaluation showed the importance of applying preventive mechanisms to anticipate risk scenarios without compromising the operational stability of the entity's services.

For the verification phase, a risk matrix was designed and visually represented by means of a heat map, which facilitated the classification and prioritization of threats according to probability and impact. With this information, security controls aligned with ISO/IEC 27001:2022 were formulated and the residual risk associated with each scenario was estimated. The technical feasibility was validated since the projected results showed a significant decrease in the level of exposure.

In the final phase, procedures were documented for the installation of SSL certificates and the configuration of backup copies, actions aimed at improving the availability and

protection of institutional data. In addition, to integrate the work carried out in the previous phases, a best practices guide was designed, adjusted to the entity's needs, which compiles regulatory and operational recommendations that strengthen the secure management of cloud services and is an important input in future decision-making for the protection of the entity's information.

The results of the project provide strategic value to the mayor's office of Fusagasugá, by providing tools to improve the digital infrastructure in a preventive manner and in accordance with national and international regulatory guidelines to reduce the gap and strengthen the entity's information security.

Key words: Information security, cloud, risk management, vulnerabilities, technological infrastructure, good practices.

Capítulo 1. Introducción

Planteamiento del Problema

En la actualidad, el uso de servicios en la nube es considerada una herramienta importante para mejorar los procesos tecnológicos y administrativos en entidades públicas. Sin embargo, su implementación requiere la adopción de buenas prácticas que garantizan la seguridad en la gestión de estos servicios, en el caso de la alcaldía de Fusagasugá, Cundinamarca en la oficina TIC y transformación digital, se identifica la necesidad de mejorar los mecanismos que respaldan la operación segura y confiable de su infraestructura en la nube.

Por lo tanto, la ausencia de lineamientos técnicos estandarizados como políticas y procedimientos que permiten la administración de los servicios en la nube pueden causar vulnerabilidades que afecten la continuidad del servicio, la protección de los datos sensibles y la capacidad de respuesta ante incidentes. Si bien el Decreto 338 de 2022 establece que “las entidades públicas deberán adoptar todas las medidas necesarias para garantizar el máximo aprovechamiento de las Tecnologías de la Información y las Comunicaciones (TIC) en el desarrollo de sus funciones” (República de Colombia, 2022, Decreto 338). Sin embargo, es necesario definir una estrategia que mejore la administración de los recursos tecnológicos, para reducir la brecha y garantizar una operación segura en el entorno digital de la alcaldía de Fusagasugá.

En este sentido, las entidades del sector público que hacen uso de tecnologías en la nube deben adoptar estrategias que aseguren la protección de los datos críticos institucionales para prevenir ataques informáticos que pueden causar perdidas de la información de la entidad. De acuerdo con la Función Pública de Colombia, “la política de administración de riesgos del Departamento Administrativo de la Función Pública – DAFP -, tiene un carácter estratégico y está fundamentada en el modelo integrado de planeación y gestión, la guía para la administración del riesgo y el diseño de controles en entidades públicas, con un enfoque

preventivo de evaluación permanente de la gestión y el control, el mejoramiento continuo y con la participación de todos los servidores de la entidad" (Función Pública, 2024, p. 6). Por lo tanto, esta política es importante en la adopción de buenas prácticas de seguridad de la información en la alcaldía de Fusagasugá ya que a través de la guía de la administración del riesgo contribuye a la protección de los datos de la infraestructura tecnológica y la gestión de los servicios de la entidad.

En el contexto internacional, la adopción de normas de seguridad como la ISO/IEC 27001: 2022 e ISO/IEC 27002:2022 brindan un marco estratégico que guía la gestión de los riesgos tecnológicos en diferentes sectores. Estas normas, desarrolladas por el Instituto Colombiano de Normas Técnicas y Certificación (ICONTEC), establecen estándares y buenas prácticas diseñadas para proteger los activos de información. Sin embargo, muchas instituciones públicas enfrentan obstáculos debido a la falta de capacitación continua, la escasez de recursos y la disponibilidad limitada de herramientas adecuadas para la implementación de prácticas que garanticen la protección de la información.

De acuerdo con lo expresado por Duarte Caviedes (2018), la gestión del riesgo requiere la adopción de tecnologías avanzadas, la integración de políticas y procedimientos definidos que permitan mitigar amenazas y garantizar la protección continua de los activos de información. Por esta razón, para mejorar la seguridad en la alcaldía de Fusagasugá se requiere invertir en herramientas modernas y también diseñar estrategias de gestión que garanticen la adecuada protección de los datos, brindándoles a los ciudadanos confianza al utilizar los servicios ofrecidos por la entidad.

Justificación

De acuerdo con las necesidades descritas en el planteamiento del problema, este proyecto busca mejorar la infraestructura tecnológica de la entidad a través del diseño de una guía de buenas prácticas para la gestión de servicios en la nube, cumpliendo con lo dispuesto

por las normas ISO/IEC 27001:2022 e ISO/IEC 27002:2022; Estas normas internacionales de seguridad de la información proporcionan una base que facilita la reducción de los riesgos asociados a los entornos tecnológicos, promueve una administración segura y confiable de los activos institucionales. Dado que estos servicios soportan procesos críticos de la administración pública, su correcta gestión resulta fundamental para asegurar la continuidad operativa; proteger la información institucional y garantizar la calidad de los servicios prestados a la ciudadanía.

Por consiguiente, este trabajo de pasantía tiene como propósito desarrollar buenas prácticas que contribuyan a la seguridad y mejoren la eficiencia en el uso de los servicios en la nube de la alcaldía de Fusagasugá, contribuyendo así a una gestión tecnológica más confiable, sostenible y alineada con los principios del Gobierno Digital. Como indica Carvajal Hurtado (2022), “la implementación de buenas prácticas de seguridad basadas en normas internacionales permite una gestión eficiente y la protección continua de los activos de información” (Carvajal Hurtado, 2022). De esta manera, la norma ISO/IEC 27001:2022 permite reducir la exposición de los recursos tecnológicos y proporcional a un marco de referencia claro para el personal encargado de la administración de los sistemas.

Este proyecto contribuye a la estandarización de procedimientos, facilita la toma de decisiones y fortalece la capacidad de respuesta ante posibles incidentes de seguridad; con el uso de herramientas como mapas de calor, se tendrá un análisis visual que identificará áreas críticas de la infraestructura tecnológica, ayudando a priorizar los riesgos y generando valor institucional. De esta manera, promueve una cultura organizacional orientada a la mejora continua en seguridad de la información.

Objetivos

Objetivo general

Desarrollar una guía de buenas prácticas para el mejoramiento de los servicios en la nube de la alcaldía de Fusagasugá.

Objetivos específicos

- Planificar un diagnóstico del estado actual del servidor web de la plataforma, identificando aspectos clave para la mejora de la infraestructura.
- Ejecutar análisis de vulnerabilidades para determinar las brechas y riesgos existentes para fortalecer la protección de los servicios en la nube de la alcaldía de Fusagasugá.
- Verificar los riesgos de los activos de información de la infraestructura TIC por medio de mapas de calor, como herramienta de análisis visual, en concordancia con las buenas prácticas de la norma ISO/IEC 27001:2022.

Alcance

Este proyecto tiene como finalidad desarrollar una guía de buenas prácticas para mejorar la seguridad y eficiencia de los servicios en la nube de la alcaldía de Fusagasugá en la oficina de las TIC y la transformación digital. Para ello, se contempla la ejecución de actividades que permitan diagnosticar el estado actual de la infraestructura tecnológica, identificar vulnerabilidades y establecer procedimientos que fortalezcan su administración; La gestión de la seguridad en este entorno responde a los criterios definidos por las normas ISO/IEC 27001:2022 y ISO/IEC 27002:2022, que proporciona un marco de referencia para reducir los riesgos tecnológicos y proteger los activos de información (ICONTEC, 2022).

De esta manera, en el desarrollo de este proyecto se tiene prevista la elaboración de un informe que documenta el estado actual de los servicios en la nube de la alcaldía de Fusagasugá, así como un diagnóstico inicial de una instancia alojada en la nube de la entidad, ambos documentos permitirán identificar los aspectos críticos que requieren intervención y

proponer acciones de mejora; Según Mora Guamán (2022), un diagnóstico del entorno tecnológico es fundamental para comprender las vulnerabilidades existentes y definir acciones correctivas. De igual manera, se diseñará un diagrama de la topología de los servicios en la nube, el cual facilitará la comprensión de la estructura tecnológica actual y servirá como base para formular recomendaciones para la mejora continua de las plataformas de la entidad.

Por otra parte, se realizará la elaboración de una matriz de riesgos de seguridad de la información y el diseño de un mapa de calor con la intención de visibilizar las áreas de mayor exposición y priorizar acciones correctivas, estas herramientas son importantes para identificar los puntos críticos de la infraestructura tecnológica. De igual forma, se desarrollarán procedimientos para la instalación de certificados SSL y la configuración de copias de seguridad, permitiendo estandarizar estas tareas para mejorar la seguridad y la disponibilidad del servicio.

Para terminar, se tendrá como resultado una guía de buenas prácticas para la gestión de servicios en la nube que servirá como documento de referencia para el personal técnico de la alcaldía de Fusagasugá, facilitando una administración segura, y documentada de la infraestructura digital; fomentando la mejora continua en la institución de acuerdo con los principios del Gobierno Digital.

Descripción de la organización

La alcaldía de Fusagasugá es una entidad pública que se encarga de la administración municipal, ubicada en el departamento de Cundinamarca. Su misión institucional es "Administrar eficientemente los recursos institucionales, sociales, naturales y económicos, con inclusión social y participación ciudadana, para promover el desarrollo sostenible, la prosperidad, la equidad, mejorando la calidad de vida de quienes viven en Fusagasugá" (Alcaldía de Fusagasugá, 2024); promueve el bienestar de la ciudadanía y el fortalecimiento institucional.

En cuanto a su compromiso de modernizar sus servicios, la alcaldía de Fusagasugá ha incorporado diversas soluciones tecnológicas que optimizan la gestión interna, mejoran la atención a los ciudadanos y facilitan el acceso a la información. Además, promueve el modelo de Gobierno Digital, lo que implica crear un entorno digital accesible, transparente y participativo para la comunidad. En este contexto, la infraestructura digital de la entidad desempeña un papel estratégico ya que soporta procesos clave como la gestión administrativa, la comunicación institucional y la prestación de servicios en línea.

La dependencia responsable de la administración de las plataformas tecnológicas y servicios en la nube es la Oficina de Tecnologías de la Información y las Comunicaciones (TIC), la cual tiene a su cargo la implementación de soluciones que garanticen la seguridad, disponibilidad y eficiencia de los sistemas informáticos. Como se señala en el sitio oficial, la misión de esta dependencia es “Gestionar eficientemente los recursos, servicios e infraestructura de TI, facilitando el acceso y uso de las tecnologías de la información y las comunicaciones para consolidar un estado proactivo e innovador que genere valor público y transformación digital para Fusagasugá” (Alcaldía de Fusagasugá, 2024). Esta área es importante en el desarrollo de iniciativas que promuevan la transformación digital del municipio, de acuerdo con los objetivos del gobierno abierto y la mejora continua del servicio público.

Importancia del proyecto para la empresa

La ejecución de este proyecto representa un aporte en el fortalecimiento institucional de la alcaldía de Fusagasugá al abordar aspectos críticos relacionados con la seguridad y eficiencia de sus servicios en la nube, ya que la infraestructura tecnológica soporta los procesos administrativos, operativos y de atención ciudadana. Según el Decreto 338 de 2022, las entidades públicas deben adoptar estrategias digitales que aseguren no solo la protección de sus datos, sino también la continuidad de los servicios esenciales para la comunidad

(República de Colombia, 2022, Decreto 338), la correcta gestión de la seguridad conlleva una mayor confiabilidad, disponibilidad y calidad del servicio.

A partir de la implementación de buenas prácticas, este proyecto ayuda a reducir los riesgos de seguridad, mejorar tanto la capacidad de respuesta ante incidentes como la administración de los recursos tecnológicos. Desde el punto de vista de Mora Guamán (2022), la adopción de buenas prácticas de seguridad proporciona un marco de referencia que facilita la gestión eficiente de los recursos tecnológicos y mejora la capacidad institucional para enfrentar incidentes. De hecho, la documentación de procedimientos facilita la continuidad operativa de los servicios permitiendo que el personal técnico cuente con herramientas para la toma de decisiones y el manejo proactivo de la infraestructura.

Desde esta perspectiva, este proyecto fortalece la sostenibilidad de la transformación digital en la alcaldía de Fusagasugá, como lo plantea la gestión pública. En relación con este proceso, Carvajal Hurtado (2022) señala que la transformación digital en las instituciones públicas requiere la adopción de marcos normativos que no solo protejan los activos digitales, sino que impulsen una cultura organizacional orientada a la mejora continua. En consecuencia, los resultados de este trabajo representan un insumo importante para el cumplimiento de los objetivos estratégicos de la entidad y para el beneficio de la comunidad.

Capítulo 2. Marco referencial

Marco teórico

Base teórica

En vista del entorno actual, el avance de las tecnologías de la información ha impulsado a las entidades públicas a iniciar un proceso progresivo de migración de su información y servicios hacía la nube. Esta decisión responde a la necesidad de modernizar su infraestructura tecnológica, mejorar los recursos disponibles y la calidad de los servicios ofrecidos a la ciudadanía. Por otra parte, esta transición responde a una tendencia global enmarcada en la transformación digital y también a los lineamientos estratégicos establecidos por organismos gubernamentales que buscan fortalecer la seguridad de la información y promover la transparencia institucional.

Dentro del procesos de transformación digital de las entidades públicas, es importante implementar políticas de ciberseguridad y gestionar los riesgos tecnológicos de las instituciones públicas, aplicando normas internacionales como la ISO/IEC 27001:2022 para fortalecer los mecanismos de control. Dado lo anterior, el Decreto 338 de 2022 establece que su objetivo es “fortalecer la gobernanza de la seguridad digital, la identificación de infraestructuras criticas cibernéticas y servicios esenciales, la gestión de riesgos y la respuesta a incidentes de seguridad digital” (República de Colombia, 2022, Decreto 338). En este sentido, la implementación de políticas de ciberseguridad ayuda a mitigar los riesgos asociados a las amenazas digitales para aumentar la confianza pública en las entidades, al mejorar la capacidad de respuesta ante posibles ataques.

Para llevar a cabo este proceso, es indispensable que las entidades públicas implementen mecanismos que protejan la información de manera constante. Según el Ministerio de Tecnologías de la Información y las Comunicaciones (2016), “los servicios en la nube deben incorporar mecanismos de seguridad que aseguren la confidencialidad, integridad

y disponibilidad de la información, tanto en tránsito como en almacenamiento". De acuerdo con esto es necesario establecer prácticas, políticas y procedimientos que mitiguen las vulnerabilidades y permitan mantener la continuidad del servicio.

En el desarrollo de este proceso, la gestión del riesgo informático representa un componente importante, refiriéndose al conjunto de acciones orientadas a identificar, analizar y responder ante amenazas que puedan comprometer los activos tecnológicos de la entidad. En este sentido, Pulido & Mantilla (2016) destacan que una gestión del riesgo informático adecuada permite adoptar un enfoque preventivo frente a los problemas de seguridad, disminuyendo la exposición a amenazas internas y externas que pueden afectar la operación institucional. Este punto de vista es importante en entidades públicas como en este caso la alcaldía, debido a que manejan información sensible y dependen de plataformas digitales para su funcionamiento diario.

Al igual diversos estudios han demostrado que la adopción de servicios en la nube representa una mejora en el desempeño institucional. Según el Ministerio de Tecnologías de la Información y las Comunicaciones (2016), el uso de servicios en la nube facilita el acceso a la información y contribuye a la modernización de los servicios digitales. Sin embargo, su implementación exige el fortalecimiento de mecanismos de control y la adopción de marcos normativos que garanticen la protección de los activos de información, en coherencia con los principios establecidos en la norma ISO/IEC 27001:2022 y en las directrices del Gobierno Digital.

Como parte del proceso de fortalecimiento institucional, el Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC) ha desarrollado instrumentos específicos, entre la Matriz de Riesgos de Seguridad de la Información y diversas guías destinadas al diseño de controles orientados a salvaguardar la privacidad y la protección de los datos institucionales (Ministerio de Tecnologías de la Información y las Comunicaciones, 2016). Estas herramientas

son fundamentales para que las entidades públicas puedan fortalecer sus mecanismos de seguridad de la información, de acuerdo con sus prácticas con los estándares internacionales, pero siempre adaptándolas a las realidades operativas y necesidades específicas del contexto nacional.

De esta manera las instituciones públicas deben gestionar el riesgo para garantizas la seguridad de la información al identificar amenazas y vulnerabilidades en las actividades que se desarrollan a diario dentro de estas entidades. Para ello, el Ministerio de Tecnologías de la Información y las Comunicaciones (MINTIC) cuenta con un Modelo de gestión de riesgos de Seguridad Digital (MGRSD) que ofrece una estructura para la identificación, evaluación y gestión de riesgos en el entorno digital, " El MGRSD instrumentaliza sus lineamientos generales para las entidades públicas a través de la "Guía para la Administración de Riesgos y el Diseño de Controles en Entidades Públicas" y su anexo 4 denominado "Lineamientos para la Gestión de Riesgos de Seguridad Digital en Entidades Públicas " (Ministerio de Tecnologías de la Información y las Comunicaciones, 2024). Además, esta guía se alinea con los marcos normativos del Gobierno Digital para facilitar la implementación en entidades públicas del territorio nacional.

Antecedentes

Con base en diferentes estudios realizados en el sector público colombiano, se ha evidenciado la necesidad de fortalecer los mecanismos de seguridad en la nube y establecer metodologías para la gestión del riesgo informático. En este ámbito, Pulido & Mantilla (2016) una investigación aplicada en la alcaldía de Fusagasugá, donde propusieron un modelo de implementación de un sistema general de seguridad informática. Basado en un análisis de riesgos tecnológicos, su trabajo permitió identificar falencias en la administración de los servicios digitales y plantear protocolos orientados a mitigar amenazas. Los autores advierten que “la inexistencia de un marco de políticas estructurado en las oficinas TIC dificulta la

protección integral de la infraestructura tecnológica y aumenta la exposición frente a ataques o pérdidas de información", evidenciando la importancia de contar con políticas y estructuras organizadas para garantizar una gestión eficiente de la seguridad digital en las entidades territoriales.

Al analizar la situación de seguridad digital en entidades públicas, es posible identificar desafíos comunes que afectan especialmente a los gobiernos territoriales con menores capacidades operativas, un ejemplo de ello se encuentra en el estudio de Holguín Carvajal, el cual se centra en las vulnerabilidades presentes en infraestructuras tecnológicas de alcaldías de sexta categoría en Colombia. Su investigación revela que muchas de estas entidades enfrentan limitaciones significativas en cuanto a recursos técnicos, disponibilidad de personal especializado y actualización de normativas internas, estas condiciones generan una alta dependencia de soluciones externas y dificultan el establecimiento de una gestión eficiente y autónoma de la seguridad digital.

Además, luego de revisar el uso de tecnologías emergentes en el sector público, resulta pertinente el trabajo de Padilla (2021), quien exploró el impacto del uso de servicios en la nube en entidades del Estado colombiano. Su análisis advierte que, si bien estas soluciones ofrecen eficiencia y accesibilidad, su adopción sin un marco normativo adecuado puede traer riesgos significativos, especialmente en lo que respecta a la confidencialidad y al control sobre los datos institucionales. Estas conclusiones subrayan la necesidad de acompañar los procesos de migración tecnológica con políticas y herramientas de regulación y seguimiento.

Por otro lado, en el plano normativo la orientación técnica y estratégica ha jugado un papel fundamental en los procesos de transformación digital de las entidades públicas, en este contexto, los documentos elaborados por el Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC) se han consolidado como referentes clave para guiar proyectos de modernización. Instrumentos como la Guía de Seguridad en la Nube y la Matriz de Riesgos de

Seguridad de la Información han sido adoptados por diferentes instituciones como insumos técnicos esenciales para el diseño e implementación de políticas de seguridad adaptadas a las necesidades y condiciones particulares de cada entidad.

Marco conceptual

Para comprender los fundamentos que respaldan la solución propuesta en este proyecto, es importante presentar de manera general las normas y conceptos que guían la administración segura de los servicios en la nube de la alcaldía de Fusagasugá.

Seguridad de la información

La seguridad de la información es un componente importante en toda organización ya que permite proteger los datos frente a accesos no autorizados, alteraciones o pérdidas. De acuerdo con el Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC), la seguridad digital debe garantizar la confidencialidad, integridad y disponibilidad de la información, asegurando que esté accesible solo para quienes están autorizados, que se mantenga sin alteraciones indebidas y que esté disponible cuando se requiera. A partir de la seguridad se estructuran los modelos de gestión y protección de la información en contextos públicos y privados.

Gestión de la seguridad de la información

La gestión de la seguridad de la información es la aplicación sistemática de políticas, procedimientos y controles orientados a proteger los activos de información frente a amenazas internas o externas; de este modo, el Consejo Nacional de Política Económica y Social (Departamento Nacional de Planeación, 2020, CONPES 3995) señala que la gestión de la seguridad digital debe integrarse en todos los niveles de la organización, facilitando la identificación, evaluación y tratamiento de riesgos de manera estructurada. Para lo cual se

requiere tener responsabilidades definidas, un monitoreo constante y mecanismos de mejora continua, para trabajar de la mano con los estándares internacionales.

Además, la gestión de la seguridad de la información tiene como objetivo proteger los activos informáticos frente a riesgos que puedan afectar su confidencialidad, integridad o disponibilidad (ICONTEC, 2022).

- **Confidencialidad: "**Propiedad de la información que la hace no disponible o sea divulgada a individuos, entidades o procesos no autorizados" (Departamento Administrativo de la Función Pública, 2022).
- **Integridad: "**Propiedad de exactitud y completitud" (Departamento Administrativo de la Función Pública, 2022).
- **Disponibilidad: "**Propiedad de ser accesible y utilizable a demanda por una entidad" (Departamento Administrativo de la Función Pública, 2022).

Sistema de gestión de la seguridad de la información (SGSI)

El Sistema de Gestión de la Seguridad de la Información (SGSI) es un modelo estructurado que integra políticas, procedimientos, recursos y procesos interrelacionados, para preservar la información en términos de confidencialidad, integridad y disponibilidad, aplicando un proceso de gestión de riesgos continuo y dando confianza a las partes interesadas (ICONTEC, 2022). Este sistema está orientado a gestionar los riesgos que afectan la confidencialidad, integridad y disponibilidad de la información, mediante la definición de controles adaptados al contexto de la entidad.

Nube (Cloud Computing)

La computación en la nube o cloud computing es un modelo que permite el acceso a un conjunto compartido de recursos tecnológicos como servidores, almacenamiento, redes y

aplicaciones, a través de internet, este modelo facilita la escalabilidad, flexibilidad y disponibilidad de los servicios, sin necesidad de mantener una infraestructura física local.

Según Padilla (2021) la computación en la nube ha permitido a los actores del Estado colombiano optimizar el uso de sus recursos tecnológicos, mejorar la prestación de servicios y avanzar en sus procesos de transformación digital. Este modelo no solo reduce costos operativos, sino que también mejora la capacidad de respuesta frente a nuevas demandas tecnológicas.

Tipos de servicios en la nube

Dentro del modelo de computación en la nube se encuentran diferentes tipos de servicios que permiten a las organizaciones elegir la opción más conveniente de acuerdo con sus necesidades, entre ellas podemos encontrar:

- **Infraestructura como Servicio (IaaS):** Brinda a las organizaciones la posibilidad de usar recursos como servidores, almacenamiento y redes a través de internet, sin necesidad de contar con infraestructura física propia. De acuerdo con Padilla (2021), esta modalidad es útil para las entidades que buscan modernizar su infraestructura tecnológica sin realizar inversiones en hardware, ya que los recursos gestionados son responsabilidad del proveedor, de esta manera las organizaciones se enfocan principalmente en su misión. Cabe resaltar que el esquema de pago es el uso de los recursos lo que favorece el control de los costos operativos siendo eficiente desde el ámbito financiero.
- **Plataforma como Servicio (PaaS):** Es una solución tecnológica que simplifica el trabajo de los desarrolladores ya que brinda entornos especializados para creación, prueba y despliegue de aplicaciones sin que sea necesario realizar la gestión de servidores o sistemas operativos; de igual manera, se pueden utilizar contenedores,

bases de datos y servicios de automatización que ayudan a que los procesos de desarrollo sean más agiles.

- **Software como Servicio (SaaS):** Permite a los usuarios acceder a aplicaciones a través de internet sin instalación local, lo que facilita su uso desde cualquier dispositivo conectado. Además, Padilla (2021) considera que SaaS es ideal para entidades que requieren soluciones accesibles, seguras y listas para su uso inmediato. Este modelo es más práctico ya que se puede utilizar desde cualquier dispositivo con conexión a internet.

Gestión de riesgos en seguridad de la información

La gestión de riesgos en seguridad de la información es definida por MinTIC como el proceso de identificación, análisis y tratamiento de los riesgos que puedan afectar la información de la entidad. Es un proceso sistemático que permite identificar, evaluar, tratar y monitorear los riesgos que puedan afectar los activos de información de una organización. El objetivo es disminuir las posibles amenazas que comprometan la confidencialidad, integridad o disponibilidad de la información, por medio del uso de controles apropiados y estrategias de mitigación.

Matriz de riesgos: En el proceso de gestión de riesgos, la matriz de riesgos es una herramienta importante debido a que permite visualizar, clasificar y priorizar los riesgos en función de su nivel de impacto y la probabilidad de ocurrencia. De acuerdo con el Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC), su utilización facilita la toma de decisiones en materia de seguridad de la información ya que aporta un enfoque estructurado para identificar y gestionar amenazas de manera dinámica.

Amenaza: Una amenaza es definida como cualquier evento potencial que puede causar daño a los activos de información de una organización. Como señala el Ministerio de

Tecnologías de la Información y las Comunicaciones (MINTIC), este tipo de eventos puede ser intencional como un ataque cibernético dirigido o accidental, como una falla técnica o un error humano, ambos con la capacidad de comprometer la confidencialidad, integridad o disponibilidad de la información.

Vulnerabilidad: La vulnerabilidad es una debilidad que presentan los sistemas, procedimientos o configuraciones que pueden ser explotadas por una amenaza para comprometer la integridad, confidencialidad o disponibilidad de los activos de información. El Ministerio de Tecnologías de la Información y las Comunicaciones (MINTIC) resalta que la existencia de vulnerabilidades incrementa de manera significativa la probabilidad de que ocurra un incidente de seguridad, afectando la estabilidad y confiabilidad de los servicios institucionales.

Riesgo: El riesgo se define como la combinación de una amenaza y una vulnerabilidad que al materializarse puede comprometer la confidencialidad, integridad o disponibilidad de los activos de información (ICONTEC, 2022); la probabilidad del impacto exige a las organizaciones implementar mecanismos de control para mitigar el riesgo y proteger la infraestructura tecnológica.

Marco normativo

Para el desarrollo de este proyecto se tuvo en cuenta las disposiciones legales, estándares internacionales y políticas públicas que manejan la seguridad de la información y la transformación digital en Colombia, estas normas proporcionan los lineamientos para garantizar una gestión responsable y segura de los servicios tecnológicos en entornos en la nube dentro de la entidad.

ISO/IEC 27001 – Sistema de Gestión de Seguridad de la Información (SGSI):

La norma ISO/IEC 27001:2022 establece los requisitos para implementar, mantener y mejorar un Sistema de Gestión de Seguridad de la Información (SGSI), para proteger la

confidencialidad, integridad y disponibilidad de la información en las organizaciones (ICONTEC, 2022). De esta manera, el estándar propone aplicar controles de seguridad acordes al contexto institucional, gestionando los riesgos de forma planificada y estructurada.

ISO/IEC 27002:2022 – Controles de Seguridad de la Información:

Esta norma proporciona una guía para la implementación de controles de seguridad de la información. Establece buenas prácticas para la protección de activos de información y el fortalecimiento de la resiliencia digital. Según la norma, “los controles se seleccionan y aplican para cumplir con los requisitos identificados a través del tratamiento del riesgo de seguridad de la información” (ICONTEC, 2022).

Decreto 767 de 2022 – Política de Gobierno Digital:

Este decreto establece la política de gobierno digital como “el uso y aprovechamiento de las Tecnologías de la Información y las Comunicaciones, con el objetivo de impactar positivamente la calidad de vida de los ciudadanos y, en general, los habitantes del territorio nacional y la competitividad del país” (República de Colombia, 2022, Decreto 767).

Decreto 1263 de 2022 – Lineamientos de Transformación Digital Pública:

El decreto 1263 de 2022 establece que el objetivo principal es “establecer lineamientos y estándares para la Transformación Digita de la Administración Pública en el marco de la Política de Gobierno Digital” (República de Colombia, 2022, Decreto 1263). Además, también tiene el propósito de impulsar la automatización, digitalización y adopción de tecnologías emergentes en los procesos institucionales.

Ley 1581 de 2012 – Protección de Datos Personales:

Norma que regula el tratamiento de datos personales en Colombia. Establece principios fundamentales como la legalidad, finalidad, libertad, veracidad, seguridad y confidencialidad. En su artículo 4°, establece que el tratamiento de datos personales debe obedecer a una

finalidad legítima, la cual debe ser informada al titular. Esta ley es especialmente relevante en proyectos donde se gestionan datos sensibles a través de plataformas en la nube.

CONPES 3854 de 2016 – Política Nacional de Seguridad Digital:

Este documento del Consejo Nacional de Política Económica y Social (CONPES) establece la hoja de ruta para fortalecer la seguridad digital del país. Define acciones para proteger los activos de información del Estado, promover una cultura de seguridad digital y mejorar la capacidad de respuesta frente a incidentes. Según el CONPES, “la seguridad digital es una condición necesaria para el desarrollo económico y social del país, ya que genera confianza en el uso y aprovechamiento de las TIC por parte del Estado, las empresas y los ciudadanos” (Departamento Nacional de Planeación, 2020, CONPES 3854).

Capítulo 3. Diseño metodológico

Para el desarrollo del proyecto se adoptó la metodología Deming basada en la calidad de los procesos, orientada a generar soluciones prácticas frente a los problemas identificados en la infraestructura tecnológica de la alcaldía de Fusagasugá. Según Duarte Caviedes (2018), "la metodología Deming es eficaz para identificar áreas de mejora continua y aplicar soluciones que optimicen tanto los procesos operativos como la gestión de riesgos" (Duarte Caviedes, 2018). Por ende, esta metodología permite comprender el contexto institucional, analizar los riesgos en los servicios en la nube y proponer mejoras que fortalezcan la seguridad de la información de la entidad.

Como complemento a la estrategia de mejora continua, se aplicó el ciclo PHVA (Planear – Hacer – Verificar – Actuar), como señala Carvajal Hurtado (2022), "el ciclo PHVA es clave para estructurar cualquier proyecto de mejora continua, permitiendo evaluar constantemente los procesos y realizar ajustes necesarios para asegurar su efectividad" (Carvajal Hurtado, 2022). Esta herramienta permitió estructurar el trabajo en fases, se inició con el diagnóstico del estado actual de los servicios en la nube de la alcaldía de Fusagasugá (planear), se realizó el escaneo de vulnerabilidades con Nmap (hacer), se continuó con la documentación de procedimientos y configuración de controles para mitigar los riesgos de la entidad (verificar) y finalmente se formularon recomendaciones para garantizar la continuidad y sostenibilidad de las mejoras propuestas al equipo de seguridad de la oficina TIC y transformación digital (actuar).

Durante el proceso, se hizo uso de la Guía para la Gestión del Riesgo de la Función Pública la cual se ha consolidado como una herramienta esencial en el sector público colombiano para estructurar políticas de gestión del riesgo (Departamento Administrativo de la Función Pública2022). Esta guía sirvió como referencia para identificar amenazas, evaluar el impacto de estas y priorizar acciones de mitigación, lo que permitió construir una visión de los

factores de riesgo existentes, su nivel de criticidad y las oportunidades de mejora que podían ser abordadas de forma técnica y estructurada.

A su vez, se tomaron en cuenta los lineamientos establecidos en la norma ISO/IEC 27001:2022, que orienta la implementación de controles de seguridad para proteger la confidencialidad, integridad y disponibilidad de la información. La ISO/IEC 27001:2022 proporciona una estructura para la gestión de riesgos tecnológicos y la protección de los activos de información, como lo señala Mora Guamán (2022), quien destaca la relevancia de aplicar estándares internacionales en entidades gubernamentales para minimizar los riesgos tecnológicos. Sin embargo, aunque la entidad no cuenta con la certificación oficial se reconoció la importancia de adaptar buenas prácticas internacionales a su contexto local, buscando fortalecer la gestión de la seguridad desde un enfoque preventivo.

Capítulo 4. Desarrollo del proyecto

En el presente capítulo se describe el trabajo realizado durante el desarrollo del proyecto, para comprender la secuencia lógica de las tareas y los tiempos de ejecución de cada una de ellas, puede consultar Apéndice. Cronograma de actividades.

Descripción de la actividad principal de la pasantía

La actividad principal desarrollada durante la pasantía estuvo orientada a diagnosticar la seguridad y la gestión de los servicios en la nube de la alcaldía de Fusagasugá con el propósito de aportar a la mejora continua de la infraestructura tecnológica institucional, este objetivo se abordó desde un enfoque preventivo, técnico y estratégico, realizando la identificación de riesgos y vulnerabilidades, y proponiendo acciones para mitigar posibles amenazas.

El trabajo realizado se centró en la formulación de una guía de buenas prácticas en la gestión de servicios en la nube, basada en los hallazgos de un diagnóstico técnico, el análisis de riesgos y las recomendaciones de normas internacionales como la ISO/IEC 27001 y 27002. Según la ISO/IEC 27001:2022, "la implementación de un sistema de gestión de seguridad de la información permite identificar y mitigar los riesgos que afectan la confidencialidad, integridad y disponibilidad de los activos de información" (ICONTEC, 2022). Este documento busca servir como referencia para el equipo técnico de la entidad, aportando lineamientos claves para una administración más segura.

Además, la pasantía permitió aplicar conocimientos en gestión del riesgo, seguridad de la información y normativas TIC dentro de un contexto real, generando productos que pueden contribuir a la toma de decisiones y a la sostenibilidad tecnológica de la organización.

Descripción de las actividades realizadas durante la pasantía

Durante el período de pasantía en la alcaldía de Fusagasugá se desarrollaron diversas actividades orientadas a evaluar, documentar y proponer mejoras para la gestión de los servicios en la nube de la entidad, estas actividades respondieron a una necesidad real de

mejorar la seguridad y la eficiencia de la infraestructura tecnológica y se ejecutaron de manera progresiva, aplicando metodologías estructuradas como el ciclo PHVA y los lineamientos establecidos por la normativa vigente en seguridad digital. Según Duarte Caviedes (2018), la aplicación del ciclo PHVA (Planear, Hacer, Verificar, Actuar) proporciona una estructura continua de mejora que permite evaluar y ajustar los procesos a medida que avanzan, garantizando resultados más efectivos y sostenibles.

En la etapa inicial del proyecto se desarrolló el diagnóstico del estado actual de los servicios en la nube en el que se recopiló información importante sobre la distribución de los componentes del entorno computacional en la nube, su configuración, uso y nivel de exposición a vulnerabilidades, este análisis permitió plantear las acciones de mejora que se recomienda en las siguientes fases que la entidad implemente. De acuerdo con Mora Guamán (2022), el análisis inicial de la infraestructura es importante para establecer una base sobre la cual construir mejoras de seguridad. Este diagnóstico también sirvió para que la entidad identificará las áreas de riesgo que necesitaban ser tratadas para reducir la brecha y garantizar la protección de la información, salvaguardando los datos de los ciudadanos.

Posteriormente, se diseñó el diagrama de la topología de los servicios en la nube un recurso visual que ilustra de forma esquemática la arquitectura tecnológica de la alcaldía, para facilitar la identificación de los puntos que presentan vulnerabilidades, pero no representa la distribución real de los recursos en la nube para garantizar la seguridad y confidencialidad de la infraestructura de la entidad.

Tomando en cuenta esa información, se realizó un diagnóstico inicial de la instancia_12 del servidor en la nube de la alcaldía de Fusagasugá, evaluando la seguridad en la plataforma, configuraciones activas y posibles brechas en los servicios prestados, permitiendo establecer prioridades y orientar las acciones hacia los aspectos sensibles que presentaban un riesgo en la seguridad de la información. En este proceso, se aplicaron los principios de gestión de

riesgos de la ISO/IEC 27001:2022, que recomienda evaluar los riesgos en función de su impacto y probabilidad de ocurrencia.

A partir de los hallazgos en el diagnóstico de la instancia_12, se eleaboró una matriz de riesgos de seguridad de la información en la que se clasificaron y priorizaron los riesgos identificados tomando como referencia criterios como el impacto, la probabilidad de ocurrencia y la criticidad, este documento fue acompañado por un mapa de calor, que ofreció una representación visual para identificar áreas críticas dentro del entorno cloud de la entidad que no interrumpía el desarrollo de las actividades pero al igual si representaba un riesgo en los servicios.

En el área de Redes y Seguridad, se documentaron dos procedimientos importantes en el fortalecimiento de la seguridad de la alcaldía de Fusagasugá. El primero describe el proceso paso a paso de la implementación de certificados SSL y el otro aborda garantiza la recuperación de la información ante posibles incidentes al realizar copias de seguridad. Ambos procedimientos son aseguran la confidencialidad, integridad y disponibilidad de la información, como lo establece la ISO/IEC 27002:2022.

Como resultado luego de realizar todo el proceso, se elaboró una guía de buenas prácticas en la gestión de servicios en la nube, basada en los hallazgos del diagnóstico, los riesgos identificados y las recomendaciones de normas como la ISO/IEC 27001:2022 y 27002:2022. Esta guía tiene como objetivo servir de referencia para el personal técnico de la entidad, promoviendo una gestión más segura, estructurada y eficiente de su infraestructura en la nube.

Análisis de los problemas y desafíos enfrentados

Entre los desafíos que se presentaron durante el desarrollo del proyecto se encuentra el acceso limitado a la documentación interna de la alcaldía de Fusagasugá. La información pública está disponible, sin embargo, el acceso a documentos con información sensible es

restringida ya que puede comprometer la confidencialidad de la entidad, lo que hizo más complejo el trabajo inicial, retrasando el desarrollo del diagnóstico de la infraestructura tecnológica al no tener todos los datos.

Además, como estudiante, la gestión de seguridad de la información en la nube era un tema nuevo lo que presentó un desafío adicional. A pesar de contar con el acompañamiento y la asesoría del equipo técnico de la alcaldía y el director interno, el aprendizaje continuo sobre las normas internacionales y la gestión de riesgos en un contexto gubernamental fue un reto ya que estos conceptos requerían una implementación práctica adaptada a la realidad de la alcaldía y sus recursos.

Por último, la falta de procedimientos estandarizados y la ausencia de políticas claras para gestionar los servicios en la nube dificultaron la estructuración del proyecto ya que no existían lineamientos definidos que guiaran las acciones a tomar para garantizar una gestión segura y eficiente de los recursos tecnológicos. La ausencia de un marco normativo interno dificultó la identificación de buenas prácticas a seguir y requirió la adopción de marcos normativos internacionales como la ISO/IEC 27001:2022, para poder garantizar la protección de los servicios en la nube en la alcaldía de Fusagasugá.

Soluciones implementadas

Se trabajó de manera colaborativa con el equipo de redes y seguridad de la alcaldía de Fusagasugá en la oficina de las TIC y la transformación digital, lo que permitió obtener la información necesaria para el desarrollo de las actividades dentro de los límites establecidos por las normativas internas. Gracias a esta colaboración, fue posible realizar el análisis de la infraestructura tecnológica con los datos disponibles lo que permitió realizar de manera adecuada el diagnóstico del estado actual de los servicios en la nube.

Además, se implementó un proceso continuo de autoformación y aprendizaje práctico con el acompañamiento del equipo de la oficina TIC de la alcaldía y el director interno, gestor

de conocimiento de la Universidad de Cundinamarca. Comprender la gestión de la seguridad de la información en la nube, las normativas internacionales, como la ISO/IEC 27001:2022, fueron una guía importante en la toma de decisiones del proyecto siempre buscando alinear las mejores prácticas con la realidad tecnológica de la entidad, lo que permitió superar el desafío de adaptar los conceptos globales al contexto local, asegurando que la gestión de la seguridad estuviera acorde con los objetivos del proyecto siendo alcanzables en el tiempo propuesto.

Con respecto a la falta de procedimientos estandarizados, se documentaron procedimientos internos para la gestión de los servicios en la nube de la alcaldía de Fusagasugá, estos procedimientos se basaron en las normas ISO/IEC 27001:2022 e ISO/IEC 27002:2022 adaptadas a las necesidades de la entidad para proteger la información y garantizar la seguridad en los servicios. La guía de buenas prácticas desarrollada se convirtió en una referencia importante para el equipo técnico contribuyendo a una gestión segura y organizada de los servicios en la nube.

Finalmente, para garantizar la continuidad operativa y proteger la infraestructura tecnológica de la alcaldía de Fusagasugá a largo plazo, se documentaron procedimientos clave como la configuración de copias de seguridad y la instalación de certificados SSL, estas acciones aseguraron la protección de los datos y la disponibilidad continua de los servicios.

Fases de la metodología

Fase 1: Planear

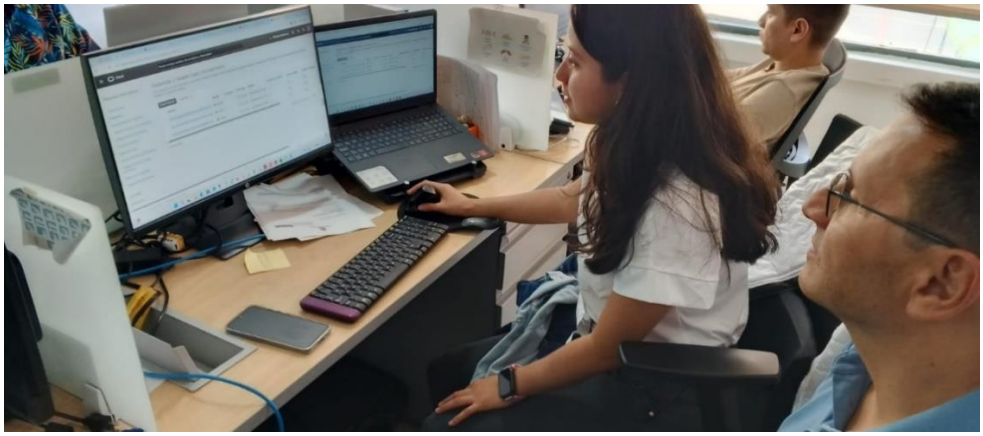
En esta fase se realizó el diagnóstico inicial en la alcaldía de Fusagasugá con el objetivo de comprender el funcionamiento general de la infraestructura tecnológica en la nube que soporta los servicios institucionales. El proceso comenzó con una etapa de levantamiento de información, en la cual se consultaron fuentes técnicas y bibliográficas vinculadas a la operación de servicios en entornos de computación en la nube. De acuerdo con lo expresado por Carvajal Hurtado (2022), la identificación del entorno técnico desde el inicio de un proyecto

es clave para establecer una línea base sobre la cual construir un sistema de gestión seguro y estructurado. En este sentido, el análisis documental permitió enmarcar la revisión desde una perspectiva metodológica y fortalecer la comprensión del modelo adoptado por la entidad.

La recolección de información se desarrolló con el acompañamiento del personal encargado de la gestión tecnológica, adscrito a la Oficina de las TIC y la Transformación Digital. Gracias a este acompañamiento fue posible acceder a información relacionada con la configuración, distribución y administración de los servicios actuales de la entidad. Esta aproximación directa coincide con lo propuesto por Pulido & Mantilla (2016), quienes argumentan que el diagnóstico situacional es un paso indispensable para caracterizar los activos tecnológicos y sus condiciones operativas reales.

Figura 1

Interacción con la plataforma de Oracle Cloud para acceder a la configuración de los servicios de la entidad



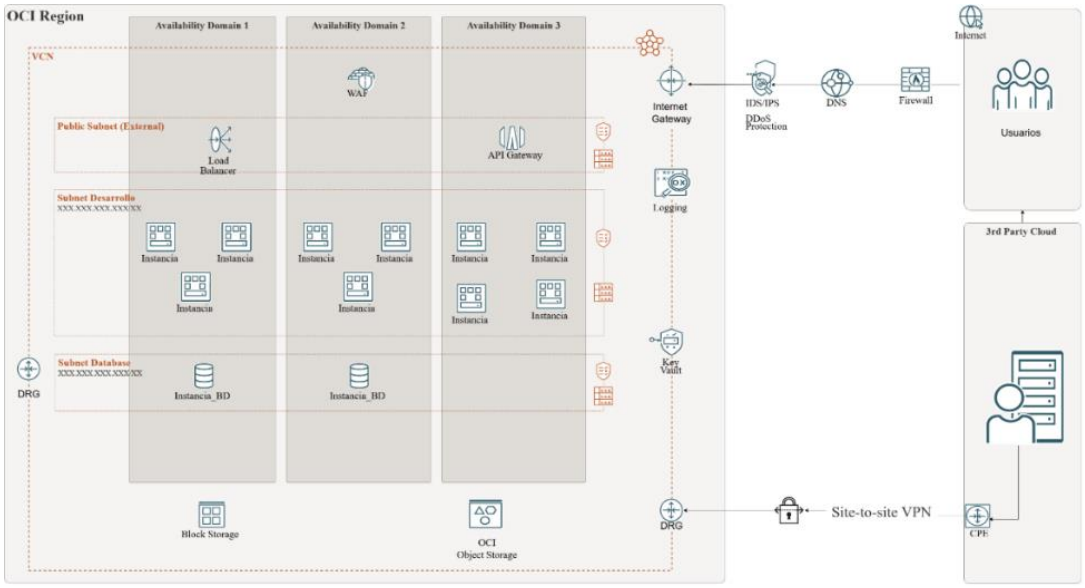
Nota. La figura ilustra el proceso de recolección de información, donde se muestra el trabajo conjunto con el personal de la Oficina de las TIC y la Transformación Digital para el diagnóstico de la infraestructura tecnológica en la nube.

Está exploración facilitó la elaboración de un diagrama de la arquitectura de la nube. No obstante, debido a políticas de confidencialidad institucional, en la Figura 1 se ilustró de manera general la estructura lógica del entorno cloud sin exponer información sensible. Desde la

perspectiva metodológica descrita por Mora Guamán (2022), la representación gráfica de la arquitectura técnica aporta insumos útiles para predecir medidas de seguridad según el nivel de exposición de los recursos. Es así como la representación esquemática de la nube permite identificar componentes visibles del sistema y delimita su estructura sin comprometer detalles críticos de la infraestructura de la entidad.

Figura 2

Representación general de la arquitectura lógica del entorno cloud



Nota. La figura ilustra de manera general la distribución de servicios de un entorno cloud y los componentes de seguridad implementados para proteger la información institucional.

La figura 2 muestra la arquitectura de la nube en la que se evidencia una infraestructura distribuida del diseño lógico orientado a la seguridad de los servicios digitales de la entidad. Al estar organizado por dominios de disponibilidad permite que los recursos estén segmentados en diferentes zonas físicas lo que refuerza la tolerancia a fallos y favorece la continuidad del servicio ante posibles contingencias en las plataformas de la entidad.

En la parte superior de la estructura se observa una red virtual en la nube (VCN), la cual se subdivide en diferentes subredes que cumplen funciones específicas dentro del entorno.

Entre ellas se encuentra la subred pública que aloja componentes que se comunican con el exterior permitiendo administrar de forma adecuada el tráfico de entrada, distribuyendo las solicitudes hacía instancias internas y protegiendo al mismo tiempo la infraestructura central. Esta segmentación funcional está en consonancia con el modelo propuesto por Osorio Corredor (2018), quien destaca que una arquitectura lógica bien definida contribuye a una mejor gestión de riesgos operativos y a la aplicación efectiva de controles.

Por su parte, la subred de desarrollo concentra el entorno de instancias virtuales donde residen las aplicaciones y servicios que operan en la institución. Esta segmentación facilita la administración de cargas de trabajo y la escalabilidad de los recursos conforme a las necesidades técnicas de cada proceso. En paralelo, la subred de base de datos agrupa instancias especializadas para el almacenamiento estructurado de la información, configuradas para soportar los sistemas de registro y procesamiento de datos institucionales de forma segura. Respondiendo a los principios establecidos en la ISO/IEC 27001:2022, que destaca la necesidad de identificar y proteger los activos de información según su criticidad y uso.

En cuanto a los componentes de seguridad, se evidencia la incorporación de herramientas como el firewall, los sistemas de detección y prevención de intrusos (IDS/IPS), la protección contra ataques distribuidos de denegación de servicios (DDoS) y el control mediante claves criptográficas almacenadas en una bóveda especializada (Key Vault); Mora Guamán (2022) resalta que la implementación de mecanismos de seguridad en capas, acompañados de segmentación lógica, representa una práctica esencial para mantener el control sobre entornos cloud dinámicos. Estas medidas permiten gestionar el riesgo de acceso no autorizado y garantizar la confidencialidad e integridad de la información procesada, en cumplimiento con los principios de seguridad establecidos por estándares como la ISO/IEC 27001:2022.

En este contexto, el entorno dispone de soluciones de almacenamiento en bloque y de objetos que permiten organizar los datos según su naturaleza, frecuencia de acceso y tiempo

de retención, lo que lo hace relevante en la administración del ciclo de vida de la información, considerando que, de acuerdo con las políticas internas de la alcaldía de Fusagasugá, los documentos deben mantenerse durante seis años en archivo activo antes de ser almacenados en un repositorio de almacenamiento pasivo. De este modo, la configuración descrita permite que las instancias respondan a las necesidades técnicas de cada proceso, conforme a las políticas de gestión del ciclo de vida de la información, reafirmando lo propuesto por Carvajal Hurtado (2022), quien destaca que la adecuada gestión documental en entornos digitales fortalece la trazabilidad y la seguridad de la información institucional.

A continuación, se presenta el estado actual de las instancias activas en la plataforma en la nube, en términos de capacidad de memoria, uso de CPU y estado operativo, lo que refuerza el análisis realizado sobre la infraestructura observada.

Figura 3

Estado actual de las instancias activas en la plataforma en la nube

Nombre	Memoria	CPU	Estado actual
Instancia_01	64	4	En ejecución
Instancia_02	16	2	En ejecución
Instancia_03	16	4	En ejecución
Instancia_04	64	4	En ejecución
Instancia_05	16	1	En ejecución
Instancia_06	4	1	En ejecución
Instancia_07	4	1	En ejecución
Instancia_08	8	1	En ejecución
Instancia_09	4	1	Parado
Instancia_10	8	2	Parado
Instancia_11	8	2	Parado
Instancia_12	16	4	En ejecución

Nota. La figura presenta el estado actual de las instancias activas, detallando la relación de la memoria, el uso de la CPU y el estado operativo de las instancias en la plataforma en la nube.

Como se puede observar en la figura 3, la configuración y el estado actual de las instancias muestran que cada componente cumple un papel especifico en el entorno digital de la alcaldía de Fusagasugá. Las instancias activas tienen un rol importante en el funcionamiento

diario de los procesos institucionales ya que alojan aplicaciones críticas que dan soporte a la gestión administrativa y la interacción con la ciudadanía; estos servicios permiten centralizar información, automatizar procesos y ofrecer plataformas accesibles que facilitan la prestación de servicios gubernamentales en línea.

Respecto a la distribución de memoria y capacidad de procesamiento (CPU) de las instancias que se alojan en el entorno de computación en la nube de la entidad, en la Figura 3 se evidencian los resultados que indican que las instancias con mayores recursos están destinadas a plataformas de alta complejidad y demanda, como sistemas de información geográfica, entornos educativos virtuales y soluciones de interoperabilidad, que son gestionadas a diario por entidades públicas. Esta organización de los recursos refleja una planificación coherente con las mejores prácticas recomendadas por Osorio Corredor (2018), quien destaca la importancia de distribuir adecuadamente los recursos en infraestructuras en la nube para satisfacer las necesidades específicas de cada sistema.

Por otra parte, algunas instancias presentan configuraciones más ligeras ya que soportan aplicaciones que no requieren alta disponibilidad de memoria o procesamiento constante. Porque son instancias que se encargan de servicios más específicos, informativos o de soporte técnico, debido a que el consumo de recursos es menor. Este enfoque coincide con lo indicado por Padilla (2021), quien señala que la escalabilidad y la flexibilidad en la asignación de recursos son esenciales para maximizar el rendimiento y asegurar la disponibilidad de los servicios. Además, esta diferencia de capacidades permite mantener un equilibrio entre el rendimiento y el uso de la infraestructura.

En cuanto a las instancias que se encuentran en estado inactivo, estas también forman parte del modelo de gestión en la nube, ya que garantiza la posibilidad de escalar rápidamente ante un aumento en la demanda de servicios o en caso de contingencia; Osorio Corredor (2018) señala que disponer de recursos previamente aprovisionados permite mejorar la

resiliencia institucional y anticiparse a escenarios de variabilidad operativa sin comprometer la calidad del servicio. Esta estrategia de disponibilidad latente permite a la entidad adaptarse con agilidad a nuevos requerimientos sin necesidad de aprovisionar infraestructura desde cero, lo cual refuerza la capacidad de respuesta y la sostenibilidad técnica en el mediano plazo.

En consecuencia, este diagnóstico brindó una interpretación del entorno tecnológico en la nube de la alcaldía de Fusagasugá aportando evidencia de la situación actual de la infraestructura tecnológica de la entidad, apoyándonos en dicha información, podemos definir medidas concretas para ajustar los recursos al contexto público, garantizando una transición organizada que se ajuste a las demandas cambiantes de la entidad. De igual manera, el conocimiento obtenido facilita la identificación de áreas que requieren mejorar, lo que permite priorizar acciones para asegurar la sostenibilidad y resiliencia del sistema en el futuro.

Asimismo, esta fase permite establecer una ruta para la implementación de mejoras, con un enfoque de adaptación progresiva que considera las capacidades actuales y los objetivos estratégicos de la alcaldía de Fusagasugá. Este proceso de planificación es importante para avanzar de manera correcta hacia las siguientes etapas del proyecto, asegurando que la infraestructura tecnológica sea capaz de anticipar y responder de forma ágil a los desafíos y demandas inherentes a la gestión pública digital, permitiendo a la entidad mantener un servicio continuo y de calidad para la comunidad.

Fase 2: Hacer

Durante esta fase se realizó un diagnóstico para identificar las posibles vulnerabilidades en los servicios en la nube de la alcaldía de Fusagasugá, este análisis se realizó en la Instancia_12. La actividad se desarrolló en un entorno controlado que permitió examinar configuraciones que pudieran implicar riesgos de seguridad en la infraestructura tecnológica de la entidad. Por lo tanto, el resultado de esta revisión sirvió para conocer áreas críticas que

deben ser atendidas en manera prioritaria y fortalecer las decisiones que se tomarán en la entidad para continuar con las siguientes fases del proyecto.

Figura 4

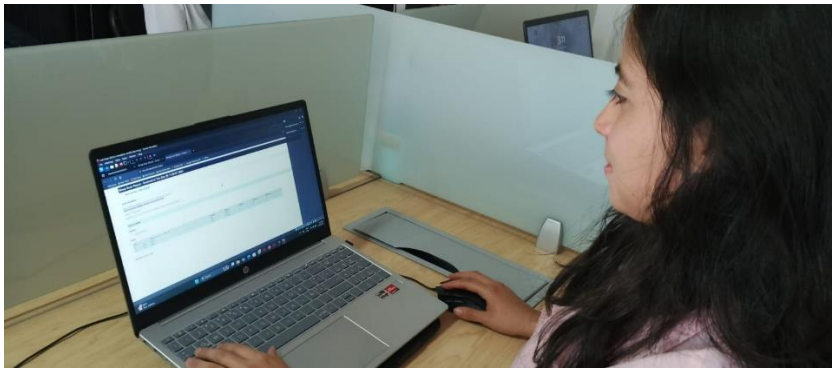
Configuración de la máquina virtual con Kali Linux en VirtualBox

Nota. La figura muestra el entorno de pruebas de seguridad utilizado para realizar el análisis de vulnerabilidades en la infraestructura de la alcaldía de Fusagasugá.

Para la ejecución de este análisis, se utilizó una máquina virtual con el sistema operativo Kali Linux instalada en VirtualBox que permitió crear un entorno autónomo destinado a pruebas de seguridad. Para esto, se empleó Nmap, una herramienta que permitió escanear y detectar servicios, puertos y configuraciones expuestas en la Instancia_12 de la entidad. Está técnica de evaluación sigue las buenas prácticas recomendadas en la Guía No. 12: Seguridad en la nube del Ministerio de Tecnologías de la Información y las Comunicaciones (2016), en la guía de que promueve el uso de herramientas especializadas como parte de un enfoque preventivo en la gestión de vulnerabilidades. Al realizar este proceso de forma continua en las plataformas que aloja la alcaldía en la nube disminuirá el nivel de exposición a riesgos que afecten la confidencialidad, integridad y disponibilidad de la información.

Figura 5

Actividad de ejecución de comandos para la detección de vulnerabilidades



Nota. La figura muestra el desarrollo de la actividad en el proceso de ejecución de scripts en la máquina virtual para detectar vulnerabilidades en la instancia_12 de la alcaldía de Fusagasugá

El análisis se centró en una dirección IP interna correspondiente a la instancia seleccionada. Para realizar la tarea que se evidencia en la Figura 5, se aplicaron diferentes tipos de escaneos que permitieron ver como responden los servicios ante las pruebas de seguridad y facilitó la detección de configuraciones que podrían representar vulnerabilidades dentro del entorno computacional de la entidad. Además, los resultados obtenidos ayudaron a identificar áreas que necesitan ajustes, lo que aporta información importante para reforzar la seguridad de la infraestructura y reducir los riesgos a los que está expuesta la alcaldía de Fusagasugá.

Figura 6

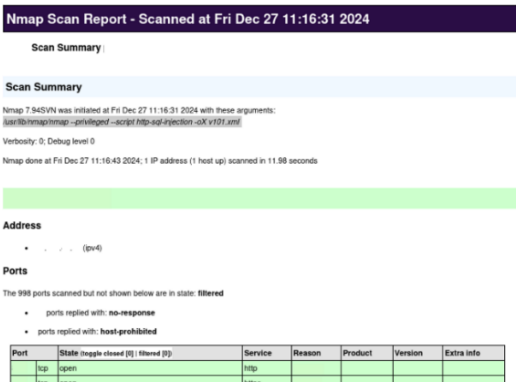
Reporte escaneo de Nmap utilizando el script http-xss

Nota. La figura evidencia el resultado del escaneo realizado con el script http-xss de Nmap, utilizado para identificar vulnerabilidades de Cross-Site Scripting (XSS).

Durante el proceso de escaneo de vulnerabilidades, como se evidencia en la figura 6, se utilizó el script http-xss que se caracteriza por detectar vulnerabilidades de Cross-Site Scripting (XSS). La ejecución de este script permitió observar como el servidor responde ante solicitudes manipuladas, lo que facilitó la identificación de patrones; estos hallazgos sirven para mejorar la sanitización de datos en las aplicaciones web internas y prevenir posibles inyecciones de código malicioso, garantizando la seguridad en la infraestructura tecnológica de la alcaldía de Fusagasugá.

Figura 7

Reporte escaneo de Nmap utilizando el script http-sql-injection



Nota. La figura presenta el resultado del escaneo realizado con el script http-sql-injection de Nmap que permite detectar vulnerabilidades de inyección SQL en aplicaciones web.

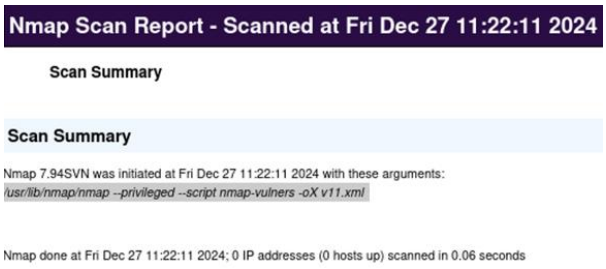
En la figura 7 se muestra el uso del script http-sql-injection, que permitió detectar posibles vulnerabilidades de inyección SQL en aplicaciones web, para identificar si había algún riesgo en la instancia_12 con respecto a este tipo de vulnerabilidades.

Según Carvajal Hurtado (2022), una validación adecuada de los parámetros es necesaria para evitar vulnerabilidades que puedan comprometer la seguridad de los sistemas. Además, es importante realizar pruebas de seguridad de manera continua durante todo el ciclo de vida de la aplicación ya que las vulnerabilidades pueden surgir incluso después de la

implementación inicial, debido a actualizaciones o cambios en el entorno operativo de las plataformas de la entidad.

Figura 8

Reporte de escaneo de Nmap utilizando el script nmap-vulners



Nota. La figura presenta el resultado del escaneo realizado con el script nmap-vulners de Nmap, que se utiliza para revisar vulnerabilidades conocidas (CVE) asociadas a los servicios detectados en el host.

También se empleó el script nmap-vulners, como se muestra en la figura 8, esta verificación es coherente con lo establecido en la norma ISO/IEC 27001:2022, que contempla la identificación y tratamiento de vulnerabilidades como parte integral del proceso de seguridad (Carvajal Hurtado, 2022). Además, este script cruza la información obtenida con bases de datos públicas de vulnerabilidades, lo que facilita la identificación de servicios que podrían requerir actualización o refuerzo de seguridad para evitar riesgos conocidos.

Como resultado del escaneo, se detectaron ciertas configuraciones que podrían representar una exposición innecesaria frente agentes maliciosos. Sin embargo, por motivos de seguridad y conforme a los principios de ética profesional, este documento no detalla las vulnerabilidades detectadas, debido que su publicación podría comprometer la integridad de la infraestructura digital de la entidad; Osorio Corredor (2018) plantea que el reconocimiento anticipado de amenazas, a través de metodologías estructuradas, permite a las organizaciones públicas prepararse frente a incidentes sin comprometer la continuidad operativa. Es así como,

en la entidad se deben revisar los escenarios donde se presentan las vulnerabilidades para prevenir riesgos futuros.

El análisis técnico realizado sobre la instancia_12 permitió identificar configuraciones que no afectan la operación actual, pero requieren atención para reducir riesgos en la infraestructura digital de la alcaldía de Fusagasugá. Esta evaluación aportó insumos valiosos para las acciones correctivas que serán planteadas en la fase siguiente del ciclo PHVA. Como advierte Osorio Corredor (2018), anticiparse a las amenazas mediante diagnósticos técnicos oportunos es esencial en la gestión de seguridad en entidades públicas. Este ejercicio reafirma la importancia de mantener una vigilancia continua sobre los servicios en la nube y demuestra que la prevención es una condición necesaria para garantizar la estabilidad institucional en entornos digitales.

Fase 3: Verificar

En esta fase del ciclo Deming, se elaboró una matriz de riesgos que permitió organizar y analizar las principales vulnerabilidades identificadas previamente en la Instancia_12 de la alcaldía de Fusagasugá. Para la construcción de este producto se tomaron seis riesgos como base; los cuales fueron seleccionados por su criticidad y potencial impacto en la seguridad de la información, para su creación se consideraron elementos técnicos y operativos de acuerdo con las recomendaciones de Ministerio de las Tecnologías y las Comunicaciones (MINTIC) sobre la gestión de riesgos en entornos públicos.

Para establecer el nivel de exposición de los activos de información ante las amenazas identificadas, se procedió inicialmente con la determinación de la zona de riesgo inherente, es decir, el riesgo que se presenta antes de aplicar cualquier medida de control. De este modo, el análisis permite visualizar con mayor precisión los escenarios críticos y priorizar acciones correctivas en función de su nivel de impacto y probabilidad, para evaluar la magnitud de un riesgo y un evento en conjunto.

Figura 9

Valoración de la Probabilidad Inherente en el Análisis de Riesgos

PROBABILIDAD INHERENTE		
NIVEL	**FRECUENCIA**	**PROBABILIDAD**
Muy Baja	La actividad que conlleva el riesgo se ejecuta como máximos 2 veces por año	20%
Baja	La actividad que con lleva el riesgo se ejecuta de 3 a 24 veces por año	40%
Media	La actividad que conlleva el riesgo se ejecuta de 24 a 500 veces por año	60%
Alta	La actividad que conlleva el riesgo se ejecuta mínimo 500 veces al año y máximo 5000 veces por año	80%
Muy Alta	La actividad que conlleva el riesgo se ejecuta más de 5000 veces por año	100%

Nota. La figura muestra la valoración de la probabilidad inherente, basada en la frecuencia de los eventos y categorizada con un valor porcentual para facilitar el análisis cuantitativo.

De esta manera, se define la probabilidad inherente como la posibilidad de que un evento de riesgo ocurra cuando no se han implementado controles. Esta variable fue evaluada con base en la frecuencia de ejecución de la actividad relacionada, empleando una escala cualitativa que contempla desde eventos muy poco frecuentes hasta actividades altamente recurrentes; cada nivel fue categorizado con un valor porcentual, lo que facilita su incorporación en el análisis cuantitativo posterior.

Luego de estimar la probabilidad inherente, se evaluó el impacto inherente, que se refiere al alcance de las consecuencias que podría generar la materialización de un riesgo sobre los activos de información y las operaciones que se desarrollan a diario en la entidad. Para ello, se tuvo en cuenta, la afectación económica que representa la medida en salarios mínimos legales mensuales vigentes (SMLMV) y la afectación reputacional que se vincula al grado de exposición pública que generaría el evento, como se presenta en la Figura 13.

Figura 10

Valoración del impacto inherente en el análisis de riesgos

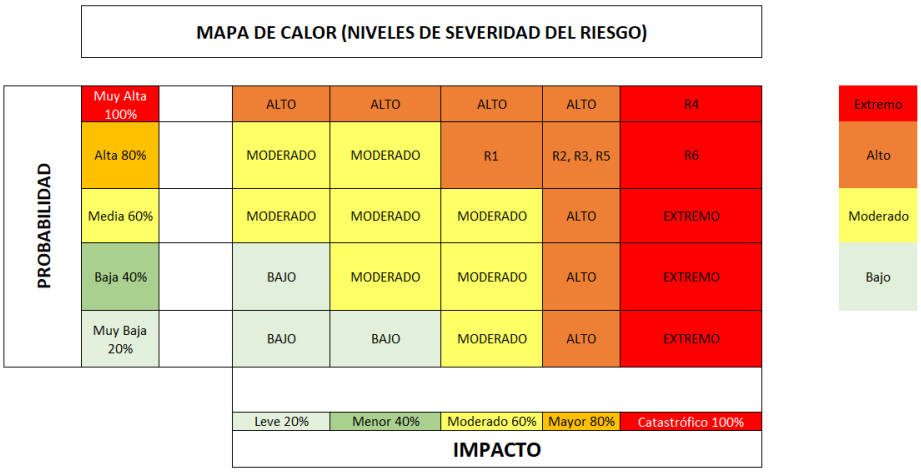
IMPACTO INHERENTE		
NIVEL	**AFECTACIÓN ECONÓMICA**	**REPUTACIONAL**
Leve	Afectación menor a 10 SMLMV	El riesgo afecta la imagen de algún área de la organización.
Menor	Entre 10 y 50 SMLMV	El riesgo afecta la imagen de la entidad internamente, de conocimiento general nivel interno, de junta directiva y accionistas y/o de proveedores.
Moderado	Entre 50 y 100 SMLMV	El riesgo afecta la imagen de la entidad con algunos usuarios de relevancia frente al logro de los objetivos.
Mayor	Entre 100 y 500 SMLMV	El riesgo afecta la imagen de la entidad con efecto publicitario sostenido a nivel de sector administrativo, nivel departamental o municipal.
Catastrófico	Mayor a 500 SMLMV	El riesgo afecta la imagen de la entidad a nivel nacional, con efecto publicitario sostenido a nivel país.

Nota. La figura presenta la valoración del impacto inherente, que considera la afectación económica en (SMLMV) y la afectación reputacional, ayudando a clasificar el impacto potencial de cada riesgo.

Al determinar las características inherentes de cada riesgo, se continuo con la construcción del mapa de calor donde se evidencian los niveles de severidad del riesgo. Esta representación gráfica permite visualizar el grado de exposición que enfrenta cada escenario antes de aplicar medidas de mitigación. Esta herramienta permite priorizar los riesgos en función de su impacto, marcando en rojo los que demandan atención inmediata. De igual manera, el mapa es en un recurso estratégico en la toma de decisiones, porque representa el estado inicial de riesgo de la entidad ante posibles amenazas en la Instancia_12.

Figura 11

Mapa de Calor de los Niveles de Severidad del Riesgo



Nota. La figura presenta el mapa de calor que visualiza el grado de exposición de cada riesgo, facilitando la ubicación de la zona de criticidad y priorizando acciones correctivas según el impacto y la probabilidad estimada.

El diseño del mapa que se presenta en la Figura 14 permitió ubicar cada riesgo dentro de la zona de criticidad, que parte de la relación entre la probabilidad de ocurrencia y el impacto estimado sobre la entidad que está siendo revisada. Los resultados evidencian que el riesgo se posiciona en los niveles alto y extremo, lo que indica una brecha que requiere atención de manera inmediata para que no afecte la seguridad de la información de la entidad. Este comportamiento afirma la necesidad de adoptar medidas correctivas para mitigar posibles afectaciones sobre la infraestructura tecnológica y los procesos institucionales que lleva a cabo la entidad, al igual que la protección de los datos de los usuarios.

Entre los eventos evaluados, el riesgo R4 fue el que resalto dentro del modelo por su nivel de criticidad, al presentar una combinación de alta probabilidad con un impacto crítico sobre la integridad institucional presentando una brecha que necesita ser intervenida para mitigar el riesgo, se deben realizar acciones como la aplicación de controles técnicos y la

definición de planes de contingencia y protocolos de respuesta ante incidentes, como recomienda la norma ISO/IEC 27002:2022.

Además, el riesgo R6 también se ubica en la zona de exposición extrema, a pesar de que su frecuencia de ocurrencia resulta levemente inferior a la del riesgo R4, el impacto asociado sigue siendo considerable lo que justifica su permanencia en una condición crítica que puede afectar a la entidad. Debido a su posible afectación directa sobre la estabilidad operativa de los servicios en la nube, su tratamiento debe considerarse prioritario dentro de los planes orientados al fortalecimiento de la seguridad de la información en la entidad.

El mapa de riesgos permitió observar que todos los eventos analizados se concentran en niveles altos o críticos de exposición. De esta manera, los riesgos R1, R2, R3 y R5 fueron clasificados dentro de una zona de riesgo elevado lo que representa una condición notable para la gestión del riesgo en la entidad. En el caso del riesgo R1, la recurrencia del evento indica que debe ser atendido de forma inmediata para no afectar la seguridad de la entidad. Por otro lado, los riesgos R2, R3 y R5 presentan un perfil que podrían desencadenar efectos visibles en aspectos financieros o en la percepción pública. Frente a este panorama, resulta conveniente establecer mecanismos de control que permitan anticiparse a posibles incidentes y reforzar los procesos existentes sin comprometer la continuidad de los servicios de la entidad.

Controles aplicados

De acuerdo con los resultados obtenidos en la matriz de riesgos de la seguridad de la información en la nube de la alcaldía de Fusagasugá, se estimó la aplicación de controles de seguridad para proteger la información institucional, siguiendo los lineamientos establecidos por la norma ISO/IEC 27001:2022. Esta normativa internacional establece un marco metodológico para abordar la gestión del riesgo de la información, permitiendo ajustar las medidas de protección según las condiciones específicas de cada entorno organizacional o territorial. Entre

sus principios, se destaca la necesidad de incorporar controles técnicos orientados a garantizar la confidencialidad, integridad y disponibilidad de los activos de información (ICONTEC, 2022), principios fundamentales en entornos institucionales con alta dependencia tecnológica.

Cada control es valorado de acuerdo con su eficiencia, teniendo en cuenta que a partir del tipo de control y su modo de implementación, se asigna un porcentaje, que al ser sumado representa el nivel de eficiencia del control frente al riesgo analizado como se muestra en la siguiente figura.

Figura 12

Valoración de la eficiencia del control frente al riesgo

			Peso
EFICIENCIA DEL CONTROL	**TIPO DE CONTROL**	Preventivo	25%
		Detectivo	15%
		Correctivo	10%
	IMPLEMENTACIÓN	Automático	25%
		Manual	10%

Nota. La figura presenta la valoración de la eficiencia del control, que asigna un porcentaje según el tipo de control y su implementación, permitiendo estimar el nivel de contribución de cada control en la reducción del riesgo inherente.

A través de este enfoque fue posible estimar el nivel de aporte que cada control podría tener en la reducción del riesgo inherente. La metodología utilizada se mantuvo en coherencia con las recomendaciones de la norma ISO/IEC 27001:2022, que establece la necesidad de aplicar controles ajustados al grado de exposición identificado en cada escenario. En el contexto de la alcaldía de Fusagasugá, aplicar esta técnica representa una oportunidad para fortalecer la capacidad de la entidad y los recursos disponibles para implementar un modelo de seguridad preventivo que contribuya al desarrollo de la entidad.

A continuación, se presentan los controles que son asignados a cada riesgo para mitigar el riesgo inherente con su respectiva calificación.

Figura 13

Controles recomendados de acuerdo con el riesgo y la calificación del control

CodigoRiesgo	No Control	Control Anexo A	Atributos				
			Tipo	%	Implementación	%	Calificación del Control
R1	1	A.5.16 Gestión de Identidades	Preventivo	25%	Automático	25%	50%
	2	A.5.17 Información de Autenticación	Preventivo	25%	Manual	15%	40%
	3	A.8.5 Autenticación Segura	Correctivo	10%	Automático	25%	35%
R2	1	A.8.8 Gestión de Vulnerabilidades Técnicas	Preventivo	25%	Automático	25%	50%
	2	A.8.9 Gestión de la Configuración	Preventivo	25%	Automático	25%	50%
	3	A.8.16 Actividad de seguimiento	Detectivo	15%	Automático	25%	40%
R3	1	A.8.20 Seguridad de redes	Preventivo	25%	Automático	25%	50%
	2	A.8.16 Actividad de seguiemiento	Detectivo	15%	Automático	25%	40%
	3	A.8.8 Gestión de Vulnerabilidades Técnicas	Detectivo	15%	Manual	15%	30%
R4	1	A.8.20 Seguridad en el desarrollo de Aplicaciones	Preventivo	25%	Manual	15%	40%
	2	A.8.8 Gestión de Vulnerabilidades Técnicas	Correctivo	10%	Automático	25%	35%
R5	1	A.8.16 Actividades de seguimiento	Detectivo	15%	Automático	25%	40%
R6	1	A.8.7 Protección contra malware	Preventivo	25%	Automático	25%	50%

Nota. La figura muestra los controles asignados a cada riesgo y la calificación preliminar, basada en el tipo de acción y la implementación prevista, para mitigar el riesgo inherente en la infraestructura de la alcaldía de Fusagasugá.

La gráfica presentada permite visualizar una estimación del comportamiento esperado de los controles propuestos frente a los riesgos identificados. Aunque estos controles no han sido implementados, se realizó un ejercicio de valoración basado en sus características, como el tipo de acción que representan y la forma en que podrían aplicarse. Tomando en cuenta estos atributos, se proyectó un posible nivel de respuesta de cada control, lo que permite anticipar en qué medida podrían contribuir a mitigar el riesgo si se llegaran a incorporar en el entorno tecnológico de la alcaldía de Fusagasugá.

En general, los controles evaluados alcanzaron una valoración alta, lo que indica que, en caso de ser implementados, tendrían el potencial de ofrecer una respuesta funcional adecuada frente a los riesgos identificados. Varios de estos controles fueron diseñados para operar de forma automatizada lo que favorecería la capacidad de respuesta ante eventos y la reducción de la capa operativa asociada a procesos manuales. Esta estrategia está alineada con los lineamientos del Ministerio de Tecnologías de la Información y las Comunicaciones (MINTIC), así como con los principios establecidos en la norma ISO/IEC 27001:2022, que

promueven la aplicación de controles proporcionales al nivel de riesgo, adaptados al entorno específico de la organización y orientados a garantizar la protección integral de la información.

Una vez valorados los controles propuestos frente a cada riesgo identificado, se procedió a calcular el riesgo residual, es decir, el nivel de exposición que permanece después de aplicar las medidas de mitigación. A diferencia del riesgo inherente, el riesgo residual permite visualizar con mayor precisión el efecto que podrían tener los controles seleccionados en la reducción de la probabilidad y el impacto de cada amenaza sobre la infraestructura tecnológica.

Para estimar el riesgo residual, se calculó la probabilidad residual utilizando la siguiente expresión:

Probabilidad residual = Probabilidad inherente – (Probabilidad inherente × Calificación del control)

El mismo procedimiento se aplica para calcular el impacto residual, con la fórmula:

Impacto residual = Impacto inherente – (Impacto inherente × Calificación del control)

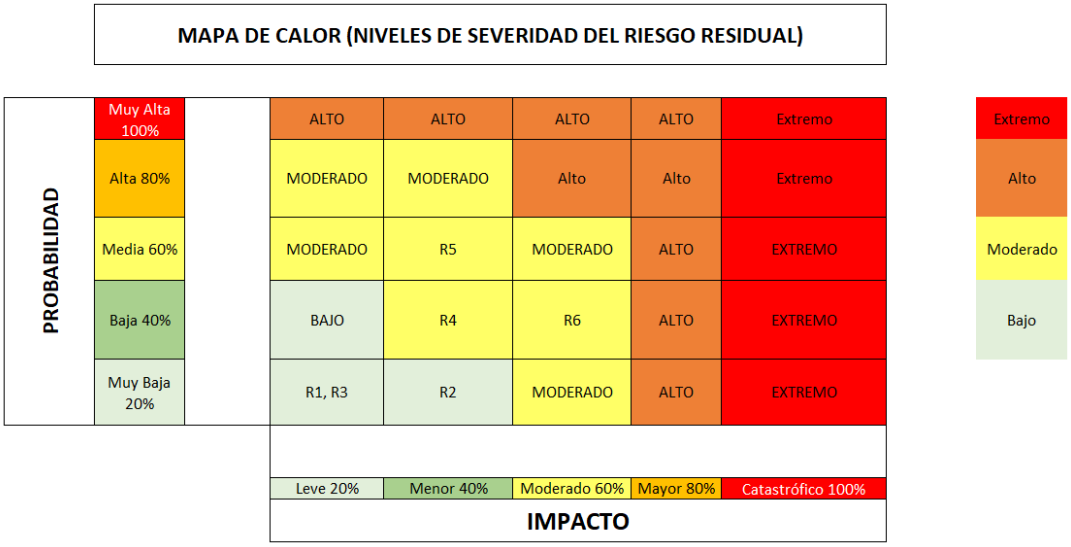
Cuando un riesgo cuenta con más de un control asociado, el cálculo se realiza de forma progresiva, es decir, el primer control se aplica sobre los valores inherentes y el resultado obtenido se utiliza como nuevo punto de partida para evaluar el segundo control y así sucesivamente hasta completar todos los controles asignados al riesgo. Esta metodología permite observar cómo, paso a paso, los controles contribuyen a reducir el nivel de exposición de manera acumulativa.

A continuación, se presenta el mapa de riesgo residual, el cual refleja el estado proyectado de cada riesgo una vez aplicadas las medidas correspondientes. Esta representación visual facilita la comparación entre el riesgo inherente y el residual, y permite

identificar cuáles amenazas se mantienen en niveles críticos y cuáles podrían considerarse bajo control si se implementan los controles sugeridos.

Figura 14

Mapa de calor de los niveles de severidad del riesgo residual



Nota. La figura presenta el mapa de riesgo residual, que refleja el estado proyectado de cada riesgo tras la implementación de los controles, mostrando una reducción en el nivel de exposición y mejorando la gestión del riesgo de la entidad.

El mapa de riesgo residual muestra un panorama favorable en comparación con el riesgo inherente, evidenciando una reducción general en el nivel de exposición frente a los riesgos analizados. A medida que se apliquen los controles propuestos, se estima que la mayoría de los riesgos podrían trasladarse desde zonas de alta y extrema criticidad hacía niveles moderados o bajos, lo que representaría un avance positivo en la gestión del riesgo de las plataformas de la entidad.

Por consiguiente, el comportamiento refleja que la selección y combinación de controles fue adecuada porque responde a las características de cada riesgo y contempla medidas preventivas, detectivas y correctivas, abordando el riesgo desde distintos frentes para lograr la

reducción gradual de la probabilidad de ocurrencia y el impacto asociado. En este sentido, el mapa de calor plantea como podría cambiar el estado del riesgo si la entidad decide implementar estas medidas para fortalecer la seguridad de la información y la continuidad de los servicios en entornos digitales.

Los resultados obtenidos en esta fase ofrecen una perspectiva del nivel de exposición a riesgos que enfrenta la infraestructura tecnológica de la entidad, convirtiéndose en un insumo estratégico para la toma de decisiones orientadas a la protección de los activos de información. El trabajo realizado hasta este punto sienta las bases para que, una vez iniciado el proceso de mejora continua, la entidad pueda reforzar su capacidad de respuesta frente a los riesgos que comprometen la integridad, disponibilidad y confidencialidad de la información.

Fase 4: Actuar

Esta fase del proyecto corresponde la elaboración de documentos técnicos con soluciones tecnológicas para mejorar la seguridad de los servicios web de la alcaldía de Fusagasugá; Para iniciar se documentó el procedimiento para la generación de certificados SSL tipo Wildcard con suscripción por un año, este ejercicio garantizo la protección de las comunicaciones digitales institucionales mediante el cifrado de datos en plataformas como la instancia_12 que se encuentra alojada en la nube y gestiona información de los usuarios.

Procedimiento para la Instalación de Certificados SSL Tipo Wildcard. El procedimiento se ejecutó sobre un servidor Linux con Apache. Para dar inicio, el proveedor de servicios en la nube genero la solicitud de firma del certificado (CSR), junto con los archivos necesarios para su posterior implementación. Una vez completado este proceso, la entidad recibió por medio del correo electrónico los archivos requeridos para la configuración, entre ellos la clave privada y los certificados emitidos por la autoridad certificadora.

Posteriormente, una vez validada la solicitud se descargaron los archivos cert.pem, chain.pem, fullchain.pem y privkey.pem. los cuales fueron organizados y almacenados dentro del directorio de Apache en Linux para su actualización.

Figura 15

Directorio de archivos de la instalación de certificados SSL tipo Wildcard en un servidor Linux

Nota. La figura muestra el directorio /etc/letsencrypt/live/ en el servidor Linux, donde se encuentran los archivos necesarios para la instalación del certificado SSL tipo Wildcard.

Con los certificados ubicados en el servidor, se reinició el servicio Apache para aplicar los cambios, activando el protocolo HTTPS en todos los servicios expuestos en la instancia_12.

Figura 16

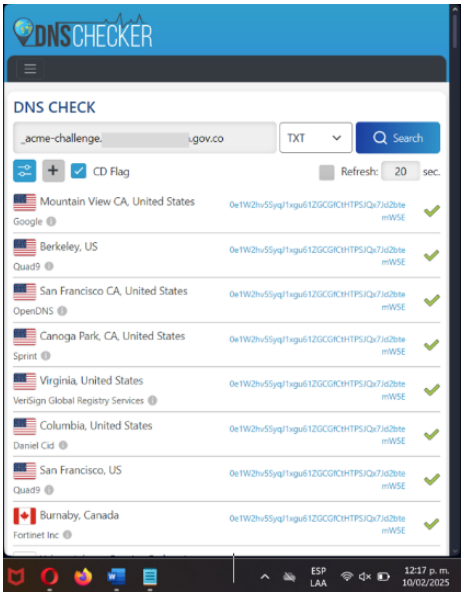
Reinicio del servicio Apache para aplicar los certificados SSL

Nota. La figura muestra el comando ejecutado para reiniciar el servicio Apache, después de la instalación de los certificados SSL, lo que activa el protocolo HTTPS en los servicios expuestos en la instancia_12.

Continuando con la validación del dominio que fue gestionada a través del protocolo ACME que permite automatizar la validación, instalación y gestión de dominios de los certificados SSL, incorporando un registro TXT (_acme-challenge) en el panel de administración DNSChecker, esta acción permitió verificar la autoridad del dominio mediante el registro propagado en internet.

Figura 17

DNSChecker validando del dominio mediante el registro TXT (_acme-challenge)



Nota. La figura muestra el resultado de DNSChecker al validar el dominio mediante el registro TXT (_acme-challenge), lo que permitió verificar la autoridad del dominio y habilitar la conexión segura (HTTPS) en todos los subdominios de la instancia_12.

La instalación del certificado SSL tipo Wildcard logró habilitar una conexión segura (HTTPS) en todos los subdominios operativos de la instancia_12, protegiendo así la confidencialidad e integridad de la información transmitida. Desde el punto de vista normativo, la ejecución de este procedimiento apoya el cumplimiento de los lineamientos establecidos en la norma ISO/IEC 27001:2022, que promueve la implementación de controles técnicos orientados a preservar la confidencialidad, integridad y disponibilidad de la información (ICONTEC, 2022).

Además, aplicar este tipo de certificado ayuda a establecer una práctica segura y organizada en el uso de plataformas digitales, lo cual representa un paso importante para mejorar la seguridad de los servicios de la Alcaldía de Fusagasugá. Gracias a esta medida, los servicios en línea pueden seguir funcionando de forma estable, se mejora la confianza de los

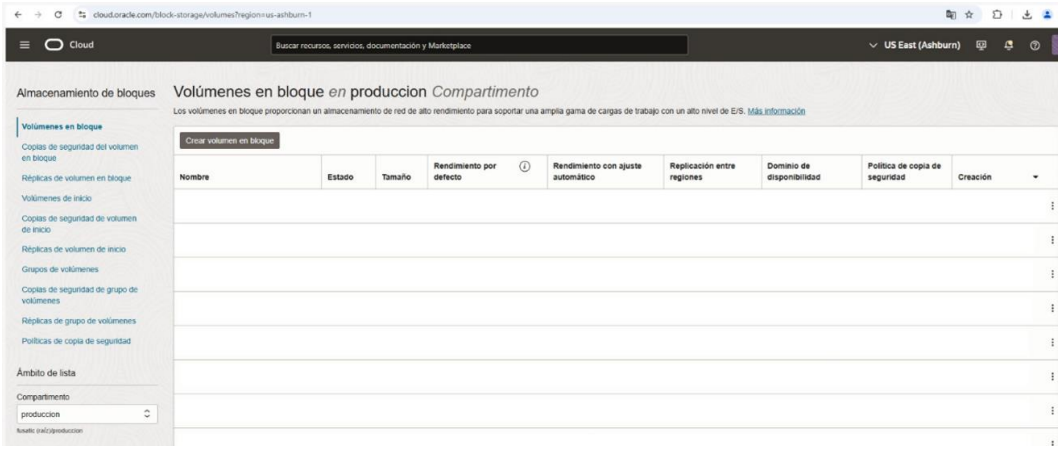
usuarios y se reducen los riesgos ante intentos de interceptación o suplantación. Este trabajo se relaciona con los esfuerzos de modernización tecnológica que adelanta la entidad y con la necesidad de proteger sus recursos digitales de forma constante.

Procedimiento para la Instalación de Copias de Seguridad en la Instancia_12

Dentro de esta fase se entregó el procedimiento documentado para la configuración de copias de seguridad en la instancia_12. Estas acciones fortalecen la seguridad de los servicios digitales al proteger los datos almacenados, disminuir el riesgo de pérdida de información y mantener la continuidad de los servicios que funcionan sobre esta infraestructura. La configuración se realizó utilizando Oracle Cloud Infrastructure Block Volume, una herramienta que permite programar respaldos automáticos según las políticas que define el usuario.

Figura 18

Interfaz de volumen en bloque en Oracle Cloud para configurar copias de seguridad



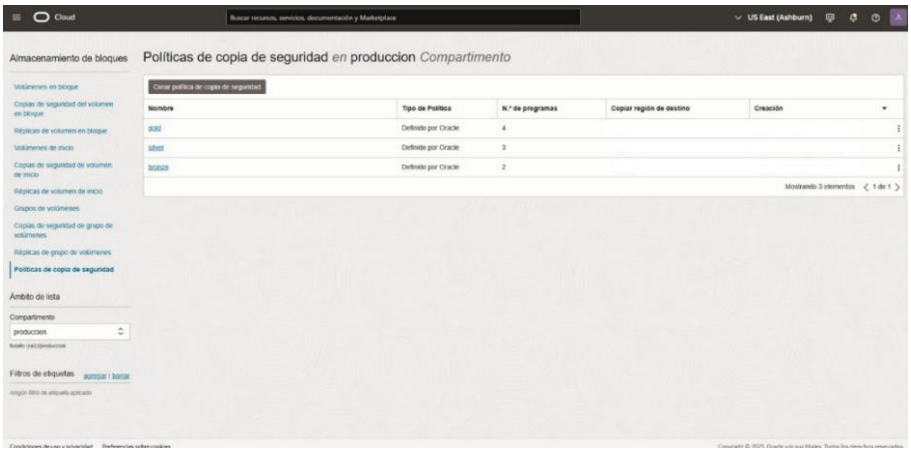
Nota. La figura muestra la interfaz de Oracle Cloud Infrastructure Block Volume, utilizada para configurar y programar copias de seguridad automáticas, lo que contribuye a proteger los datos almacenados y garantizar la continuidad de los servicios.

Posteriormente, se accedió a la pestaña Políticas de copia de seguridad donde es posible gestionar las políticas de respaldo. La plataforma permite seleccionar políticas ya definidas, las cuales automatizan el proceso de copias de seguridad según una frecuencia

especifica y son clasificadas en Gold, Silver y Bronze, se diferencian por los parámetros de frecuencia y el tiempo de retención de las copias.

Figura 19

Interfaz de políticas de copias de seguridad en Oracle Cloud

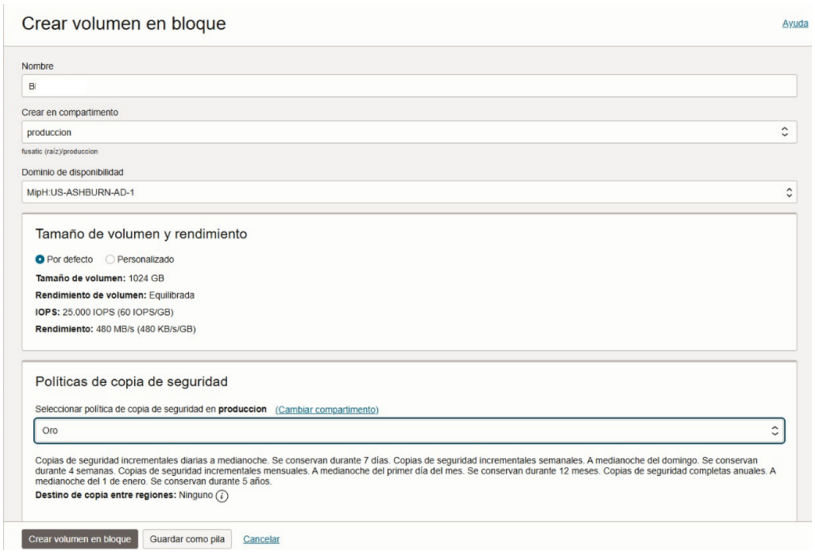


Nota. La figura muestra la interfaz de Políticas de copia de seguridad de Oracle Cloud, que gestionan las políticas de respaldo clasificadas de acuerdo con los parámetros de frecuencia y el tiempo de retención de las copias.

Después de analizar las opciones disponibles, se eligió la política oro debido a que tiene un esquema de copias de seguridad incrementales con diferentes frecuencias que le permite garantizar una cobertura continua y a largo plazo de los datos de respaldo, siendo la más adecuada para las necesidades del servicio. Esta selección se aplicó directamente al volumen, quedando configurada para realizar respaldos automáticos sin intervención manual; esta automatización asegura que siempre exista una copia reciente de los datos más importantes.

Figura 20

Interfaz para la creación de un volumen en bloque en Oracle Cloud



Nota. La figura muestra la interfaz para crear un volumen en bloque en Oracle Cloud, donde se selecciona y configura automáticamente la política de copias de seguridad.

Para verificar que todo funcionaba correctamente, se accedió a la sección de Copias de seguridad del volumen en bloque, donde es posible visualizar cada respaldo realizado. En este caso, se verifico que el sistema ya había generado copias de seguridad conforme a la política aplicada, mostrado un estado activo en el respaldo de la información de la entidad.

Figura 21

Interfaz de copias de seguridad del volumen en bloque

Nota. La figura presenta la sección de Copias de seguridad del volumen en bloque, donde se visualizan los respaldos realizados automáticamente, confirmando que el sistema ha generado copias conforme a la política de respaldo aplicada.

Con la implementación de este procedimiento, la instancia_12 cuenta ahora con un respaldo confiable y automatizado de su información, lo cual reduce significativamente los riesgos ante posibles pérdidas de datos. Este tipo de configuración es recomendado por la norma ISO/IEC 27001:2022, que sugiere establecer controles técnicos para mantener la disponibilidad de los activos de información (ICONTEC, 2022).

Además, según el Ministerio de Tecnologías de la Información y Comunicaciones de Colombia (MINTIC), las entidades públicas deben contar con mecanismos claros de respaldo que protejan la integridad y continuidad de los servicios digitales. En este sentido, lo realizado en la instancia_12 representa una mejora tangible en la gestión tecnológica de la Alcaldía, permitiendo una respuesta más rápida ante cualquier eventualidad.

Para el cierre de la fase 4 de la metodología PHVA, se entregó como producto la Guía de Buenas Prácticas en la Gestión de Servicios en la Nube para mejorar la seguridad del entorno tecnológico de la alcaldía de Fusagasugá, en el desarrollo de este documento se tuvo en cuenta recomendaciones técnicas y estratégicas fundamentadas en normas internacionales como la ISO/IEC 27002:2022, al igual que los lineamientos del Ministerio de Tecnologías de la Información y las Comunicaciones (MINTIC); De esta manera, la guía responde a la necesidad institucional de contar con un marco de referencia que oriente al personal encargado en la adecuada administración de los servicios en la nube.

Guía de buenas prácticas en los servicios en la nube de la alcaldía de Fusagasugá

Como actividad de cierre correspondiente a esta fase del ciclo Deming y de acuerdo con el diagnóstico previo y los procedimientos técnicos implementados, se elaboró una guía de buenas prácticas en los servicios en la nube, orientada a estandarizar acciones básicas que fortalezcan la seguridad de la información gestionada en entornos digitales; este documento tiene como propósito servir como herramienta de consulta para los equipos técnicos de la entidad,

promoviendo una administración segura de los recursos tecnológicos vinculados a la nube, aunque se realizó el diagnostico en base a la instancia_12, estos controles pueden ser aplicados a cualquiera de las plataformas que están alojadas en la nube de la entidad.

Para la elaboración de esta guía se tomaron seis controles seleccionados de la norma ISO/IEC 27002:2022, lo cuales fueron escogidos por su aplicación directa sobre los procedimientos implementados previamente, como la instalación de certificados SSL y la configuración de copias de seguridad en la instancia_12; la guía recopila acciones que buscan generar conciencia institucional sobre prácticas necesarias para mantener la seguridad y el orden en el uso de tecnologías en la nube.

Para iniciar el desarrollo de la guía se abordó el control 5.17. Información de autenticación, el cual orienta la gestión segura de las credenciales utilizadas para acceder a los sistemas institucionales. Allí se propone establecer un proceso estructurado de gestión de identidad y acceso teniendo en cuenta la asignación de usuarios y capacitar al personal sobre el uso adecuado de contraseñas, minimizando así los riesgos de accesos no autorizados o el uso indebido de cuentas internas.

De forma complementaria, se incluyó el control 8.5. Autenticación de seguridad, que sugiere implementar mecanismos de autenticación que se ajusten a los niveles de sensibilidad de la información. En este sentido, la guía promueve el uso de autenticación multifactor (MFA), el cierre automático de sesiones inactivas al transcurrir 30 segundos y el uso de claves temporales o tokens, para asegurar que solo las personas autorizadas accedan a los servicios digitales de la entidad.

Avanzando hacía la protección de la infraestructura frente a amenazas externas, se aplicaron los principios del control 8.7. Protección contra malware, el cual recomienda adoptar medidas preventivas que ayuden a reducir los riesgos derivados de software malicioso como la

instalación y actualización de software de antivirus, configuración de firewall y realizar un respaldo de la seguridad de manera continua. Al igual que la gestión oportuna de fallas técnicas, a través del control 8.8. Gestión de vulnerabilidades técnicas, que plantea la necesidad de contar con un proceso continuo de identificación, evaluación y respuesta ante vulnerabilidades. Para ello, la guía sugiere realizar prácticas de actualización de los sistemas de protección, como los parches de seguridad y documentar los hallazgos para su tratamiento oportuno, anticipándose a posibles incidentes y manteniendo la estabilidad de los servicios.

En cuanto a la organización interna de los recursos tecnológicos, se tomó como base el control 8.9. Gestión de la configuración, el cual señala la importancia de definir y mantener configuraciones seguras en el hardware, software y las redes utilizadas. La guía recomienda registrar cada cambio que se realice, mantener un histórico de configuraciones base y evitar modificaciones sin autorización, como forma de proteger la integridad y funcionalidad de los sistemas institucionales.

En la guía se destaca el uso de protocolos seguros como HTTPS, el almacenamiento cifrado de datos sensibles y la gestión adecuada de claves de acuerdo con las políticas que defina la entidad. De esta manera, se vincula el control 8.24. Uso de cifrado, que establece la importancia de utilizar mecanismos de criptografía para proteger la información sensible. Estas medidas buscan garantizar que la información se mantenga protegida, cuando está en tránsito o en almacenamiento, respetando los principios de confidencialidad, autenticidad e integridad.

La elaboración de esta guía de buenas prácticas representa un avance importante para la alcaldía de Fusagasugá, ya que permite contar con un documento técnico que traduce los principios normativos de la seguridad de la información en acciones, aplicables al entorno real de los servicios en la nube de la entidad. Esta guía orienta al personal responsable en la toma de decisiones técnicas y establece una base que puede ser actualizada, complementada y adaptada conforme evolucionen las necesidades tecnológicas de la organización.

Además, contar con esta guía fortalece la posición de la alcaldía frente a auditorías internas o externas, dado que demuestra una apropiación real de los marcos internacionales como ISO/IEC 27002:2022. También permite alinear las actividades técnicas con los lineamientos estratégicos del Gobierno Digital promovidos por el MinTIC, generando un respaldo normativo que es valorado en procesos de planificación, seguimiento y evaluación institucional.

Capítulo 5. Análisis de resultados

Los resultados del desarrollo del proyecto que se realizó en la oficina TIC y transformación digital de la alcaldía de Fusagasugá se presentaron en el capítulo 4 del presente documento. En este capítulo, la información se ordenó de acuerdo con la metodología PHVA o Deming, lo que permitió realizar un análisis estructurado de cada fase del proyecto. Dado que el análisis de los resultados ya se presentó en el capítulo anterior, en este apartado se hará un resumen de los puntos discutidos previamente.

En la primera fase, se realizó un diagnóstico para evaluar el estado de la infraestructura tecnológica en la nube de la entidad, este análisis permitió identificar áreas críticas que requerían atención, lo que ayudó a priorizar las acciones a seguir, sentando las bases en la toma de decisiones de las fases posteriores.

En la fase “Hacer” se detectaron posibles vulnerabilidades en los servicios expuestos en la nube, con ayuda de la herramienta Nmap que se ejecutó en una máquina virtual con Kali Linux. De esta manera, la actividad efectuó dentro de un entorno controlado para continuar con el trabajo y no afectar la continuidad operativa de los sistemas. A partir del análisis se encontró configuraciones que necesitaban ajustes para reducir los riesgos de acceso no autorizado y mejorar la seguridad de la infraestructura en el entorno de computación en la nube de la entidad, de igual manera, este producto sirvió para continuar con las actividades de la siguiente fase.

Se diseñó una matriz de riesgos en la fase de verificación para establecer las zonas de riesgo inherente teniendo en cuenta la probabilidad y el impacto de cada evento, luego se representó visualmente mediante un mapa de calor para identificar por medio de colores los niveles críticos. Con ello, se formularon controles que están acordes con la norma ISO/IEC 27001:2022 para mitigar el riesgo y mejorar la seguridad de la entidad. A partir de estos controles, se estimó el riesgo residual, es decir, el nivel de exposición cuando sean aplicado las

medidas de mitigación, lo que permitió prever el resultado que podrían tener los controles sobre la reducción de la probabilidad y el impacto de los eventos analizados al realizar su implementación.

En el desarrollo de las fases anteriores, se identificó posibles vulnerabilidades en la infraestructura tecnológica de la alcaldía de Fusagasugá, de acuerdo con esto en la fase 4 se documentaron procedimientos para la ejecución de copias de seguridad para garantizar la disponibilidad de la información de la entidad, los cuales fueron diseñados a partir de criterios técnicos que se adaptan a las necesidades de la entidad. De igual manera, se estructuró una guía de buenas prácticas en los servicios en la nube que recolecta las recomendaciones derivadas de los resultados de las fases anteriores. Este documento es un recurso estratégico en el apoyo en la toma de decisiones del equipo de redes y seguridad de la entidad que está orientado a fortalecer la seguridad de la información y promover la mejora continua como lo recomienda la norma ISO/IEC 27001:2022.

Capítulo 7. Conclusiones

La evaluación inicial de la infraestructura tecnológica de la alcaldía de Fusagasugá permitió identificar características importantes en las operaciones que se despliegan en los servicios en la nube de la entidad que permitieron continuar con las siguientes actividades. A través del levantamiento de información que se realizó con el acompañamiento del personal de la oficina TIC y transformación digital se logró cumplir con el análisis del entorno cloud y comprender como estaba distribuido, identificar los recursos disponibles, lo que permitió evidenciar las fortalezas en cuanto a la escalabilidad del entorno y la segmentación lógica de los servicios. Sin embargo, también se evidenciaron debilidades como la carencia de procedimientos técnicos para la gestión de respaldos y monitoreo continuo, lo cual permitió orientar el desarrollo de las acciones en las siguientes fases del ciclo.

El análisis desarrollado a través de herramientas de escaneo en un entorno controlado que permitió detectar seis riesgos ubicados en las zonas Alto y Extremo del mapa de calor inherente, lo cual comprometía la disponibilidad, integridad y confidencialidad de la información. El uso de scripts especializados facilitó la identificación de amenazas en la instancia evaluada fortaleciendo la capacidad de respuesta frente a posibles incidentes en los servicios alojados en la nube de la alcaldía de Fusagasugá. Al aplicar los controles correctivos, estos riesgos se desplazarían a las zonas Bajo y Moderado, logrando una mitigación de hasta el 80% de los riesgos identificados en el mapa de calor residual. Sin embargo, este porcentaje de mitigación corresponde solo a los riesgos detectados en este análisis y podría variar debido a nuevas vulnerabilidades o cambios en las condiciones del entorno.

Por medio del diseño de un matriz de riesgos se presentó un mapa de calor para clasificar los eventos de acuerdo con el nivel de probabilidad e impacto, esta gráfica permitió enfatizar en la priorización de implementar medidas correctivas en los riesgos que se encontraban en estado crítico y necesitaban ser evaluados de carácter prioritario. De igual

modo, los controles que se recomendaron aplicar eran acordes al desarrollo de buenas prácticas que se encuentran en la norma ISO/IEC 27001:2022, aportando un marco técnico para evaluar y reducir la exposición de los activos de información ante amenazas que se pueden estar presentando dentro del entorno tecnológico de la entidad y contribuye a que la institución tome la iniciativa de utilizar buenas prácticas y más adelante lograr tener la certificación de seguridad ISO/IEC 27001:2022.

Se diseñó una guía de buenas prácticas la cual se ajustó al contexto tecnológico de la entidad para cumplir con este objetivo primero se tenían que desarrollar las fases anteriores ya que a partir de estas fue posible identificar las vulnerabilidades y realizar recomendaciones de normativas vigentes que se adaptaran a las necesidades de la alcaldía de Fusagasugá, es documentó será una herramienta importante en la toma de decisiones del equipo de seguridad para proteger la información y asegurar la correcta gestión de los servicios en la nube, fortaleciendo el entorno institucional y estandarizando los procesos para adoptar medidas preventivas que contribuyan a la administración de los recursos digitales.

Capítulo 8. Recomendaciones para la Empresa

Luego de culminar el desarrollo del proyecto, se recomienda que la alcaldía de Fusagasugá desde la oficina TIC y la transformación digital, brinde capacitación al personal en buenas prácticas de seguridad y gestión de entornos en la nube, de modo que cada integrante del equipo asuma un rol activo en la protección de los servicios digitales. Como complemento la entidad podrá aplicar la guía de buenas prácticas elaborada durante el proyecto, cerrando las brechas detectadas y estableciendo un protocolo interno de gestión del riesgo para las plataformas alojadas en la nube de la entidad.

De esta manera, la alcaldía podrá incorporar las recomendaciones de la Política de Gobierno Digital, especialmente la adopción de estándares de interoperabilidad que faciliten el intercambio de información con otras entidades; la publicación de datos abiertos en portales accesibles para fomentar la transparencia; el diseño de interfaces centradas en el usuario que mejoren la experiencia y usabilidad de los servicios en línea; y el cumplimiento de las normas de accesibilidad y seguridad definidas por el Gobierno Nacional. De esta forma, las soluciones tecnológicas y los procesos estandarizados responderán a las necesidades operativas, alineándose con los objetivos de modernización y participación ciudadana en las entidades públicas del territorio nacional.

Estos cambios contribuyen a que en un futuro la alcaldía de Fusagasugá se certifique en la norma ISO/IEC 27001:2022 aumentando la confianza a los ciudadanos que utilizan los servicios en línea de la entidad. De igual manera, es recomendable aplicar un sistema de monitoreo continuo que supervise en tiempo real el estado de la infraestructura en la nube, genere alertas automáticas ante cualquier falla en el sistema, así la entidad avanzará en el proceso de mejora continua y fortalecerá la calidad de los procesos digitales a largo plazo.

Referencias Bibliográficas

Mora Guamán, R. J. (2022). *Análisis y diseño de un modelo para establecer un sistema de gestión de la seguridad de la información dentro de un ambiente cloud computing, aplicando la norma ISO 27001 en la empresa DATA-FIBER* [Tesis de grado Universidad Técnica de Babahoyo] http://dspace.utb.edu.ec/handle/49000/11844

Carvajal Hurtado, L. V. (2022). *Análisis y Diseño de un Sistema de Gestión de Seguridad de la Información Basado en ISO 27001: 2013 para el Área de TI de Pignus Solutions SAS*. [Trabajo de grado Especialización Universidad Piloto de Colombia] http://repository.unipiloto.edu.co/handle/20.500.12277/12495

Duarte Caviedes, O. A. (2018). *Gestión de riesgo de activos de información.* [PDF] http://repository.unipiloto.edu.co/handle/20.500.12277/8586

Osorio Corredor, L. E. (2018). *Gestión de riesgos de seguridad de la información en el sector público.* [PDF] http://repository.unipiloto.edu.co/handle/20.500.12277/4646

Pulido Barreto, A. M., & Mantilla Rodriguez, J. M. (2016). *Modelo para la implementación del sistema general de seguridad informática y protocolos de seguridad informática en la oficina TIC de la alcaldía municipal de Fusagasugá, basados en la gestión del riesgo informático.* [Trabajo de grado Especialización Universidad Nacional Abierta y A Distancia] https://repository.unad.edu.co/handle/10596/6327

Padilla, D. E. C. (2021). Servicios en la nube para los actores estratégicos del Estado: caso Colombia. *Revista Ibérica de Sistemas e Tecnologias de Informação*, (E43), 314-326.

República de Colombia. (2022). Decreto 338 de 2022 por el cual se adopta la política de ciberseguridad y el modelo de gestión de seguridad de la información en las entidades públicas. Diario Oficial No. 51970. https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=181866

Función Pública. (2024). Política de administración de riesgos en función pública. Departamento Administrativo de la Función Pública. https://www1.funcionpublica.gov.co/documents/34645357/34702985/Politica-administracion-riesgos-direccionamiento-estrategico-v19.pdf/206b683f-e5d4-4919-99e5-ada49fadf8e6?t=1714477947431

Ministerio de Tecnologías de la Información y las Comunicaciones. (2024). Modelo de gestión de riesgos de seguridad digital (MGRSD). Gobierno Digital. https://gobiernodigital.mintic.gov.co/seguridadyprivacidad/portal/Estrategias/MGRSD/

República de Colombia. (2022). Decreto 767 de 2022 por el cual se adopta la política de gobierno digital. Diario Oficial No. 52036. https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=186766

República de Colombia. (2022). Decreto 1263 de 2022 por el cual se establecen los lineamientos y estándares para la transformación digital de la administración pública en el marco de la Política de Gobierno Digital. Diario Oficial No. 52103. https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=190206

Instituto Colombiano de Normas Técnicas y Certificación (ICONTEC). (2022). NTC-ISO/IEC 27001: Seguridad de la información, ciberseguridad y protección de la privacidad. Sistemas de gestión de seguridad de la información. Requisitos (2.ª act.). https://tienda.icontec.org/gp-ntc-iso-iec-seguridad-de-la-informacion-ciberseguridad-y-proteccion-de-la-privacidad-sistemas-de-gestion-de-seguridad-de-la-informacion-requisitos-ntc-iso-iec27001-2022.html

Instituto Colombiano de Normas Técnicas y Certificación (ICONTEC). (2022). NTC-ISO/IEC 27002: Seguridad de la información, ciberseguridad y protección de la privacidad. Controles de seguridad de la información. https://tienda.icontec.org/gp-gtc-iso-iec-

seguridad-de-la-informacion-ciberseguridad-y-proteccion-de-la-privacidad-controles-de-seguridad-de-la-informacion-gtc-iso-iec27002-2022.html

Alcaldía de Fusagasugá. (2024). *Misión y visión*. Alcaldía de Fusagasugá. https://www.fusagasuga.gov.co/alcaldia/mision-y-vision

Ministerio de Tecnologías de la Información y las Comunicaciones. (2016). *Seguridad en la nube: Guía No. 12* [PDF]. Gobierno Digital. https://gobiernodigital.mintic.gov.co/692/articles-150518_G12_Seguridad_Nube.pdf

Departamento Nacional de Planeación. (2020). *Política nacional de confianza y seguridad digital (CONPES 3995)* [PDF]. Gobierno de Colombia.

https://colaboracion.dnp.gov.co/CDT/Conpes/Econ%C3%B3micos/3995.pdf

Departamento Nacional de Planeación. (2016). *Política nacional de seguridad digital en Colombia (CONPES 3854)* [PDF]. Gobierno de Colombia. https://colaboracion.dnp.gov.co/CDT/Conpes/Económicos/3854.pdf

Departamento Administrativo de la Función Pública. (2022). *Guía para la Administración del Riesgo y el diseño de controles en entidades públicas Versión 6* [PDF] https://www1.funcionpublica.gov.co/documents/28587410/34299967/Guia_administracion_riesgos_capitulo_riesgo_fiscal.pdf

Apéndice

Apéndice A. Cronograma de Actividades

Cronograma de Actividades Pasantía - Karen Escalante.xlsx