ANÁLISIS DE LOS RIESGOS DE SEGURIDAD DE LA INFORMACIÓN DEL SISTEMA DE GESTIÓN DOCUMENTAL DE LA ALCALDÍA MUNICIPAL DE IBAGUÉ

ALBA DENYS VALENCIA BAUTISTA

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA - ECBTI
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
IBAGUÉ
2022

ANÁLISIS DE LOS RIESGOS DE SEGURIDAD DE LA INFORMACIÓN DEL SISTEMA DE GESTIÓN DOCUMENTAL DE LA ALCALDÍA MUNICIPAL DE IBAGUÉ

ALBA DENYS VALENCIA BAUTISTA

Proyecto de Grado – Proyecto Aplicado presentado para optar por el título de
ESPECIALISTA EN SEGURIDAD INFORMÁTICA

Edgar Mauricio López Rojas
Director Trabajo de Grado

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA - ECBTI
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
IBAGUÉ
2022

NOTA DE ACEPTACIÓN

Firma del Presidente de Jurado

Firma del Jurado

Firma del Jurado

Ciudad., Fecha sustentación

DEDICATORIA

Especialmente a mi madre Bellanid Bautista, por el apoyo incondicional en el desarrollo de mis actividades académicas, laborales y personales, quien ha sido diariamente esa voz de aliento y motivación para lograr las metas proyectadas; así mismo agradezco a mis sobrinos y hermanos quienes han estado hay para motivarme y demostrarme que cada día podemos ser mejores si nos esforzamos y luchamos por ello.

AGRADECIMIENTOS

Agradezco inicialmente al personal en general de la Universidad Nacional Abierta y a Distancia UNAD, quienes con sus estrategias y flexibilidad para acceder a la universidad, permite que sin discriminación alguna se pueda contar con un servicio académico de calidad, brindado por directores, tutores y asesores idóneos y con total disposición, así mismo, presento mi agradecimiento a la Alcaldía de Ibagué por medio de la Secretaría Administrativa, por permitirme desarrollar el proyecto de investigación con información de la entidad.

CONTENIDO

pág.

LISTA DE TABLAS

LISTA DE FIGURAS

LISTA DE CUADROS

GLOSARIO

AUTENTICIDAD: Proceso de identificación del autor como emisor original de un mensaje de datos, validando con ello la no suplantación.

ARCHIVO ELECTRÓNICO DE DOCUMENTOS: Salvaguarda de cada uno de los instrumentos electrónicos y/o expedientes.

ARCHIVO PÚBLICO: Conjunto de archivos propiedad de entidades oficiales, los cuales también se emanan del servicio público efectuado por organizaciones privadas.

EXPEDIENTE ELECTRÓNICO: Serie de documentos electrónicos pertenecientes a un proceso.

GESTIÓN DOCUMENTAL: Acciones administrativas, técnicas orientadas a la planeación, administración y control, de los instrumentos emitidos por las entidades de estado.

GOBIERNO EN LÍNEA: Usabilidad de las Tecnologías de la Información y las Comunicaciones (TIC) orientadas a para optimar el servicio ante la ciudadanía.

INTEGRIDAD: Seguridad de la información mediante la cual se garantiza su exactitud al ser almacenada o custodiada.

MARGERIT: Denominada “Proceso de Gestión de Riesgos”, la implanta la gestión de riesgos en el marco de trabajo para la toma de decisiones basado en los riesgos derivados de la usabilidad de tecnología de la información[1]

[1] ADMINISTRACIÓN ELECTRÓNICA [Sitio Web] MARGERIT v.3 Metodología de Análisis y Gestión de los Riesgos de los Sistemas de Información. [Consulta: 01 de mayo de 2021]. Disponible

MEDIO ELECTRÓNICO: Mecanismo tecnológicos orientados a producir, almacenar datos en general.

POLÍTICA DE SEGURIDAD: Se considera como una determinación formal de reglamentos, directrices y prácticas que fundamental la forma de gestión de activos de tecnología de la información al interior de una organización.[2]**.**

PISAMI: "Plataforma Integrada de Sistemas de la Administración Municipal de Ibagué"

RIESGO: Composición de la probabilidad de un evento y sus derivaciones[3].

en:https://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_Magerit.html

[2] SISTESEG. [Sitio Web]. Recomendaciones para Estructurar Documentos de Políticas ISO 27001:2013. [Consulta: 01 de mayo de 2021] Disponible en: https://www.sisteseg.com/files/Recomendaciones_para_estructurar_documentos_de_pol_ticas_ISO_27001.pdf. p.6

[3] ISO. [Sitio Web]. ISO 31000:2018 Gestión del Riesgo - Directrices. [Consulta 01 de mayo de 2021]. Disponible en: https://www.iso.org/obp/ui#iso:std:iso:31000:ed-2:v1:es

RESUMEN

El presente proyecto busca brindar a la Alcaldía de Ibagué un plan de mitigación de riesgos mediante el análisis de riesgo de seguridad de la información del Sistema de Gestión Documental llamado, “Plataforma Integrada de Sistema Municipal de Ibagué – PISAMI, la cual fue desarrollada por personal adscrito a la entidad e implementada en el año 2014; dicho plan se realizará mediante el perfeccionamiento de la metodología de análisis de riesgos MARGERIT, basada en la Norma Internacional ISO 27001:2013 y con el fin de identificar los activos (hardware y software) que evidencien vulnerabilidades y sobre las mismas proponer control y gestión que las minimice.

El desarrollo de este proyecto cual servirá de apoyo para demostrar la importancia de contar con un sistema que cumpla a cabalidad con los pilares de la seguridad, asentados en la Norma Internacional ISO 27001:2013 y la ISO 31000:2018 que tiene como fin de garantizar, la integridad, disponibilidad y confidencialidad de la información.

ABSTRACT

This project seeks to provide the Ibagué Mayor's Office with a risk mitigation plan by analyzing the information security risk of the Document Management System called, "Integrated Platform of the Municipal System of Ibagué - PISAMI, which was developed by staff attached to the entity and implemented in 2014; Said plan will be carried out through the improvement of the MARGERIT risk analysis methodology, based on the International Standard ISO 27001: 2013 and in order to identify the assets (hardware and software) that show vulnerabilities and on these propose control and management that minimize them.

The development of this project, which will serve as support to demonstrate the importance of having a system that fully complies with the pillars of security, established in the International Standard ISO 27001: 2013 and ISO 31000, which aims to guarantee, the integrity, availability and confidentiality of information.

INTRODUCCIÓN

Teniendo en cuenta las exigencias actuales, en cuanto el empleo de la Tecnología, Información y comunicación – TIC en toda entidad público/privada, como estrategia para la mejora continua de los procesos y procedimientos, aseguramiento de la información física y electrónica, la cual demanda de un trabajo mancomunado entre directivo del área de la TIC, y Gestión Documental, profesionales, técnicos y/o auxiliares responsables de Sistema de Gestión Documental de toda entidad; para la proyección de políticas y perfeccionamiento de estrategias de gestión de documental que avalen una gestión veraz de la información documental.

Por lo tanto, se requiere de la ejecución de sistemas de Información de Gestión Documental, que cumpla con los estándares de calidad y buenas prácticas señaladas en la ISO 27001 “Sistema de Gestión de Seguridad de la Información”, ISO 31000 y demás normativa archivista emitida para Colombia; que permitan salvaguardar o custodiar a cabalidad la información.

Así mismo considerando las exigencias de conservar una entidad operativa ante amenazas y riesgos vigentes, se han diseñado variedad de metodologías y estándares para la tipificación de riesgos, análisis y su debido control y tratamiento en aras de mitigas los riesgos.

Por consiguiente, basados en lo anterior se efectúa el planteamiento del problema en el cual por medio de una metodología de riesgos se realiza la identificación aspectos relevantes para la Alcaldía de Ibagué, con la finalidad de establecer procesos que conlleven a implementar estándares como ISO 31000 y metodologías como MARGERIT, con los cuales se logre identificar los riesgos, controlarlos y conservar un nivel de riesgo admisible ante las exigencias de la actualidad.

1. DEFINICIÓN DEL PROBLEMA

1.1 ANTECEDENTES DEL PROBLEMA

Para todas aquellas entidades públicas y privadas, la información respaldada tanto de manera física como electrónica; se cataloga como un activo de vital importancia, la cual se debe manipular y custodiar de manera exhaustiva y prudente, puesto que de ello dependerá la integridad y el buen nombre una entidad o usuario en general.

Es por ello que basado en los actos de vandalismo con respecto a ataques informáticos presentados cada día a nivel local, Nacional e Internacional, gracias a las vulnerabilidades de seguridad de sus sistemas, perdida de documentos en las entidades por falta de organización y adecuada custodia de la misma, demora en los procesos por deficiente accesibilidad a la información, y duplicidad de documentación (físico) por la falta de cultura con respecto al uso del papel; las entidades de Orden Nacional establecieron requerimientos en los se exige a las entidades públicas la implementación Sistemas de Gestión Documental, en los cuales se plantee a su vez, Políticas Cero Papel[4] Sistemas de conservación de documentos y archivos que permitan la preservación de la memoria institucional de toda entidad[5], e implantación de un modelo de Seguridad y Privacidad de la información[6].

De esta manera se puede concluir que la importancia de establero un método de tratamiento de riesgos de los Sistemas de Gestión Documental en una entidad es muy alta; puesto que, no solo dar cumplimiento a las normas es una prioridad, sino también lo es implementar Sistemas que permitan salvaguardar la información de tal manera que se garantice la integridad, disponibilidad y confidencialidad de la misma.

[4] GOBIERNO EN LÍNEA. [Sitio Web]. Buenas Prácticas para reducir el consumo de papel. Bogotá: [Consulta: 01 de mayo de 2021]. Disponible: https://estrategia.gobiernoenlinea.gov.co/623/articles-8257_papel_buenaspracticas.pdf.
[5] ARCHIVO GENERAL DE LA NACIÓN. [Sitio Web]. Ley 1712 de 2014. Bogotá: AGN. [Consulta: 01 de mayo de 2021]. Disponible: https://normativa.archivogeneral.gov.co/ley-1712-de-2014/
[6] MINTIC. [Sitio Web]. Modelo de Seguridad y Privacidad de la Información. Bogotá. [Consulta: 01 de mayo de 2021]. Disponible: https://www.mintic.gov.co/gestionti/615/articles-5482_Modelo_de_Seguridad_Privacidad.pdf

Por consiguiente, el uso de la metodología MAGERIT la cual está asociada con las normas ISO 31000 y la ISO 27001:2013, se realizará un análisis de los riesgos de seguridad de la información del Sistema de Gestión Documental de la Administración Municipal, con el fin de identificar sus vulnerabilidades y así proponer un método de tratamiento de riesgos que coadyuben a mitigar y controlar los riesgos identificados que afectan de manera significativa los activos de la entidad.

1.2 FORMULACIÓN DEL PROBLEMA

¿Cómo el análisis de los riesgos de seguridad de la información del Sistema de Gestión Documental de la Alcaldía Municipal de Ibagué, contribuye a la protección y tratamiento de los datos?

2 JUSTIFICACIÓN

Alcaldía de Ibagué, como entidad pública orientada a brindar servicios a la comunidad, ha recepcionado un gran numero documentos entre Peticiones, Quejas, Reclamos y Solicitudes (P.Q.R.S); tanto en medio físico como electrónico, así mismo emite información correspondiente a cada uno de los procesos internos de la Administración Municipal (Informes de Gestión, a entes de Control, Historia Laboral, etc); generando con ello un alto volumen de documentos y datos, que por su grado importancia y categorización (de reserva o publica) requerían un Sistema de Gestión Documental, adecuado que garantizara no solo la integridad, disponibilidad y confidencialidad de la información, sino también que permitiera dar cumplimiento a los requerimientos establecidos por la Ley.

Teniendo en cuenta lo expuesto anteriormente, para la Alcaldía de Ibagué titular de la Plataforma del Sistema de Gestión Documental, será de gran importancia contar con información puntual de los riesgos a los que se encuentra sometida los datos y el contar con información clara y concisa de como mitigar y controlar las vulnerabilidades identificadas, permitirá que a futuro el sistema de gestión se mantenga confiable, integral y disponible, cumpliendo con los estándares establecidos en las norma ISO 27001:2013 y 31000.

3 OBJETIVOS

3.1 OBJETIVOS GENERAL

Analizar los riesgos de seguridad de la información del Sistema de Gestión Documental de la Alcaldía Municipal de Ibagué, aplicando la metodología MAGERIT la cual está asociada con las normas ISO 31000:2018 y la ISO 27001:2013.

3.2 OBJETIVOS ESPECÍFICOS

- Aplicar la metodología MARGERIT para la evaluación de riesgos que permita identificar vulnerabilidades y amenazas de seguridad, así como evaluar los riesgos conforme lo establece la metodología.

- Proponer mecanismos de control y gestión que reduzcan las vulnerabilidades identificadas en el análisis realizado.

- Elaborar informe de hallazgos y recomendaciones que permita precisar un Sistema de Seguridad de la información concreta a la realidad de la Alcaldía Municipal de Ibagué.

4 MARCO REFERENCIAL

4.1 MARCO TEÓRICO

La Administración Municipal de Ibagué como todas las entidades Territoriales, Nacionales e Internacionales, prestadoras de servicio público, están en la obligación de aplicar Sistemas de Gestión de Documental, con el fin de virtualizar la documentación que diariamente se emite en cada una de ellas, teniendo en cuenta que el volumen de P.Q.R.S que la comunidad allega y los informes y/o comunicados que se generan internamente dentro de las entidades es exorbitante; conllevando a la perdida de información, deficiencia en la calidad del servicio, y desorden en los archivos físicos, etc; problemática que día a día se acrecienta.

Por tal razón a nivel Colombia, el Archivo General de la Nación mediante la Ley 594 de 2000 en su artículo 19[7] "***Soporte documental**. Las entidades del Estado podrán incorporar tecnologías de avanzada en la administración y conservación de sus archivos, empleando cualquier medio técnico, electrónico, informático, óptico o telemático, siempre y cuando cumplan con los siguientes requisitos:*

a) Organización archivística de los documentos;

b) *Realización de estudios técnicos para la adecuada decisión, teniendo en cuenta aspectos como la conservación física, las condiciones ambientales y operacionales, la seguridad, perdurabilidad y reproducción de la información contenida en estos soportes, así como el funcionamiento razonable del sistema*."

Ordena a las entidades a aplicar sistemas tecnológicos que mejoren de manera relevante el manejo de sus archivos (físico y electrónicos), basado en lo reglamentado en la Ley

[7] ARCHIVO GENERAL DE LA NACIÓN. [Sitio Web]. Bogotá: AGN, Ley 594 de 2000 [Consulta: 01 de mayo de 2021]. Disponible en: https://normativa.archivogeneral.gov.co/ley-594-de-2000/.

527 de 1999, (Senado de la República, 1999)" *Por medio de la cual se define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales, y se establecen las entidades de certificación y se dictan otras disposiciones"*[8]. Y teniendo en cuenta lo determinado en el Acuerdo 03 del 17 de febrero de 2015[9], se emiten los lineamientos a las entidades del Estado a implementar Sistemas de Gestión Documental orientados a el uso medios electrónicos, a fin de asegurar la información, conservación de documentos que garanticen a su vez la los tramites y servicios; de esta manera con el fin de ubicarnos a lo que respecta al aseguramiento del Sistemas de Gestión Documental, se conceptualiza los siguientes términos según el Archivo General de la Nación en la Ley 594 / 2000 y en el Acuerdo 03 de 2015.

Por lo anterior, para el desarrollo del análisis de riesgos de un Sistema de Gestión Documental, es necesario utilizar conceptos de Seguridad de la Información que son aplicados tanto en entidades públicas como privadas.

Sistema de Gestión de la Seguridad de la Información - SGSI[10]. Considerado como un conjunto de normas de Administración de la Información, dicho termino se designa como "Information Security Management System" (ISMS). Dicho termino es aplicado específicamente por la norma ISO/IEC 27001, el cual corresponde al estándar internacional avalado en el año 2005 y actualizado en la vigencia 2013.

Seguridad de la Información: Como lo enuncia la ISO 27001, seguridad de la información se basa en la conservación de la confidencialidad, integridad y disponibilidad

[8] ARCHIVO GENERAL DE LA NACIÓN. [Sitio Web]. Bogotá: AGN, Ley 527 de 1999 [Consulta: 01 de mayo de 2021]. Disponible en: https://normativa.archivogeneral.gov.co/ley-527-de-1999/
[9] ARCHIVO GENERAL DE LA NACIÓN. [Sitio Web]. Bogotá: AGN, Acuerdo 003 de 2015 [Consulta: 01 de mayo de 2021]. Disponible en: https://normativa.archivogeneral.gov.co/acuerdo-003-de-2015/
[10] FIRMA-e. [Sitio Web]. ¿Qué es un SGSI - Sistema de Gestión de la Información? [Consulta: 01 de mayo de 2021] Disponible en: https://www.firma-e.com/blog/que-es-un-sgsi-sistema-de-gestion-de-seguridad-de-la-informacion/

de la información, así mismo se cuenta con propiedades tales como la autenticidad, responsabilidad, no repudio y confiabilidad[11].

De tal manera se enuncia términos correspondientes a Seguridad de la Información, aplicados en el desarrollo del presente proyecto.

Confidencialidad: Propiedad por la que la información no se sitúa a disposición o se divulgación de terceros[12].

Disponibilidad: Propiedad que tienen los activos de ser accesible y aprovechable a petición de la organización autorizada[13].

Integridad: Propiedad de la veracidad de la información, la cual salvaguarda la precisión y estado de los activos[14].

Gestión documental: Teniendo en cuenta el concepto emitido por el Archivo General de la Nación, el término "Gestión Documental", consiste en grupo de acciones administrativas y técnicas, orientadas a planificar, manejar y organizar el acervo documental producido y allegado por las entidades, partiendo de su origen a su destino final con el objeto de facilitar su uso y conservación. [15]

Basados en este concepto, es importante resaltar los beneficios de contar con un **Sistema de Gestión Documental** en una organización, ello teniendo en cuenta que no

[11] NORMA ISO 27001. [Sitio Web]. Madrid: Referencias Normativas Iso 27000 [Consulta: 01 de mayo de 2021]. Disponible en: https://normaiso27001.es/referencias-normativas-iso-27000/#def328
[12] NORMA ISO 27001. [Sitio Web]. Madrid: Referencias Normativas Iso 27000 [Consulta: 01 de mayo de 2021]. Disponible en: https://normaiso27001.es/referencias-normativas-iso-27000/#def310.
[13] NORMA ISO 27001. [Sitio Web]. Madrid: Referencias Normativas Iso 27000 [Consulta: 01 de mayo de 2021]. Disponible en: https://normaiso27001.es/referencias-normativas-iso-27000/#def37.
[14] NORMA ISO 27001. [Sitio Web]. Madrid: Referencias Normativas Iso 27000 [Consulta: 01 de mayo de 2021]. Disponible en: https://normaiso27001.es/referencias-normativas-iso-27000/#def336.
[15] ARCHIVO GENERAL DE LA NACIÓN – AGN. [Sitio Web]. Glosario [Consulta: 17 de mayo de 2021]. Disponible en: https://www.archivogeneral.gov.co/Transparencia/informacion-interes/Glosario

solo se garantiza la disponibilidad de la información, sino también da alcance a la iniciativa del orden nacional, **"Cero Papel",** la consiste en una serie de lineamientos orientados a formular una desarrollo "efectivo, eficiente y eficaz", mediante la aplicación de los ejes: "*Implantación de buenas Prácticas,* ***Sistema para la Gestión documentos electrónicos*** *y optimización y automatización de procesos*"[16]

En cuanto la Alcaldía de Ibagué, como entidad pública, prestadora de servicios a la comunidad Ibaguereña, emite y recibe anualmente un promedio de **101.439** (ver cuadro 1) P.Q.R.S "Peticiones, Quejas, Reclamos y Solicitudes"

Cuadro. 1 Estadística Peticiones

Vigencia	Correspondencia Interna	Correspondencia Externa
2018	124.991	121.005
2019	123.000	108.388
2020	61.214	70.033
Promedio por proceso	**103.068**	**99.809**
Promedio Total	**101.439**	

Fuente. Plataforma PISAMI - Alcaldía de Ibagué

Por tal razón contar con un Sistema de Gestión Documental, con los niveles de seguridad adecuados beneficia significativamente generando:

- Eficacia en la gestión de los procesos administrativos, cumpliendo con aspectos tales como:
  - Calidad en los procesos.
  - Seguimiento y control de las acciones realizadas.
  - Información veraz en línea.
  - Reducción de tiempo.
  - Aporta información relevante para la toma de decisiones.

[16] CENTRO DE INNOVACIÓN PÚBLICA DIGITAL. [Sitio Web]. Iniciativa Cero Papel MINTIC [Consulta: 17 de mayo de 2021]. Disponible: https://centrodeinnovacion.mintic.gov.co/es/experiencias/iniciativa-cero-papel-mintic

- Agiliza los procesos para el acceso de la información, puesto que garantiza veracidad en la búsqueda de información, y minimiza los tiempos de respuesta, optimizando la productividad organizacional.

- Reducción de acervo documental, en los espacios físicos tales como: Archivadores, estantería, Cajas Archivísticas.

- Reduce los riesgos de perdida y daños documentales.

- Minimiza costos de procesos archivísticos. (almacenamiento, recuperación)

4.2 MARCO CONCEPTUAL

El soporte para el desarrollo de este proyecto, se da sobre el Sistema de Gestión Documental de la Alcaldía de Ibagué; así como la metodología de riesgos MARGERIT, la cual es adaptable a los procesos y procedimientos de la entidad.

Con esta metodología busca trazar la identificación de los activos y procedimientos de gestión tecnológica, que conlleven a efectuar el análisis cualitativo y cuantitativo de escenarios que pueden tener una probabilidad de vulneración e impacto en cuanto lo identificado, con la finalidad de valorarlo y brindar una serie de controles preventivos y correctivos que permitan contribuir a la protección y tratamiento de datos de la entidad.

De esta manera para el desarrollo del presente proyecto, será necesario tener en cuenta conceptos relacionados con Seguridad de la Información, Análisis de Riesgos, metodología de riesgos entre otros términos que pueden ser considerados para la aplicación del Análisis de Riesgos del Sistema de información de la Alcaldía Municipal de Ibagué y que conllevan a generar mayor comprensión del proyecto.

Activo: Se define como activo a todo aquello que tiene un alto valor para la organización, el cual contiene información relevante y de vital importancia por lo que es necesario proteger, ello incluyendo soportes físicos, intelectuales, o informativas[17]

Amenaza: Causa potencial de un suceso no esperado, el cual puede causar un daño a un sistema u los procesos de una organización[18].

Autenticidad: Se considera como autenticidad a la seguridad de que un mensaje, transacción o intercambio de información proviene de una fuente confiable[19].

Análisis de Riesgos[20]: Según la norma ISO 31000:2018, El Análisis del Riesgo tiene como propósito alcanzar la naturaleza del riesgo y sus tipologías incluyendo cuando se adecuado el nivel del riesgo. Se puede realizar con diferentes niveles de detalle y complejidad, dependiendo objetivo del análisis, la disponibilidad y confidencialidad de la información y los recursos con los que se cuenta; este proceso se puede desarrollar mediante técnicas cualitativas, cuantitativas o combinadas.

Evaluación del Riesgo: Tiene como propósito apoyar en la toma de decisiones, mediante la comparación de resultados obtenidos en el análisis del riesgo.[21]

Gestión del Riesgo: Acciones sistematizadas orientadas a instituir estrategias, lograr objetivos y permitir la toma de decisiones en base a la información obtenida.[22].

[17] NORMA ISO 27001. [Sitio Web]. Madrid: ISO 27001 Seguridad de la Información [Consulta: 01 de mayo de 2021]. Disponible en: https://normaiso27001.es/referencias-normativas-iso-27000/#def328
[18] NORMAS ISO.[Sitio Web]. ISO 27001 Seguridad de la Información [Consulta: 01 de mayo de 2021], Disponible en: https://www.normas-iso.com/iso-27001/
[19] NORMA ISO 27001. [Sitio Web]. Madrid: Referencias Normativas Iso 27000 [Consulta: 01 de mayo de 2021]. Disponible en: https://normaiso27001.es/referencias-normativas-iso-27000/#def36
[20] ISO. [Sitio Web]. ISO 31000:2018 Gestión del Riesgo, Evaluación del Riesgo. [Consulta 01 de mayo de 2021]. Disponible en: https://www.iso.org/obp/ui/es/#iso:std:iso:31000:ed-2:v1:es
[21] Ibid.
[22] ISOTools. [Sitio Web]. ¿Cuál es la terminología que utiliza la nueva ISO 31000?. [Consulta 01 de mayo de 2021]. Disponible en: https://www.isotools.org/2018/02/28/la-terminologia-utiliza-la-nueva-iso-31000/

Incidente de Seguridad de la Información: Suceso o sucesos imprevistos de seguridad de la información, con una alta probabilidad de afectar el buen funcionamiento de la entidad y amenazar la seguridad de la información[23].

Control: Medios de gestionar el riesgo, incluyen políticas, procedimientos, directrices, practicas o estructuras de la organización que pueden ser de naturaleza administrativa, técnica y gestión o legal[24].

Mapa de Riesgos: Herramienta idónea para la identificación de riesgos de toda entidad, la cual es planteada por la Alta Dirección y personal responsable de los procesos,[25].

Valoración del Riesgo: Proceso de cotejo del riesgo considerado frente a criterios de riesgo determinados para fijar la importancia del riesgo[26].

Vulnerabilidad: Debilidad que posee un activo o conjunto de activos que puede ser aprovechada por una o gran variedad de amenazas.

[23] SISTESEG. [Sitio Web]. Recomendaciones para Estructurar Documentos de Políticas ISO 27001:2013. [Consulta: 01 de mayo de 2021] Disponible en: https://www.sisteseg.com/files/Recomendaciones_para_estructurar_documentos_de_pol_ticas_ISO_27001.pdf. p.13
[24] ISO. [Sitio Web]. ISO 3100:2018 Gestión del Riesgo - Directrices. [Consulta 01 de mayo de 2021]. Disponible en: https://www.iso.org/obp/ui#iso:std:iso:31000:ed-2:v1:es
[25] MININTERIOR. [Sitio Web]. Bogotá: Mapa de Riesgos [Consulta: 01 de mayo de 2021]. Disponible en: https://www.mininterior.gov.co/content/mapa-de-riesgos
[26] ISO. [Sitio Web]. ISO 3100:2018 Gestión del Riesgo - Directrices. [Consulta 01 de mayo de 2021]. Disponible en: https://www.iso.org/obp/ui#iso:std:iso:31000:ed-2:v1:es

4.3 MARCO LEGAL

Teniendo en cuenta el enfoque del presente proyecto a continuación se efectúa una descripción de las principales normas:

4.3.1 NORMA ISO 27001:2013:

Norma Internacional diseña por la Organización Internacional de Normalización ISO, orienta a la Seguridad de la Información la cual buscar garantizar la confidencialidad, integridad y disponibilidad de la información[27],

4.3.2 NORMA ISO 31000:2018

"Gestión del Riesgo" Norma principal en Risk Mangament establecida en 11 principios con la estructura y objetivos de la entidad u organización, relacionadas con las normativas de la implementación del riesgo[28].

4.3.3 LEY 594 DE 2000:

"Por medio de la cual se dicta la Ley General de Archivos y se dictan Otras Disposiciones[29]".

[27] NORMAS ISO. [Sitio Web]. ISO 27001 Seguridad de la Información. [Consulta: 01 de mayo de 2021]. Disponible en: https://www.normas-iso.com/iso-27001/
[28] EALDE BUSINESS SCHOOL. [Sitio Web]. Madrid: EALDE. Gestión del Riesgo. Que es la norma ISO 31000 y para qué sirve [Consulta: 01 de mayo de 2021]. Disponible en: https://www.ealde.es/iso-31000-para-que-sirve/.
[29] APC-COLOMBIA. Bo [Sitio Web]. Programa de Gestión Documental. [Consulta: 01 de mayo de 2021]. Disponible en: https://www.apccolombia.gov.co/sites/default/files/archivos_usuario/2017/a-ot-009programagestiondocumentalv5.pdf

4.3.4 Ley 527 de 1999:

“Por medio de la cual se define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las demás firmas digitales y se establecen las entidades de certificación y se dictan otras disposiciones[30].”

[30] FUNCION PUBLICA. [Sitio Web]. Ley 527 de 1999. [Consulta: 01 de mayo de 2021]. Disponible en: https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=4276

5 DISEÑO METODOLÓGICO

Para el desarrollo de los objetivos planteados en el presente proyecto, se realizará la metodología MAGERIT[31] la cual está asociada con las normas ISO 31000 y la ISO 27001:2013, dicha metodología contas de un conjunto de actividades por etapas (Inicio, análisis y diseño) enfocadas fin alcanzar los resultados del proyecto propuesto.

De esta manera a continuación se detalla las actividades a ejecutar:

5.1 PLANTEAMIENTO DE LA PROPUESTA.

En la presente etapa se ajustó el anteproyecto, conforme las observaciones planteadas por la Universidad, contando así con viabilidad para la ejecución del mismo y posterior formalización con la Alcaldía Municipal de Ibagué, Secretaría Administrativa, propietarios del Sistema de Gestión Documental, sobre la plataforma Integrada de Sistemas de la Alcaldía de Ibagué – PISAMI, quienes otorgaron autorización para la aplicación del análisis del riesgo de la plataforma objeto del presente proyecto, conforme el cronograma planteado.

Como evidencia del planteamiento y aceptación, se adjunta el anexo 1: Autorización Empresa V1 y anexo 2: Acuerdo de confidencialidad - Empresa Estudiante V1, firmados por la Secretaría Administrativa Doctora Juliana Cuartas Candamil.

5.2 RECOLECCIÓN DE INFORMACIÓN.

Con el fin de reconocer los lineamientos con los cuales se desarrolla la plataforma en la se desarrolla Sistema de Gestión Documental, características de su funcionamiento y

[31] GOBIERNO DE ESPAÑA. [Sitio Web]. MAGERIT v.3 : Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. España. Administración Electrónica. [Consulta: 17 de mayo 2021]. Disponible en: https://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_Magerit.html

estado actual de su seguridad en la infraestructura Tecnológica en la cual se aloja la información, se efectuó las siguientes actividades:

1. Entrevista con el coordinador del Grupo de Ciencia, Tecnología e Información (Desarrollo) y Grupo de Infraestructura Tecnológica (soporte), los cuales se evidencian en los anexos C y D.

2. Revisión ocular de las áreas administrativas de la Alcaldía Municipal de Ibagué, ubicadas en el palacio municipal dependencias, efectuó lista de chequeo.

5.3 ETAPA DISEÑO:

Determinar la metodología aplicar para el desarrollo del análisis de riesgo de seguridad del Sistema de Gestión Documental de la Alcaldía de Ibagué.

Para el desarrollo de la metodología, se realizará análisis y gestión de los riesgos del Sistema de Gestión Documental de la Alcaldía de Ibagué, con la aplicación de la metodología MARGERIT, asociada en el marco de la norma ISO 31000:2018 para la Gestión del Riesgo y Norma ISO 27001:2013.

De esta manera la Gestión del Riesgo se encuentra dividida en dos acciones principales, las cuales corresponden a: Análisis de riesgo y tratamiento de riesgos, en cuanto análisis de riesgo, este atañe específicamente a los activos, amenazas y salvaguardas, con la cual permite obtener un resultado del estado de la entidad u organización y estimado de lo que podría pasar en cuanto su nivel de seguridad y tratamiento de riesgos, permite minimizar los riesgos a nivel residual, asumido por la alta dirección, generando con ello una contribución a la protección y tratamiento adecuado de los datos.

6 APLICAR LA METODOLOGÍA MARGERIT PARA LA EVALUACIÓN DE RIESGOS QUE PERMITA IDENTIFICAR VULNERABILIDADES Y AMENAZAS DE SEGURIDAD, ASÍ COMO EVALUAR LOS RIESGOS CONFORME LO ESTABLECE LA METODOLOGÍA.

Con el fin de aplicar la metodología MARGERIT para la evaluación de riesgos que permita identificar las vulnerabilidades y amenazas de seguridad de la información del Sistema de Gestión Documental de la Administración Municipal de Ibagué, fue necesario tomar como base lo enmarcado en la norma ISO 31000:2018 y 27001:2013, para lo cual se procedió a determinar como primera medida lo siguiente:

6.1 RECOLECCIÓN DE LA INFORMACIÓN:

Para la recolección de la información necesaria para el desarrollo del proyecto fue necesario recopilar de datos y/o documentos alojados el sitio web de la Alcaldía Municipal, los cuales aportaron como herramienta de trabajo para identificar las políticas, Planeas y Programas implementados por la misma, en pro de proteger la información y los activos de informáticos, de amenazas, vulnerabilidades, garantizando la integridad, confidencialidad y disponibilidad de la información.

Así mismo se recopiló información sensible de la entidad, en relación a los activos tecnológicos, por medio de entrevistas realizada a funcionarios responsables de las áreas de Ciencia, Tecnología e Información; Infraestructura Tecnología y Dirección de Talento Humano.

Como evidencia de lo anteriormente citado a continuación, se detalla la información recopilada la cual se divide en:

6.1.1 Información General de la Organización:

Como resultado de la ejecución de cada uno de los procesos para la identificación, clasificación, criticidad y categorización de activos de la información, se procede a

efectuar el levantamiento de la información dando cumpliendo con los estándares establecidos en la norma ISO 27001:2013.

Para iniciar, se realizó reunión con los profesionales Universitario líderes del grupo de la Ciencia Tecnología e Innovación y el Grupo de Infraestructura Tecnológica **,** con el fin de solicitar la información correspondiente a los activos de la Administración Municipal, quienes posterior a la reunión efectuaron entrega referente a los activos tales como: **Aplicaciones, Hardware, Red, Tecnología Equipamiento Auxiliar**, conforme se acordó en el Acta Reunión No. 001, anexo C, dicho proceso se realiza previa autorización efectuada por parte de la Secretaria Administrativa, quien es la responsable del Sistema de Gestión Documental.

Así mismo se efectuó reunión con el profesional especializado adscrita a la Secretaria Administrativa, responsable de la información correspondiente a la estructura organizacional de la Administración Municipal, quien suministro información referente a los activos: Personal e Instalaciones, la cual se evidenciar en el Anexo D “Acta de Reunión 02”

Teniendo en cuenta la información suministrada por parte de la profesional, se evidencia que la Alcaldía de Ibagué cuenta con un total activo de personal de **2.464** (ver tabla 6) entre funcionarios de planta y contratistas, distribuidos entre **102** dependencias. Ver tabla 7, de la manera se anexa el Organigrama Institucional de la Administración Municipal (Ver Anexo: E) con el fin de evidenciar la distribución.

Tabla 1. Activo Persona

Alcalde	1
Secretarios	15
Jefes de oficina	5
Directores	38
Asesores	60
Carrera - prov.	645
Contratistas	1.700
TOTA	**2.464**

Fuente. 1. El autor

Tabla 2. Cantidad Dependencias

Dependencia	Cant
Despacho alcalde	1
Secretarías	15
Gerencias	1
Direcciones	38
Oficinas	5
Grupos	42
TOTAL	**102**

Fuente. 2. El autor

6.1.2 Información Específica del Sistema:

Una vez efectuado el levantamiento de información General de la Administración Municipal, se procedió a recopilar datos precisos del sistema de Gestión Documental, que servirá como herramienta de trabajo para la aplicación de la metodología MARGERIT, para ello se efectuó entrevista (Ver: Anexo H) personalizada a funcionarios de planta con funciones relacionadas al Sistema de Gestión Documental, en la Plataforma PISAMI:

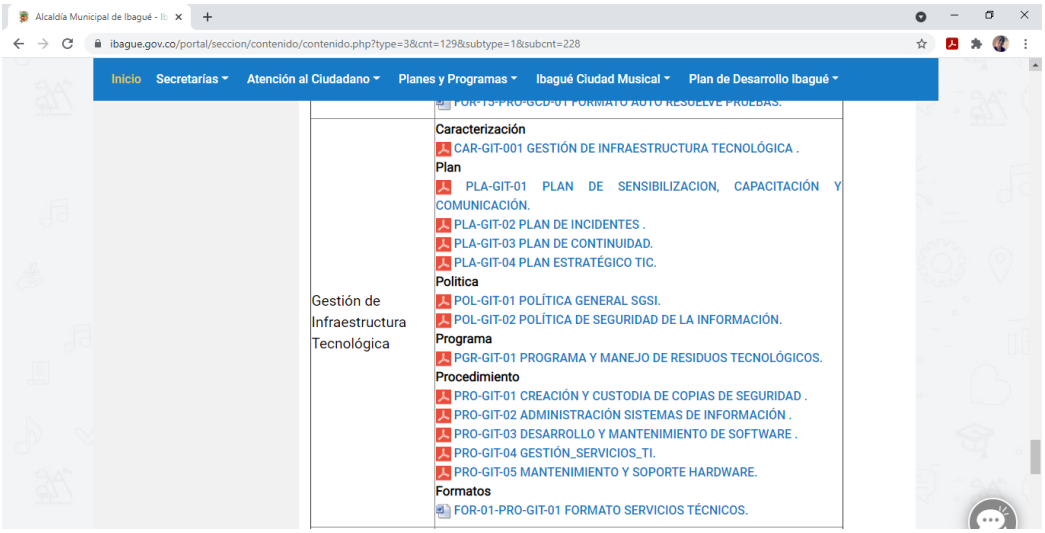
Tabla 3. Dependencias Encuestadas

Dependencia	Responsabilidad / Procesos	Cargo
Despacho Secretaría Administrativa	Proceso Gestión de Documental.	Técnico Operativo
Dirección de Recursos Físicos.	Proceso Gestión de Documental.	Técnico Operativo
Dirección de Talento Humano	Proceso Gestión de Documental.	Técnico Operativo
Grupo de Ciencia, Tecnología e Innovación	Responsable Aplicaciones – Plataforma PISAMI.	Profesional Universitario – Coordinador
Grupo Infraestructura Tecnológica.	Responsable Hardware, Red,	Profesional Universitario – Coordinador

Fuente. El Autor

Así mismo, se efectuó revisión de la información publicada en la página web de la Administración Municipal, en relación a los procesos de Infraestructura Tecnológica y Gestión Documental, para ello fue necesario acceder al link: https://ibague.gov.co/portal/seccion/contenido/contenido.php?type=3&cnt=129&subtype=1&subcnt=228[32], en el cual se enuncian los activos de datos que la conforman como se observa en la figura No. 4.

Figura 1. Activo Datos – Infraestructura Tecnológica



Fuente. ALCALDÍA MUNICIPAL DE IBAGUÉ. [Sitio Web]. Ibagué: Alcaldía. [Consulta: 29 de septiembre 2021] https://ibague.gov.co/portal/seccion/contenido/contenido.php?type=3&cnt=129&subtype=1&subcnt=228

Tabla 4. Proceso Infraestructura Tecnológica

Código	Documento
CAR-GIT.001	Gestión de Infraestructura Tecnológica[33].

[32] ALCALDÍA MUNICIPAL DE IBAGUÉ. [Sitio Web]. Sistema Integrado de Gestión. Ibagué. [Consulta: 01 de mayo de 2021]. Disponible en: https://ibague.gov.co/portal/seccion/contenido/contenido.php?type=3&cnt=129&subtype=1&subcnt=228

[33] ALCALDÍA MUNICIPAL DE IBAGUÉ. [Sitio Web]. Ibagué, Gestión de Infraestructura Tecnológica. [Consulta: 29 de septiembre de 2021]. Disponible en: https://ibague.gov.co/portal/admin/archivos/publicaciones/2020/25046-DOC-20200814093308.pdf

Código	Documento
PLA-GIT-01	Plan de sensibilización capacitación y Comunicación.[34]
PLA-GIT-02	Plan de Incidentes[35]
PLA-GIT-03	Plan de Continuidad[36]
PLA-GIT-04	Plan Estratégico de TIC[37]
POL-GIT-01	Política General de SGSI[38]
POL-GIT-02	Política de Seguridad de la Información[39]
PGR-GIT-01	Programa y Manejo de Residuos Tecnológicos.[40]
PRO-GIT-01	Creación y Custodia de Copias de Seguridad[41].
PRO-GIT-03	Desarrollo y Mantenimiento de Software[42]
PRO-GIT-04	Gestión de Servicios T.I.[43]
PRO-GIT-05	Mantenimiento y Soporte Hardware[44]

Fuente. ALCALDÍA MUNICIPAL DE IBAGUÉ. [Sitio Web]. Ibagué: Alcaldía. [Consulta: 29 de septiembre 2021] https://ibague.gov.co/portal/seccion/contenido/contenido.php?type=3&cnt=129&subtype=1&subcnt=228

[34] ALCALDÍA MUNICIPAL DE IBAGUÉ. [Sitio Web]. Ibagué, Plan de Sensibilización Capacitación y Comunicación. [Consulta: 29 de septiembre de 2021]. Disponible en: https://ibague.gov.co/portal/admin/archivos/publicaciones/2019/29355-DOC-20191221.pdf

[35] ALCALDÍA MUNICIPAL DE IBAGUÉ. [Sitio Web]. Ibagué, Plan de Incidentes. [Consulta: 29 de septiembre de 2021]. Disponible en: https://ibague.gov.co/portal/admin/archivos/publicaciones/2019/29356-DOC-20191222.pdf

[36] ALCALDÍA MUNICIPAL DE IBAGUÉ. [Sitio Web]. Ibagué, Plan de Continuidad. [Consulta: 29 de septiembre de 2021]. Disponible en: https://ibague.gov.co/portal/admin/archivos/publicaciones/2019/29357-DOC-20191223.pdf

[37] ALCALDÍA MUNICIPAL DE IBAGUÉ. [Sitio Web]. Ibagué. Plan Estratégico de TIC. [Consulta: 29 de septiembre de 2021]. Disponible en: https://ibague.gov.co/portal/admin/archivos/publicaciones/2019/29358-DOC-20191224.pdf

[38] ALCALDÍA MUNICIPAL DE IBAGUÉ. [Sitio Web]. Ibagué. Política General de SGSI. [Consulta: 29 de septiembre de 2021]. Disponible en: https://ibague.gov.co/portal/admin/archivos/publicaciones/2021/25289-DOC-20210511151205.pdf

[39] ALCALDÍA MUNICIPAL DE IBAGUÉ. [Sitio Web]. Ibagué. Política de Seguridad de la Información. [Consulta: 29 de septiembre de 2021]. Disponible en: https://ibague.gov.co/portal/admin/archivos/publicaciones/2021/25290-DOC-20210511151206.pdf

[40] ALCALDÍA MUNICIPAL DE IBAGUÉ. [Sitio Web]. Ibagué. Programa y Manejo de Residuos Tecnológicos. [Consulta: 29 de septiembre de 2021]. Disponible en: https://ibague.gov.co/portal/admin/archivos/publicaciones/2019/25049-DOC-20191127143142.pdf

[41] ALCALDÍA MUNICIPAL DE IBAGUÉ. [Sitio Web]. Ibagué. Creación y Custodia de Copias de Seguridad de la Información. [Consulta: 29 de septiembre de 2021]. Disponible en: https://ibague.gov.co/portal/admin/archivos/publicaciones/2019/25050-DOC-20191127142431.pdf

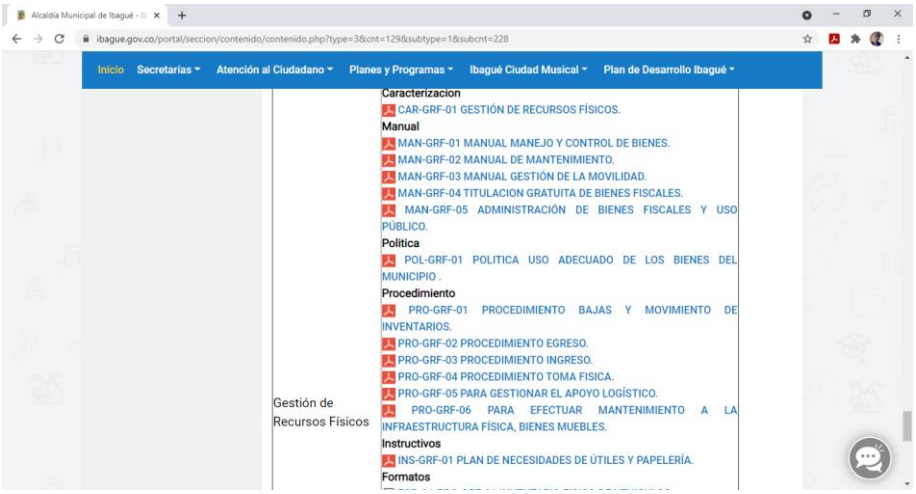
[42] ALCALDÍA MUNICIPAL DE IBAGUÉ. [Sitio Web]. Ibagué. Desarrollo y Mantenimiento de Software. .[Consulta: 29 de septiembre de 2021]. Disponible en: https://ibague.gov.co/portal/admin/archivos/publicaciones/2019/25054-DOC-20191127144526.pdf

[43] ALCALDÍA MUNICIPAL DE IBAGUÉ. [Sitio Web]. Ibagué. Gestión de Servicios. [Consulta: 29 de septiembre de 2021]. Disponible en: https://ibague.gov.co/portal/admin/archivos/publicaciones/2019/26883-DOC-20191127143617.pdf

[44] ALCALDÍA MUNICIPAL DE IBAGUÉ. [Sitio Web]. Ibagué. Gestión de Servicios. [Consulta: 29 de septiembre de 2021]. Disponible en: https://ibague.gov.co/portal/admin/archivos/publicaciones/2019/27438-DOC-20191127144210.pdf

Dentro del proceso de identificación de activos de datos, se pudo evidenciar que la Administración Municipal cuenta con información relacionada a Sistema de Gestión Documental en su sitio web, como evidencia en la figura No. 5.

Figura 2. Información Gestión Documental



Fuente. ALCALDÍA MUNICIPAL DE IBAGUÉ. [Sitio Web]. Ibagué: Alcaldía. [Consulta: 29 de septiembre 2021] https://ibague.gov.co/portal/seccion/contenido/contenido.php?type=3&cnt=129&subtype=1&subcnt=228

Tabla 5. Proceso Gestión Documental

Código	Documento
PGR-01	Programa de Gestión Documental[45]
PRO-GD-01	Conservación Documental[46]
PRO-PGD-10	Planeación de la Gestión Documental.[47]

Fuente. ALCALDÍA MUNICIPAL DE IBAGUÉ. [Sitio Web]. Ibagué: Alcaldía. [Consulta: 29 de septiembre 2021] https://ibague.gov.co/portal/seccion/contenido/contenido.php?type=3&cnt=129&subtype=1&subcnt=228

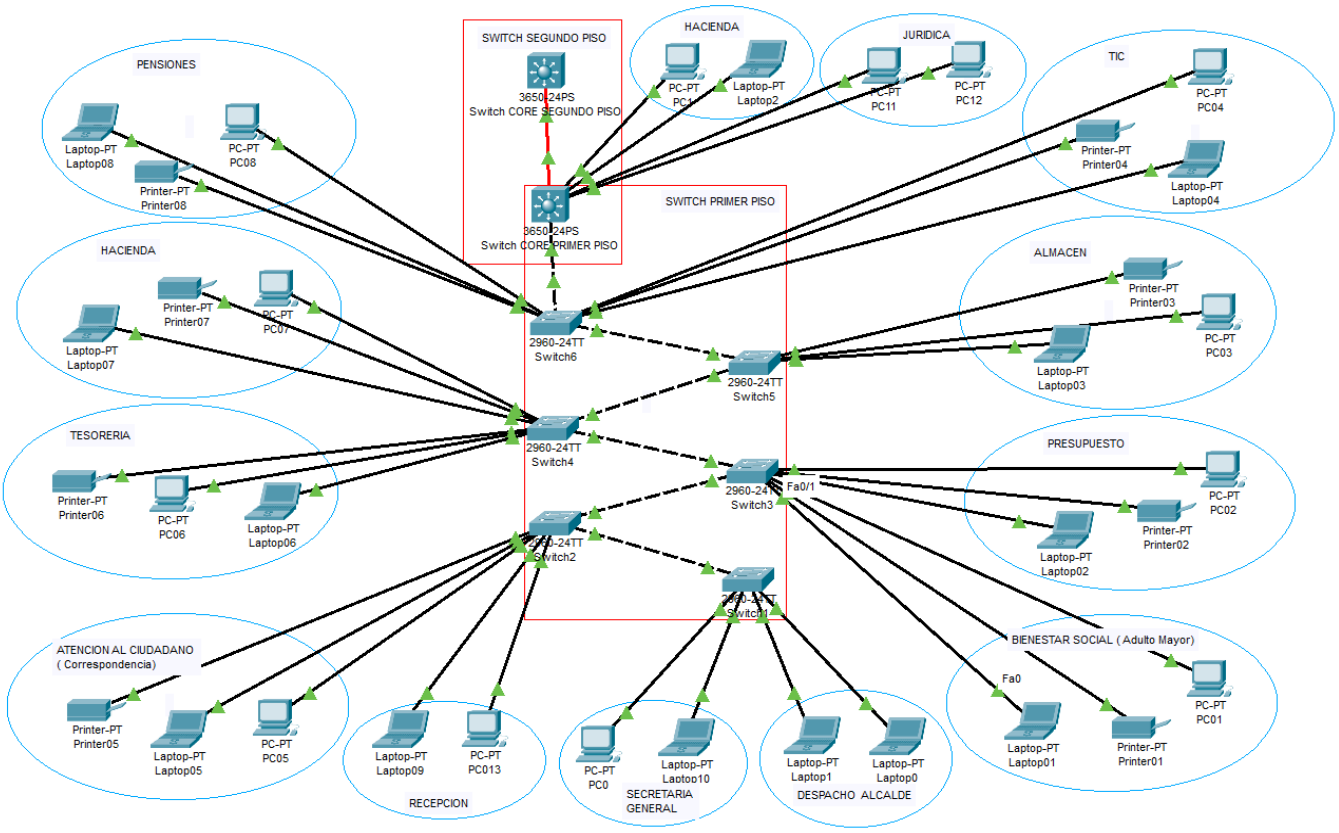
[45] ALCALDÍA MUNICIPAL DE IBAGUÉ. [Sitio Web]. Ibagué. Programa de Gestión Documental. [Consulta: 29 de septiembre de 2021]. Disponible en: https://ibague.gov.co/portal/admin/archivos/publicaciones/2018/18801-DOC-20181022.pdf

[46] ALCALDÍA MUNICIPAL DE IBAGUÉ. [Sitio Web]. Ibagué. Conservación Documental. [Consulta: 29 de septiembre de 2021]. Disponible en: https://ibague.gov.co/portal/admin/archivos/publicaciones/2017/18768-DOC-20171101.pdf

[47] ALCALDÍA MUNICIPAL DE IBAGUÉ. [Sitio Web]. Ibagué. Planeación de Gestión Documental. [Consulta: 29 de septiembre de 2021]. Disponible en: https://ibague.gov.co/portal/admin/archivos/publicaciones/2019/18777-DOC-20191107091316.pdf

En cuanto la RED de la entidad, está establecida la topología tipo Estrella, los dispositivos terciarios se encuentran alojados en el cuarto de telecomunicaciones de la Secretaria de las TIC, allí se cuenta con un Firewall Fortinet el cual tiene configuradas las políticas de acceso y denegación, en uno de sus puertos esta interconectado al Router del ISP media Commerce el cual suministra el internet y enlaza las sedes externas de la administración las cuales cuentan con sus respectivos Router también del ISP, así como se puede evidenciar en la figura No. 6.

Figura 3. Topología de Red



Fuente. Alcaldía Municipal de Ibagué

Así mismo, teniendo en cuenta la robustez de la información suministrada en cuanto personal y activos a nivel de toda la Alcaldía, se prioriza el análisis de Riesgo de las áreas que tiene principal responsabilidad y afectación en el Sistema de Gestión Documental, así como se enuncia en la tabla 8. y anexo 07

Tabla 6. Procesos a Analizar

Dependencia	Responsabilidad / Procesos	Cargo
Despacho Secretaría Administrativa	Responsable Sistema de Gestión Documental.	Secretario
Dirección de Recursos Físicos.	Proceso Gestión de Recursos Físicos -	Director
Dirección de Talento Humano	Gestión Talento Humano	
Grupo de Ciencia, Tecnología e Innovación	Responsable Aplicaciones – Plataforma PISAMI.	Profesional Universitario – Coordinador
Grupo Infraestructura Tecnológica.	Responsable Hardware, Red,	Profesional Universitario – Coordinador

Fuente. 3. El autor

Una vez se cuento con los datos totales de los Activos de Información de la Administración Municipal y demás información necesaria para el desarrollo del proyecto, se procedió con el Análisis del Riesgo, para lo cual siguiendo lo citado en la norma i la clasificación de la información, de acuerdo a lo establecido en la norma ISO 27001:2013 y Guías de MINTIC, previa depuración de la información, ver anexo 06 e Figura 7 a la 9.

6.2 ANÁLISIS DE RIESGOS:

Para el desarrollo del análisis de Riesgos, la metodología MARGERIT establece una serie de puntos esenciales idóneos para la obtención de un resultado efectivo.

6.2.1 Identificación de Activos:

En la identificación de activos se efectuó a su vez la categorización de cada uno de ellos, conforme lo establecido en Libro II: Catálogo de Elementos de la Metodología MARGERIT[48], el proceso de identificación se prioriza los activos que sean de

[48] ADMINISTRACIÓN ELECTRÓNICA [Sitio Web] MARGERIT v.3 Metodología de Análisis y Gestión de los Riesgos de los Sistemas de Información. [Consulta: 01 de mayo de 2021]. Disponible

importancia operativa para la organización, los cuales son esenciales para el cumplimiento de sus objetivos.

Tabla 7. Categorización

[D]	**Datos**
[K]	Claves criptográficas
[S]	Servicios
[SW]	Software
[HW]	Equipamiento informático
[COM]	Redes de comunicaciones
[AUX]	Equipamiento auxiliar
[L]	Instalaciones
[P]	Personal

Fuente. El Autor

Para iniciar, es pertinente determinar con exactitud que activos se tratan en la organización para posterior a ello detallar los tipos de activos[49].

Figura 4. Tipo de Activos

Fuente. El autor

en:https://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_Magerit.html

[49] INCIBE-CERT. [Sitio Web]. Inventario de Activos y Gestión de Seguridad en SCI. España. [Consulta 18 de mayo de 2021] Disponible en: https://www.incibe-cert.es/blog/inventario-activos-y-gestion-seguridad-sci

Teniendo en cuenta los conceptos anteriormente descritos, a continuación, se relaciona los activos identificados en la Administración Municipal y que a su vez hacen parte del proceso del Sistema de Gestión Documental.

Tabla 8. Identificación de Activos

SIGLA	TIPO DE ACTIVO	ACTIVO	CANT	UBICACIÓN	OBSERVACIÓN
[D] DATOS INFORMACIÓN					
[fikes]	Ficheros	Datos Correspondencia Interna y Externa		Secretaría de la TIC, Grupo Ciencia, Tecnología e Innovación	
[backu]	Copias de Respaldo	Copias de Seguridad		Secretaría de la TIC, Ciencia, Tecnología e Innovación	Copias: Sistemas de Información - Servidores Virtuales
[conf]	Datos de Configuración	Configuración de Equipos Propios del Centro		Secretaría de la TIC, Ciencia, Tecnología e Innovación	Servidores, Equipos y otros
[int]	Datos de Gestión Interna	Bases de Datos		Secretaría de la TIC, Ciencia, Tecnología e Innovación	Sistema de Registro y Control
[password]	Credenciales	Contraseñas		Secretaría de la TIC, Ciencia, Tecnología e Innovación	Acceso a la Plataforma PISAMI.
[acl]	Datos de Control de acceso	Datos de Control de Acceso del CentOs		Secretaría de la TIC, Ciencia, Tecnología e Innovación	Asignación de Permisos.
[K] CLAVES CRIPTOGRÁFICAS					
[inf]	Protección de la Información	Protección de la Información Correos Institucionales		Secretaría de la TIC, Grupo de Infraestructura Tecnológica	
[com]	Protección de las Comunicaciones	Protección de las Comunicaciones - Voz IP		Secretaría de la TIC, Grupo de Infraestructura Tecnológica	

SIGLA	TIPO DE ACTIVO	ACTIVO	CANT	UBICACIÓN	OBSERVACIÓN
		Protección de las Comunicaciones - Wifi		Secretaría de la TIC, Grupo de Infraestructura Tecnológica	
[S] SERVICIOS					
[int]	Interno	Servicios de Impresión		Secretaría de la TIC, Grupo de Infraestructura Tecnológica	
[int]	Interno	Servicio Soporte Técnico		Secretaría de la TIC, Grupo de Infraestructura Tecnológica	
[www]	World Wide Web	Servicios Pagina Web Institucional	1	Secretaría de la TIC, Grupo de Infraestructura Tecnológica	dominio1.edu.co
[email]	Correo Electrónico	Servicio Correo Electrónico - Google Sites	1	Secretaría de la TIC, Grupo de Infraestructura Tecnológica	correodominio1@.edu.co
[ftp]	Transferencia de Ficheros	Transferencia de Archivos		Secretaría de la TIC, Grupo de Infraestructura Tecnológica	
[idm]	Gestión de identidades	Gestión de usuarios y Contraseñas		Secretaría de la TIC, Grupo de Infraestructura Tecnológica	
[SW] APLICACIONES (SOFTWARE)					
[prp]	Desarrollo Propio	Plataforma PISAMI	1	Secretaría de la TIC, Ciencia, Tecnología e Innovación	http://pisami.ibague.gov.co
[std]	Estándar	PHP y Larabel	1	Secretaría de la TIC, Ciencia, Tecnología e Innovación	
[browser]	Navegador Web	Apache	1	Secretaría de la TIC, Ciencia, Tecnología e Innovación	

SIGLA	TIPO DE ACTIVO	ACTIVO	CANT	UBICACIÓN	OBSERVACIÓN
[app]	Servidor de Aplicaciones	Windows 2016 Server Linux CentOS 7		Secretaría de la TIC, Ciencia, Tecnología e Innovación	
[file]	Servidor de ficheros	Joomla V.2.5		Secretaría de la TIC, Ciencia, Tecnología e Innovación	
[dbms]	Sistema de Gestión de Bases de Datos	Bases de Datos MySQL	1	Secretaría de la TIC, Ciencia, Tecnología e Innovación	
		Oracle 10G	1	Secretaría de la TIC, Ciencia, Tecnología e Innovación	
[av]	Anti virus	Avira		Secretaría de la TIC, Ciencia, Tecnología e Innovación	
[os]	Sistema Operativo	Windows 10 Pro		Secretaría de la TIC, Ciencia, Tecnología e Innovación	
[HW] EQUIPOS INFORMÁTICOS (HARDWARE)					
[host]	Grandes Equipos	Servidor de Archivos FTP - Marca: DELL en Torre PowerEdge T130	1	Antigua Oficina de Sistemas	Administración de almacenamiento y administración de archivos. Solo puede acceder al Servidor personas autorizadas.
		Servidor DHCP - Marca: Dell en Torre PowerEdge T440	1	Antigua Oficina de Sistemas	
		Servidor DHCP - Marca: Dell en Torre PowerEdge T440	1	Antigua Oficina de Sistemas	
[mid]	Equipos Medios	Equipos de Computo	1	Secretaría de las TIC - Despacho	

SIGLA	TIPO DE ACTIVO	ACTIVO	CANT	UBICACIÓN	OBSERVACIÓN
		Equipos de Computo	6	Grupo de Ciencia, Tecnología e Innovación	
		Equipos de Computo	2	Grupo de Infraestructura Tecnológica	
		Equipos de Computo	1	Secretaría Administrativa	
		Equipos de Computo	8	Grupo de Recursos Físicos	
		Grupo de Talento Humano	7	Grupo de Talento Humano	
[peripheral]		**Periféricos**			
[print]	Medios de Impresión	Impresora Marca: HP LASERJET M1212NF	1	Secretaría de las TIC - Grupo Ciencia, Tecnología e Innovación	Se establece conexión entre más PC
		Impresora Marca: HP LASERJET ENTERPRISE M608	1	Secretaría de las TIC - Grupo Infraestructura Tecnológica	
		Impresora Marca: HP LASERJET PRO MFP M426FDW	1	Secretaría Administrativa - Despacho	
		Impresora Marca: HP LASERJET P4515x	1	Secretaría de las TIC	
		Impresora Marca: LASERJET 600 M603	1	Secretaría Administrativa - Despacho - Dirección de Recursos Físicos	
		Impresora Marca: HP OFFICEJET PRO 8600	1	Secretaría Administrativa - Despacho - Dirección de Recursos Físicos	
		Impresora Marca: HP LASERJET M1522N	1	Secretaría Administrativa - Dirección de Talento Humano	
		Impresora Marca: KYOCERA FS-1035MFP	1	Secretaría Administrativa - Dirección de Talento Humano	

SIGLA	TIPO DE ACTIVO	ACTIVO	CANT	UBICACIÓN	OBSERVACIÓN
[network]		**Soporte de la Red**			
[hub]	Concentradores	Puntos de Acceso Alámbricos		Red de Datos - Centro	Interconexión de la red de datos.
[switch]	Conmutadores	Swtches: Marca ArubaOS-Switch, ARUBA 2530 24G	6	Red de Datos - Secretaría Administrativa	Interconexión de la red de datos.
[firewall]	Cortafuegos	Cortafuegos Cisco ASA 5505	1	Secretaría de las TIC	Protección a la Red de Datos.
[wab]	Punto de acceso inalámbrico	Puntos de Acceso	2	Secretaría de las TIC	Puntos de acceso servicio internet Alcaldía de Ibagué
[ipphone]	Teléfono IP	Teléfono IP	6	Dependencias	Voz IP - Comunicación Despacho Secretarias y Direcciones.
		[COM] REDES DE COMUNICACIONES			
[ISDN]	Red Digital	Sistema Comunicación Voz IP		Palacio Municipal de Ibagué	
[wifi]	Red Inalámbrica	Red Inalámbrica - Institucional		Palacio Municipal de Ibagué	
[LAN]	Red Local	Red Local Institucional		Palacio Municipal de Ibagué	
[Internet]	Internet	Internet Centro		Palacio Municipal de Ibagué	
		[Media] SOPORTES DE INFORMACIÓN			
[vdisk]	Discos Virtuales	Cloud Plus		Departamento de Sistemas	
		[AUX] EQUIPAMIENTO AUXILIAR			
[ups]	Sistemas e Alimentación Ininterrumpida	UPS del Centro		Datacenter	
[cabling]	Cableado	Cableado Eléctrico		Palacio Municipal de Ibagué	
[cabling]	Cableado	Cableado Estructurado		Palacio Municipal de Ibagué	
		[L] INSTALACIONES			
[building]	Edificio	Instalaciones Palacio		Palacio Municipal de Ibagué	Oficina Secretaría de las TIC (Despacho y Grupos), Secretaria Administrativa

SIGLA	TIPO DE ACTIVO	ACTIVO	CANT	UBICACIÓN	OBSERVACIÓN
					(Despacho y Direcciones)
		[P] PERSONAL			
[ue]	Usuarios Externos	Comunidad Ibaguereña		Palacio Municipal de Ibagué	
[ui]	Usuarios Internos	Funcionarios de Planta y Contratistas	75	Palacio Municipal de Ibagué	Secretaría de las TIC (Despacho y Grupos), Secretaria Administrativa (Despacho y Direcciones)
[adm]	Administradores de Sistemas	Técnicos/Auxiliares de Mantenimiento	2	Secretaría de las TIC, Grupo Infraestructura Tecnológica	
[des]	Desarrolladores / Programadores	Profesionales		Secretaría de las TIC, Grupo de Ciencia, Tecnología e Innovación	Desarrollo de Plataforma PISAMI
[prov]	Proveedores	Servicio Web: MEDIA COMMERCE PARTNERS	1	Secretaría de las TIC	Plan Máximo
		Servicio Correo Institucional: ITO SOFTWARE SAS	1	Secretaría de las TIC	dominio @ibague.gov.co

Fuente. El Autor

6.2.2 Clasificación de Activos de información

De esta manera con el fin de realizar una correcta clasificación de la información, fue necesario aplicar lo establecido por la norma ISO 27001 y lo planteado por el Ministerio de las Tecnología y Telecomunicaciones MINTIC[50], los cuales determinan clasificar la información dado cumplimiento a los tres pilares de la información como los son la confidencialidad, integridad y disponibilidad, los cuales a continuación se describen de manera detallada:

[50] MINTIC. [Sitio Web]. Guía para la Gestión y Clasificación de Activos de la Información. Bogotá: EALDE. [Consulta 17 de mayo de 2021]. Disponible en: https://www.mintic.gov.co/gestionti/615/articles-5482_G5_Gestion_Clasificacion.pdf

6.2.2.1 Clasificación en cuanto la confidencialidad:

Se enfoca en la no disponibilidad de la información sensible de la organización, la cual no debe ser expuesta a terceros y/o divulgada a personal no autorizado, dicha clasificación se define en tres niveles propuesto por MINTIC y la norma ISO 27001, que consisten en:

Tabla 9. Clasificación Confidencial.

1. INFORMACIÓN PUBLICA RESERVADA	2. INFORMACIÓN PUBLICA CLASIFICADA
Información destinada para un fin en específico la cual puede ser suministrada a un tercero, pero con previa autorización, la entrega de la misma a personal no autorizado podría generar daños irreversibles en cuanto recurso económico, afectaciones legales o perdida de la imagen institucional de la entidad.	Información sensible de la entidad, necesaria para el desarrollo de los procesos, la cual en caso de ser adquirida por un tercero podría generar fallas relevantes en los procesos y procedimientos internos de la entidad.
3. INFORMACIÓN PUBLICA	**4. NO CLASIFICADA**
Corresponde a la información que está a disposición del cliente tanto interno como externo, la cual podrá ser suministrada sin restricción alguna y el suministro del mismo no acarrea ninguna afectación a la entidad.	Hace referencia a los activos de información faltantes por incluir en el inventario, los cuales no han sido clasificados, generando con ello que sean relacionados como activos de información pública reservada.

Fuente. MINTIC. Guía para la Gestión y Clasificación de Activos de Información.

6.2.2.2 Clasificación en cuanto la Integridad:

La integridad de los activos hace relación a la disposición con la que debe contar la información, garantizando que sea completa, que se reconozca por su la exactitud, presión; así mismo cuenta con una clasificación especifica la cual se detalla a continuación:

Tabla 10. Clasificación Activos - Integridad

Nivel	Detalle
A – Alta	Información precisa y compleja de alto grado de sensibilidad, la cual en caso de pérdida genera un impacto perjudicial para la organización, ocasionando así pérdidas económicas, problemas legales, perdida de Figura institucional, complicando así el correcto funcionamiento de la misma
M - Mediano	Información precisa y compleja de alto grado de sensibilidad, la cual en caso de pérdida genera un impacto perjudicial para la organización, ocasionando así pérdidas económicas, problemas legales, perdida de Figura institucional moderado, complicando así el correcto funcionamiento de la misma
B- Bajo	Información precisa y compleja de alto grado de sensibilidad, la cual en caso de pérdida genera un impacto no relevante para la organización o clientes externos.
No Clasificada	Activos de información faltantes por incluir en el inventario, los cuales no han sido clasificados, generando con ello que sean relacionados como activos de información integridad **ALTA**.

Fuente. MINTIC. Guía para la Gestión y Clasificación de Activos de Información.

6.2.2.3 Clasificación en cuanto la Disponibilidad:

La presente clasificación corresponde a que la información debe ser de fácil acceso y funcional por petición de un tercero o proceso autorizado en los plazos y manera en que lo soliciten[51].

[51] MINTIC. Guía para la Gestión y Clasificación de Activos de Información. [en línea]. Bogotá: MINTIC. [Consultado 17 de mayo 2021]. Disponible en https://www.mintic.gov.co/gestionti/615/articles-5482_G5_Gestion_Clasificacion.pdf#page=16&zoom=100,148,133.

Tabla 11. Clasificación Activos - Disponibilidad

Nivel	Detalle
1 – Alta	El no contar con la disponibilidad de la información puede generar un impacto perjudicial para la organización, generando con ello, problemas económicos, legales y perdida de la imagen institucional, complicando así el correcto funcionamiento de la misma.
2 - Mediano	El no contar con la disponibilidad de la información puede generar un impacto perjudicial para la organización, generando con ello, problemas económicos, legales y perdida de la imagen institucional, complicando así el correcto funcionamiento de la misma.
3 - Bajo	El no contar con la disponibilidad de la información puede causar afectación a la ejecución del proceso de las organizaciones, no obstante, no genera afectaciones legales, económicas y/&o perdida de Figura genera institucional.
4 - No Clasificada	Activos de información faltantes por incluir en el inventario, los cuales no han sido clasificados, generando con ello que sean relacionados como activos de información disponibilidad **ALTA**.

Fuente. MINTIC. Guía para la Gestión y Clasificación de Activos de Información.

Basados en los conceptos descritos, a continuación, se relaciona la clasificación de los activos.

Tabla 12. Clasificación de Activos

Ítem	DATOS DEL ACTIVO DE INFORMACIÓN						1. CLASIFICACIÓN DE ACTIVOS DE LA INFORMACIÓN									
							Confidencialidad				Integridad				Disponibilidad			
	Categoría de Activos	Proceso	Nombre del Activo	Propietario del Activo	Responsable	Descripción	Reservada	Clasificada	Pública	No Clasificada	A - Alta	M - Mediano	B - Bajo	No Clasificada	1 - Alta	2 Mediano	3 - Bajo	4 - No Clasificada
1	Datos	Gestión Documental	CAR-GD-01 Gestión Documental.	Dirección de Recursos Físicos - Grupo Gestión Documental	Profesional Universitario	Caracterización del proceso en el cual se especifica las entradas salidas y beneficiarios,			X				X			X		
2	Datos	Gestión Documental	PGR-GD-01 Programa de Gestión Documental.	Dirección de Recursos Físicos - Grupo Gestión Documental	Profesional Universitario	Detalle de las funciones, procesos y procedimientos de programa			X				X			X		
3	Datos	Gestión Documental	PRO-PGD-10 Planeación de la Gestión Documental.	Dirección de Recursos Físicos - Grupo Gestión Documental	Profesional Universitario	Planeación de cada uno de los procesos ejecutados por el programa			X				X			X		
4	Datos	Gestión Documental	PLA-GD-02 Plan de Conservación Documental.	Dirección de Recursos Físicos - Grupo Gestión Documental	Profesional Universitario	Se detalla los pasos y procedimientos para la conservación			X				X			X		

Ítem	DATOS DEL ACTIVO DE INFORMACIÓN						1. CLASIFICACIÓN DE ACTIVOS DE LA INFORMACIÓN									
							Confidencialidad				Integridad			Disponibilidad		
	Categoría de Activos	Proceso	Nombre del Activo	Propietario del Activo	Responsable	Descripción	Reservada	Clasificada	Pública	No Clasificada	A - Alta	M - Mediano	B - Bajo	No Clasificada	1 - Alta	2 Mediano	3 - Bajo	4 - No Clasificada
						del acervo documental												
5	Datos	Gestión de Infraestructura Tecnológica	PLA-GIT-02 Plan de incidentes .	Secretaría de las TIC	Secretaria de Despacho	Establece acciones y lineamientos para estar en la capacidad de responder a incidentes.			X				X			X		
6	Datos	Gestión de Infraestructura Tecnológica	POL-GIT-01 Política general SGSI	Secretaría de las TIC	Secretaria de Despacho	Se establece los lineamientos para el control de la información			X				X			X		
7	Datos	Gestión de Infraestructura Tecnológica	POL-GIT-02 Política de Seguridad de la Información.	Secretaría de las TIC	Secretaria de Despacho	Conjunto de reglas alineadas a las actividades de los Sistemas de Información			X				X			X		
8	Datos	Gestión de Infraestructura Tecnológica	PRO-GIT-03 Desarrollo y Mantenimiento de Software .	Secretaría de las TIC	Secretaria de Despacho	Procedimiento para efectuar mantenimiento y soporte - Software			X				X			X		

Ítem	DATOS DEL ACTIVO DE INFORMACIÓN						1. CLASIFICACIÓN DE ACTIVOS DE LA INFORMACIÓN									
							Confidencialidad				Integridad				Disponibilidad			
	Categoría de Activos	Proceso	Nombre del Activo	Propietario del Activo	Responsable	Descripción	Reservada	Clasificada	Pública	No Clasificada	A - Alta	M - Mediano	B - Bajo	No Clasificada	1 - Alta	2 Mediano	3 - Bajo	4 - No Clasificada
9	Datos	Gestión de Infraestructura Tecnológica	PRO-GIT-5 Mantenimiento y Soporte de Hardware .	Secretaría de las TIC	Secretaria de Despacho	Procedimiento para efectuar mantenimiento y soporte - Hardware			X				X			X		
10	Datos	Gestión de Infraestructura Tecnológica	PRO-GIT-01 Creación y Custodia de Copias de Seguridad .	Secretaría de las TIC	Secretaria de Despacho	Procedimiento para la creación custodia y copias de seguridad			X				X			X		
11	Datos	Gestión de Infraestructura Tecnológica	PGR-GIT-01 Programa y Manejo de Residuos Tecnológicos.	Secretaría de las TIC	Secretaria de Despacho	Detalla el proceso para la disposición final de residuos sólidos y tecnológicos			X				X			X		
12	Datos	Gestión de Infraestructura Tecnológica	Datos de Control de Acceso a la Plataforma	Secretaría de las TIC - Grupo Ciencia, Tecnología e Innovación	Profesional Universitario	Relación												

Ítem	DATOS DEL ACTIVO DE INFORMACIÓN						1. CLASIFICACIÓN DE ACTIVOS DE LA INFORMACIÓN									
							Confidencialidad				Integridad				Disponibilidad			
	Categoría de Activos	Proceso	Nombre del Activo	Propietario del Activo	Responsable	Descripción	Reservada	Clasificada	Pública	No Clasificada	A - Alta	M - Mediano	B - Bajo	No Clasificada	1 - Alta	2 Mediano	3 - Bajo	4 - No Clasificada
13	Datos	Gestión de Infraestructura Tecnológica	Copias de Seguridad	Secretaría de las TIC - Grupo Infraestructura Tecnológica	Profesional Universitario	Copias de seguridad de los equipos de cómputo de la Administración Municipal y Servidor	X				X				X			
14	Aplicaciones	Gestión de Infraestructura Tecnológica	PISAMI (Plataforma Integrada de Sistema Alcaldía Municipal Ibagué)	Secretaría de las TIC - Grupo Ciencia, Tecnología e Innovación	Profesional Universitario	Sistema Integrado, Tipo Web, desarrollado lenguaje PHP, SISTEMA OPERATIVO: Windows Server 2016 Motor BD: ORACLE 10G	X				X				X			
15	Aplicaciones	Gestión de Infraestructura Tecnológica	Lenguaje de Programación	Secretaría de las TIC - Grupo Ciencia, Tecnología e Innovación	Profesional Universitario	PHP y Laravel	X				X				X			

Ítem	DATOS DEL ACTIVO DE INFORMACIÓN						1. CLASIFICACIÓN DE ACTIVOS DE LA INFORMACIÓN									
							Confidencialidad				Integridad				Disponibilidad			
	Categoría de Activos	Proceso	Nombre del Activo	Propietario del Activo	Responsable	Descripción	Reservada	Clasificada	Pública	No Clasificada	A - Alta	M - Mediano	B - Bajo	No Clasificada	1 - Alta	2 Mediano	3 - Bajo	4 - No Clasificada
16	Aplicaciones	Gestión de Infraestructura Tecnológica	Sistemas Operativos	Secretaría de las TIC - Grupo Ciencia, Tecnología e Innovación	Profesional Universitario	Windows 10, Windows Server 2016, Win7 Pro, Win Vista, WinXP	X				X				X			
17	Aplicaciones	Gestión de Infraestructura Tecnológica	Motor Base de Datos	Secretaría de las TIC - Grupo Ciencia, Tecnología e Innovación	Profesional Universitario	Oracle 10G	X				X				X			
18	Aplicaciones	Gestión de Infraestructura Tecnológica	Antivirus	Secretaría de las TIC - Grupo Ciencia, Tecnología e Innovación	Profesional Universitario	Avira Antivirus	X				X				X			
19	Hardware	Gestión de Infraestructura Tecnológica	Equipo de Computo	Secretaría de las TIC - Grupo Ciencia, Tecnología e Innovación	Auxiliar Administrativo	HP PRODESK 400, WINPRO		X				X				X		

Ítem	DATOS DEL ACTIVO DE INFORMACIÓN						1. CLASIFICACIÓN DE ACTIVOS DE LA INFORMACIÓN									
							Confidencialidad				Integridad				Disponibilidad			
	Categoría de Activos	Proceso	Nombre del Activo	Propietario del Activo	Responsable	Descripción	Reservada	Clasificada	Pública	No Clasificada	A - Alta	M - Mediano	B - Bajo	No Clasificada	1 - Alta	2 Mediano	3 - Bajo	4 - No Clasificada
20	Hardware	Gestión de Infraestructura Tecnológica	Equipo de Computo	Secretaría de las TIC - Grupo Ciencia, Tecnología e Innovación	Auxiliar Administrativo	HP PRODESK, , WINPRO		X				X				X		
21	Hardware	Gestión de Infraestructura Tecnológica	Equipo de Computo	Secretaría de las TIC - Grupo Ciencia, Tecnología e Innovación	Profesional Especializado	HP COMPAQ PRO 6300, WINPRO		X				X				X		
22	Hardware	Gestión de Infraestructura Tecnológica	Equipo de Computo	Secretaría de las TIC - Grupo Ciencia, Tecnología e Innovación	Profesional Universitario	HP PRODESK, , WINPRO		X				X				X		
23	Hardware	Gestión de Infraestructura Tecnológica	Equipo de Cómputo - Portátil	Secretaría de las TIC - Grupo Ciencia, Tecnología e Innovación	Secretaria de Despacho	HP PROBOOK 250 G6, , WINPRO		X				X				X		

Ítem	DATOS DEL ACTIVO DE INFORMACIÓN						1. CLASIFICACIÓN DE ACTIVOS DE LA INFORMACIÓN									
							Confidencialidad				Integridad				Disponibilidad			
	Categoría de Activos	Proceso	Nombre del Activo	Propietario del Activo	Responsable	Descripción	Reservada	Clasificada	Pública	No Clasificada	A - Alta	M - Mediano	B - Bajo	No Clasificada	1 - Alta	2 Mediano	3 - Bajo	4 - No Clasificada
24	Hardware	Gestión de Infraestructura Tecnológica	Equipo de Computo	Secretaría de las TIC - Grupo Ciencia, Tecnología e Innovación	Técnico Operativo	HP PRODESK, , WINPRO		X				X				X		
25	Hardware	Gestión de Infraestructura Tecnológica	Equipo de Cómputo - Portátil	Secretaría de las TIC - Grupo Infraestructura Tecnológica	Técnico Operativo	HP PROBOOK 250 G6, , WINPRO		X				X				X		
26	Hardware	Gestión de Infraestructura Tecnológica	Equipo de Cómputo - Portátil	Secretaría de las TIC - Grupo Infraestructura Tecnológica	Técnico Operativo	HP PROBOOK 4540s, WINPRO		X				X				X		
27	Hardware	Gestión Humana	Equipo de Computo	Secretaría Administrativa - Despacho	Auxiliar Administrativo	HP PRODESK, WIN 10 PRO		X				X				X		
28	Hardware	Gestión Humana	Equipo de Computo	Secretaría Administrativa - Despacho - Dirección de Recursos Físicos	Auxiliar Administrativo	HP COMPAQ 6000 PRO, WIN 7 PRO		X				X				X		

Ítem	DATOS DEL ACTIVO DE INFORMACIÓN						1. CLASIFICACIÓN DE ACTIVOS DE LA INFORMACIÓN									
							Confidencialidad				Integridad				Disponibilidad			
	Categoría de Activos	Proceso	Nombre del Activo	Propietario del Activo	Responsable	Descripción	Reservada	Clasificada	Pública	No Clasificada	A - Alta	M - Mediano	B - Bajo	No Clasificada	1 - Alta	2 Mediano	3 - Bajo	4 - No Clasificada
29	Hardware	Gestión Humana	Equipo de Computo	Secretaría Administrativa - Despacho - Dirección de Recursos Físicos	Director	HP PRODESK 400, WIN 10 PRO		X				X				X		
30	Hardware	Gestión Humana	Equipo de Computo	Secretaría Administrativa - Despacho - Dirección de Recursos Físicos	Profesional Especializado	HP PRODESK400, WIN 10 PRO		X				X				X		
31	Hardware	Gestión Humana	Equipo de Computo	Secretaría Administrativa - Despacho - Dirección de Recursos Físicos	Profesional Universitario	DELL VOSTRO 220S, WIN VISTA BUSINESS		X				X				X		
32	Hardware	Gestión Humana	Equipo de Computo	Secretaría Administrativa - Despacho - Dirección de Recursos Físicos	Técnico Operativo	COMPAQ PAVILION 100, WIN 7 PRO		X				X				X		

Ítem	DATOS DEL ACTIVO DE INFORMACIÓN						1. CLASIFICACIÓN DE ACTIVOS DE LA INFORMACIÓN									
							Confidencialidad				Integridad				Disponibilidad			
	Categoría de Activos	Proceso	Nombre del Activo	Propietario del Activo	Responsable	Descripción	Reservada	Clasificada	Pública	No Clasificada	A - Alta	M - Mediano	B - Bajo	No Clasificada	1 - Alta	2 Mediano	3 - Bajo	4 - No Clasificada
33	Hardware	Gestión Humana	Equipo de Cómputo - Portátil	Secretaría Administrativa - Despacho - Dirección de Recursos Físicos	Técnico Operativo	HP 250 G6, WIN 10 PRO		X				X				X		
34	Hardware	Gestión Humana	Equipo de Computo	Secretaría Administrativa - Despacho - Dirección de Recursos Físicos	Técnico Operativo	DELL OPTIPLEX 745, WIN PRO		X				X				X		
35	Hardware	Gestión Humana	Equipo de Computo	Secretaría Administrativa - Despacho - Dirección de Recursos Físicos	Técnico Operativo	DELL VOSTRO 220S, WIN VISTA		X				X				X		
36	Hardware	Gestión Humana	Equipo de Computo	Secretaría Administrativa - Dirección de Talento Humano	Auxiliar Administrativo	HP PRODESK 400, WIN 7 PRO		X				X				X		

Ítem	DATOS DEL ACTIVO DE INFORMACIÓN						1. CLASIFICACIÓN DE ACTIVOS DE LA INFORMACIÓN									
							Confidencialidad				Integridad				Disponibilidad			
	Categoría de Activos	Proceso	Nombre del Activo	Propietario del Activo	Responsable	Descripción	Reservada	Clasificada	Pública	No Clasificada	A - Alta	M - Mediano	B - Bajo	No Clasificada	1 - Alta	2 Mediano	3 - Bajo	4 - No Clasificada
37	Hardware	Gestión Humana	Equipo de Computo	Secretaría Administrativa - Dirección de Talento Humano	Director	HP COMPAQ 6000 PRO, WIN10 PRO		X				X				X		
38	Hardware	Gestión Humana	Equipo de Computo	Secretaría Administrativa - Dirección de Talento Humano	Profesional Universitario	DELL OPTIPLEX 3020, WIND7 PRO		X				X				X		
39	Hardware	Gestión Humana	Equipo de Computo	Secretaría Administrativa - Dirección de Talento Humano	Asesor	DELL VOSTRO 220S, WIN7 VISTA		X				X				X		
40	Hardware	Gestión Humana	Equipo de Computo	Secretaría Administrativa - Dirección de Talento Humano	Técnico Operativo	HP COMPAQ ELITE 8300, WIN 7 PRO		X				X				X		
41	Hardware	Gestión Humana	Equipo de Computo	Secretaría Administrativa - Dirección de Talento Humano	Técnico Operativo	DELL OPTIPLEX 3020, WIND7 PRO		X				X				X		

Ítem	DATOS DEL ACTIVO DE INFORMACIÓN						1. CLASIFICACIÓN DE ACTIVOS DE LA INFORMACIÓN									
							Confidencialidad				Integridad				Disponibilidad			
	Categoría de Activos	Proceso	Nombre del Activo	Propietario del Activo	Responsable	Descripción	Reservada	Clasificada	Pública	No Clasificada	A - Alta	M - Mediano	B - Bajo	No Clasificada	1 - Alta	2 Mediano	3 - Bajo	4 - No Clasificada
42	Hardware	Gestión Humana	Equipo de Computo	Secretaría Administrativa - Dirección de Talento Humano	Técnico Operativo	HP COMPAQ PRO 6300, WIN 10 PRO		X				X				X		
43	Hardware	Gestión de Infraestructura Tecnológica	Servidor - Plataforma PISAMI	Secretaría de las TIC - Grupo Infraestructura Tecnológica	Profesional Universitario	DELL PowerEdge R510, Linux CentOS 7	X				X				X			
44	Hardware	Gestión de Infraestructura Tecnológica	Servidor - Plataforma PISAMIV2 (Soporte	Secretaría de las TIC - Grupo Infraestructura Tecnológica	Profesional Universitario	HP Proliant DL180 GEN9, Windows 2016 Server	X				X				X			
45	Hardware	Gestión de Infraestructura Tecnológica	Router	Secretaría de las TIC - Grupo Infraestructura Tecnológica	Técnico Operativo		X				X				X			
46	Hardware	Gestión de Infraestructura Tecnológica	Switches - Clientes	Secretaría de las TIC - Grupo Infraestructura Tecnológica	Técnico Operativo	ArubaOS-Switch, ARUBA 2530 24G	X				X				X			

Ítem	DATOS DEL ACTIVO DE INFORMACIÓN						1. CLASIFICACIÓN DE ACTIVOS DE LA INFORMACIÓN									
							Confidencialidad				Integridad				Disponibilidad			
	Categoría de Activos	Proceso	Nombre del Activo	Propietario del Activo	Responsable	Descripción	Reservada	Clasificada	Pública	No Clasificada	A - Alta	M - Mediano	B - Bajo	No Clasificada	1 - Alta	2 Mediano	3 - Bajo	4 - No Clasificada
47	Hardware	Gestión de Infraestructura Tecnológica	Switches - Enlaces Trunk entre SW.	Secretaría de las TIC - Grupo Infraestructura Tecnológica	Técnico Operativo	ArubaOS-Switch, ARUBA 2530 24G	X				X				X			
48	Hardware	Gestión de Infraestructura Tecnológica	Switches - CORE	Secretaría de las TIC - Grupo Infraestructura Tecnológica	Técnico Operativo	HUAWEI S5720, v200r010c00spc600b221	X				X				X			
49	Hardware	Gestión de Infraestructura Tecnológica	Impresora	Secretaría de las TIC - Grupo Ciencia, Tecnología e Innovación	Profesional Universitario	HP LASERJET M1212NF		X				X				X		
50	Hardware	Gestión de Infraestructura Tecnológica	Impresora	Secretaría de las TIC - Grupo Infraestructura Tecnológica	Profesional Universitario	HP LASERJET ENTERPRISE M608		X				X				X		
51	Hardware	Gestión Humana	Impresora	Secretaría Administrativa - Despacho	Secretaria de Despacho	HP LASERJET PRO MFP M426FDW		X				X				X		

Ítem	DATOS DEL ACTIVO DE INFORMACIÓN						1. CLASIFICACIÓN DE ACTIVOS DE LA INFORMACIÓN									
							Confidencialidad				Integridad				Disponibilidad			
	Categoría de Activos	Proceso	Nombre del Activo	Propietario del Activo	Responsable	Descripción	Reservada	Clasificada	Pública	No Clasificada	A - Alta	M - Mediano	B - Bajo	No Clasificada	1 - Alta	2 Mediano	3 - Bajo	4 - No Clasificada
52	Hardware	Gestión de Infraestructura Tecnológica	Impresora	Secretaría de las TIC	Secretaria de Despacho	HP LASERJET P4515x		X				X				X		
53	Hardware	Gestión Documental	Impresora	Secretaría Administrativa - Despacho - Dirección de Recursos Físicos	Director	LASERJET 600 M603		X				X				X		
54	Hardware	Gestión Documental	Impresora	Secretaría Administrativa - Despacho - Dirección de Recursos Físicos	Técnico Operativo	HP OFFICEJET PRO 8600		X				X				X		
55	Hardware	Gestión Humana	Impresora	Secretaría Administrativa - Dirección de Talento Humano	Director	HP LASERJET M1522N		X				X				X		
56	Hardware	Gestión Humana	Impresora	Secretaría Administrativa - Dirección de	Técnico Operativo	KYOCERA FS-1035MFP		X				X				X		

Ítem	DATOS DEL ACTIVO DE INFORMACIÓN						1. CLASIFICACIÓN DE ACTIVOS DE LA INFORMACIÓN									
							Confidencialidad				Integridad				Disponibilidad			
	Categoría de Activos	Proceso	Nombre del Activo	Propietario del Activo	Responsable	Descripción	Reservada	Clasificada	Pública	No Clasificada	A - Alta	M - Mediano	B - Bajo	No Clasificada	1 - Alta	2 Mediano	3 - Bajo	4 - No Clasificada
				Talento Humano														
57	Red	Gestión de Infraestructura Tecnológica	Red Local	Secretaría de las TIC - Grupo Infraestructura Tecnológica	Técnico Operativo	Topología de Red Estrella	X				X				X			
58	Red	Gestión de Infraestructura Tecnológica	Firewalls	Secretaría de las TIC - Grupo Infraestructura Tecnológica	Técnico Operativo	Rendimiento superior de firewall para IPv4 / IPv6, SCTP y multidifusión	X				X				X			
59	Red	Gestión de Infraestructura Tecnológica	Wi-fi	Secretaría de las TIC - Grupo Infraestructura Tecnológica	Técnico Operativo	Aruba AP-303	X				X				X			
60	Red	Gestión de Infraestructura Tecnológica	Wi-fi	Secretaría de las TIC - Grupo Infraestructura Tecnológica	Técnico Operativo	Aruba AP-303	X				X				X			

Ítem	DATOS DEL ACTIVO DE INFORMACIÓN						1. CLASIFICACIÓN DE ACTIVOS DE LA INFORMACIÓN									
							Confidencialidad				Integridad			Disponibilidad		
	Categoría de Activos	Proceso	Nombre del Activo	Propietario del Activo	Responsable	Descripción	Reservada	Clasificada	Pública	No Clasificada	A - Alta	M - Mediano	B - Bajo	No Clasificada	1 - Alta	2 Mediano	3 - Bajo	4 - No Clasificada
61	Red	Gestión de Infraestructura Tecnológica	Telefonía IP	Secretaría de las TIC - Grupo Infraestructura Tecnológica	Técnico Operativo	Unify OpenScape Business X8		X	X			X				X		
62	Personal	Alcaldía de Ibagué	Funcionarios de Planta	Secretarios, Directores, Profesionales Universitarios, Técnicos Operativos, Asesores, Auxiliares.	NA	(Provisionalidad, Carrera Administrativa, Libre nombramiento y Remisión			X				X				X	
63	Personal	Alcaldía de Ibagué	Clientes Externo	NA	NA	Comunidad que efectúa radicación de P.Q.R			X				X				X	
64	Personal	Alcaldía de Ibagué	Contratistas	NA	NA	Contrato OPS diferentes dependencias de la Administración Municipal			X				X				X	

Ítem	DATOS DEL ACTIVO DE INFORMACIÓN						1. CLASIFICACIÓN DE ACTIVOS DE LA INFORMACIÓN									
							Confidencialidad				Integridad				Disponibilidad			
	Categoría de Activos	Proceso	Nombre del Activo	Propietario del Activo	Responsable	Descripción	Reservada	Clasificada	Pública	No Clasificada	A - Alta	M - Mediano	B - Bajo	No Clasificada	1 - Alta	2 Mediano	3 - Bajo	4 - No Clasificada
65	Personal	Alcaldía de Ibagué	Proveedores	NA	NA	Prestación de Servicio de Aseo, Vigilancia, Correo Certificado, Contratos Suministros			X				X				X	
66	Instalaciones	Alcaldía de Ibagué	Palacio Municipal	Secretaría de las TIC		Oficinas de Mantenimiento, Desarrollo, Innovación y Despacho			X				X				X	
67	Instalaciones	Alcaldía de Ibagué	Palacio Municipal	Secretaría Administrativa		Oficinas Dirección de Recursos Físicos, Dirección de Talento Humano, Despacho.			X				X				X	
68	Instalaciones	Alcaldía de Ibagué	Palacio Municipal	Secretaría de las TIC		Ubicación Datacenter y UPS			X				X				X	

Ítem	DATOS DEL ACTIVO DE INFORMACIÓN						1. CLASIFICACIÓN DE ACTIVOS DE LA INFORMACIÓN									
							Confidencialidad				Integridad				Disponibilidad			
	Categoría de Activos	Proceso	Nombre del Activo	Propietario del Activo	Responsable	Descripción	Reservada	Clasificada	Pública	No Clasificada	A - Alta	M - Mediano	B - Bajo	No Clasificada	1 - Alta	2 Mediano	3 - Bajo	4 - No Clasificada
69	Equipamiento Auxiliar	Gestión de Infraestructura Tecnológica	UPS	Secretaría de las TIC		Marca PEI, 15KVA		X				X				X		

Fuente. El Autor

6.2.3 Criticidad de los activos

Continuando con la aplicación de la metodología MARGERIT se procedió a identificar la criticidad de los activos corresponde al valor que se asigna al activo conforme su clasificación[52], ejemplo de ello se evidencia en el la tabla 4

Tabla 13 Criterios de Clasificación

Confidencialidad	Integridad	Disponibilidad
Información pública Reservada	**Alta (A)**	**ALTA (1)**
Información pública Clasificada	**Media (M)**	**Media (2)**
Información pública	**Baja (B)**	**Baja (3)**
No Clasificada	**No Clasificada**	**No Clasificada**

Fuente. MINTIC. Guía para la Gestión y Clasificación de Activos de Información. [Sitio Web]. Bogotá. MINTIC. [Consulta: 17 de mayo 2021]. Disponible en: https://www.mintic.gov.co/gestionti/615/articles-5482_G5_Gestion_Clasificacion.pdf.

Teniendo en cuenta lo relacionado en la tabla 4 a continuación, se conceptualiza cada uno de los niveles de criticidad.

Tabla 14. Criticidad

Nivel	Criterio
Alta	La clasificación de la información es **alta** en dos o todas las propiedades.
Media	La clasificación de la información es **alta** en una de las propiedades o por lo menos en una se considera **media**
Baja	La clasificación de la información es **baja** en todos los niveles.

Fuente. MINTIC. Guía para la Gestión y Clasificación de Activos de Información.

[52] MINTIC. Guía para la Gestión y Clasificación de Activos de Información. [en línea]. Bogotá: MINTIC. [Consultado 17 de mayo 2021]. Disponible en https://www.mintic.gov.co/gestionti/615/articles-5482_G5_Gestion_Clasificacion.pdf#page=16&zoom=100,148,133.

Tabla 15. Criticidad de Activos

Ítem	DATOS DEL ACTIVO DE INFORMACIÓN						3. CRITICIDAD			
	Categoría de Activos	Proceso	Nombre del Activo	Propietario del Activo	Responsable	Descripción	Reservada	Clasificada	Pública	No Clasificada
1	Datos	Gestión Documental	CAR-GD-01 Gestión Documental.	Dirección de Recursos Físicos - Grupo Gestión Documental	Profesional Universitario	Caracterización del proceso en el cual se especifica las entradas salidas y beneficiarios,			X	
2	Datos	Gestión Documental	PGR-GD-01 Programa de Gestión Documental.	Dirección de Recursos Físicos - Grupo Gestión Documental	Profesional Universitario	Detalle de las funciones, procesos y procedimientos de programa			X	
3	Datos	Gestión Documental	PRO-PGD-10 Planeación de la Gestión Documental.	Dirección de Recursos Físicos - Grupo Gestión Documental	Profesional Universitario	Planeación de cada uno de los procesos ejecutados por el programa			X	
4	Datos	Gestión Documental	PLA-GD-02 Plan de Conservación Documental.	Dirección de Recursos Físicos - Grupo Gestión Documental	Profesional Universitario	Se detalla los pasos y procedimientos para la conservación del acervo documental			X	
5	Datos	Gestión de Infraestructura Tecnológica	PLA-GIT-02 Plan de incidentes .	Secretaría de las TIC	Secretaria de Despacho	Establece acciones y lineamientos para estar en la capacidad de responder a incidentes.			X	

	DATOS DEL ACTIVO DE INFORMACIÓN						3. CRITICIDAD			
Ítem	**Categoría de Activos**	**Proceso**	**Nombre del Activo**	**Propietario del Activo**	**Responsable**	**Descripción**	**Reservada**	**Clasificada**	**Pública**	**No Clasificada**
6	Datos	Gestión de Infraestructura Tecnológica	POL-GIT-01 Política general SGSI	Secretaría de las TIC	Secretaria de Despacho	Se establece los lineamientos para el control de la información			X	
7	Datos	Gestión de Infraestructura Tecnológica	POL-GIT-02 Política de Seguridad de la Información.	Secretaría de las TIC	Secretaria de Despacho	Conjunto de reglas alineadas a las actividades de los Sistemas de Información			X	
8	Datos	Gestión de Infraestructura Tecnológica	PRO-GIT-03 Desarrollo y Mantenimiento de Software .	Secretaría de las TIC	Secretaria de Despacho	Procedimiento para efectuar mantenimiento y soporte - Software			X	
9	Datos	Gestión de Infraestructura Tecnológica	PRO-GIT-5 Mantenimiento y Soporte de Hardware .	Secretaría de las TIC	Secretaria de Despacho	Procedimiento para efectuar mantenimiento y soporte - Hardware			X	
10	Datos	Gestión de Infraestructura Tecnológica	PRO-GIT-01 Creación y Custodia de Copias de Seguridad .	Secretaría de las TIC	Secretaria de Despacho	Procedimiento para la creación custodia y copias de seguridad			X	
11	Datos	Gestión de Infraestructura Tecnológica	PGR-GIT-01 Programa y Manejo de Residuos Tecnológicos.	Secretaría de las TIC	Secretaria de Despacho	Detalla el proceso para la disposición final de residuos solidos y tecnológicos			X	
12	Datos	Gestión de Infraestructura Tecnológica	Datos de Control de	Secretaría de las TIC - Grupo	Profesional Universitario	Relación				

Ítem	DATOS DEL ACTIVO DE INFORMACIÓN						3. CRITICIDAD			
	Categoría de Activos	Proceso	Nombre del Activo	Propietario del Activo	Responsable	Descripción	Reservada	Clasificada	Pública	No Clasificada
			Acceso a la Plataforma	Ciencia, Tecnología e Innovación						
13	Datos	Gestión de Infraestructura Tecnológica	Copias de Seguridad	Secretaría de las TIC - Grupo Infraestructura Tecnológica	Profesional Universitario	Copias de seguridad de los equipos de cómputo de la Administración Municipal y Servidor	X			
14	Aplicaciones	Gestión de Infraestructura Tecnológica	PISAMI (Plataforma Integrada de Sistema Alcaldía Municipal Ibagué)	Secretaría de las TIC - Grupo Ciencia, Tecnología e Innovación	Profesional Universitario	Sistema Integrado, Tipo Web, desarrollado lenguaje PHP, SISTEMA OPERATIVO: Windows Server 2016 Motor BD: ORACLE 10G	X			
15	Aplicaciones	Gestión de Infraestructura Tecnológica	Lenguaje de Programación	Secretaría de las TIC - Grupo Ciencia, Tecnología e Innovación	Profesional Universitario	PHP y Laravel	X			
16	Aplicaciones	Gestión de Infraestructura Tecnológica	Sistemas Operativos	Secretaría de las TIC - Grupo Ciencia, Tecnología e Innovación	Profesional Universitario	Windows 10, Windows Server 2016, Win7 Pro, Win Vista, WinXP	X			

Ítem	DATOS DEL ACTIVO DE INFORMACIÓN						3. CRITICIDAD			
	Categoría de Activos	Proceso	Nombre del Activo	Propietario del Activo	Responsable	Descripción	Reservada	Clasificada	Pública	No Clasificada
17	Aplicaciones	Gestión de Infraestructura Tecnológica	Motor Base de Datos	Secretaría de las TIC - Grupo Ciencia, Tecnología e Innovación	Profesional Universitario	Oracle 10G	X			
18	Aplicaciones	Gestión de Infraestructura Tecnológica	Antivirus	Secretaría de las TIC - Grupo Ciencia, Tecnología e Innovación	Profesional Universitario	Avira Antivirus	X			
19	Hardware	Gestión de Infraestructura Tecnológica	Equipo de Computo	Secretaría de las TIC - Grupo Ciencia, Tecnología e Innovación	Auxiliar Administrativo	HP PRODESK 400, WINPRO		X		
20	Hardware	Gestión de Infraestructura Tecnológica	Equipo de Computo	Secretaría de las TIC - Grupo Ciencia, Tecnología e Innovación	Auxiliar Administrativo	HP PRODESK, , WINPRO		X		
21	Hardware	Gestión de Infraestructura Tecnológica	Equipo de Computo	Secretaría de las TIC - Grupo Ciencia,	Profesional Especializado	HP COMPAQ PRO 6300, WINPRO		X		

Ítem	DATOS DEL ACTIVO DE INFORMACIÓN						3. CRITICIDAD			
	Categoría de Activos	Proceso	Nombre del Activo	Propietario del Activo	Responsable	Descripción	Reservada	Clasificada	Pública	No Clasificada
				Tecnología e Innovación						
22	Hardware	Gestión de Infraestructura Tecnológica	Equipo de Computo	Secretaría de las TIC - Grupo Ciencia, Tecnología e Innovación	Profesional Universitario	HP PRODESK, , WINPRO		X		
23	Hardware	Gestión de Infraestructura Tecnológica	Equipo de Cómputo - Portátil	Secretaría de las TIC - Grupo Ciencia, Tecnología e Innovación	Secretaria de Despacho	HP PROBOOK 250 G6, , WINPRO		X		
24	Hardware	Gestión de Infraestructura Tecnológica	Equipo de Computo	Secretaría de las TIC - Grupo Ciencia, Tecnología e Innovación	Técnico Operativo	HP PRODESK, , WINPRO		X		
25	Hardware	Gestión de Infraestructura Tecnológica	Equipo de Cómputo - Portátil	Secretaría de las TIC - Grupo Infraestructura Tecnológica	Técnico Operativo	HP PROBOOK 250 G6, , WINPRO		X		

Ítem	DATOS DEL ACTIVO DE INFORMACIÓN						3. CRITICIDAD			
	Categoría de Activos	Proceso	Nombre del Activo	Propietario del Activo	Responsable	Descripción	Reservada	Clasificada	Pública	No Clasificada
26	Hardware	Gestión de Infraestructura Tecnológica	Equipo de Cómputo - Portátil	Secretaría de las TIC - Grupo Infraestructura Tecnológica	Técnico Operativo	HP PROBOOK 4540s, WINPRO		X		
27	Hardware	Gestión Humana	Equipo de Computo	Secretaría Administrativa - Despacho	Auxiliar Administrativo	HP PRODESK, WIN 10 PRO		X		
28	Hardware	Gestión Humana	Equipo de Computo	Secretaría Administrativa - Despacho - Dirección de Recursos Físicos	Auxiliar Administrativo	HP COMPAQ 6000 PRO, WIN 7 PRO		X		
29	Hardware	Gestión Humana	Equipo de Computo	Secretaría Administrativa - Despacho - Dirección de Recursos Físicos	Director	HP PRODESK 400, WIN 10 PRO		X		
30	Hardware	Gestión Humana	Equipo de Computo	Secretaría Administrativa - Despacho - Dirección de Recursos Físicos	Profesional Especializado	HP PRODESK400, WIN 10 PRO		X		
31	Hardware	Gestión Humana	Equipo de Computo	Secretaría Administrativa	Profesional Universitario	DELL VOSTRO 220S, WIN VISTA BUSINESS		X		

Ítem	DATOS DEL ACTIVO DE INFORMACIÓN						3. CRITICIDAD			
	Categoría de Activos	Proceso	Nombre del Activo	Propietario del Activo	Responsable	Descripción	Reservada	Clasificada	Pública	No Clasificada
				- Despacho - Dirección de Recursos Físicos						
32	Hardware	Gestión Humana	Equipo de Computo	Secretaría Administrativa - Despacho - Dirección de Recursos Físicos	Técnico Operativo	COMPAQ PAVILION 100, WIN 7 PRO		X		
33	Hardware	Gestión Humana	Equipo de Cómputo - Portátil	Secretaría Administrativa - Despacho - Dirección de Recursos Físicos	Técnico Operativo	HP 250 G6, WIN 10 PRO		X		
34	Hardware	Gestión Humana	Equipo de Computo	Secretaría Administrativa - Despacho - Dirección de Recursos Físicos	Técnico Operativo	DELL OPTIPLEX 745, WIN PRO		X		
35	Hardware	Gestión Humana	Equipo de Computo	Secretaría Administrativa - Despacho - Dirección de Recursos Físicos	Técnico Operativo	DELL VOSTRO 220S, WIN VISTA		X		

Ítem	DATOS DEL ACTIVO DE INFORMACIÓN						3. CRITICIDAD			
	Categoría de Activos	Proceso	Nombre del Activo	Propietario del Activo	Responsable	Descripción	Reservada	Clasificada	Pública	No Clasificada
36	Hardware	Gestión Humana	Equipo de Computo	Secretaría Administrativa - Dirección de Talento Humano	Auxiliar Administrativo	HP PRODESK 400, WIN 7 PRO		X		
37	Hardware	Gestión Humana	Equipo de Computo	Secretaría Administrativa - Dirección de Talento Humano	Director	HP COMPAQ 6000 PRO, WIN10 PRO		X		
38	Hardware	Gestión Humana	Equipo de Computo	Secretaría Administrativa - Dirección de Talento Humano	Profesional Universitario	DELL OPTIPLEX 3020, WIND7 PRO		X		
39	Hardware	Gestión Humana	Equipo de Computo	Secretaría Administrativa - Dirección de Talento Humano	Asesor	DELL VOSTRO 220S, WIN7 VISTA		X		
40	Hardware	Gestión Humana	Equipo de Computo	Secretaría Administrativa - Dirección de Talento Humano	Técnico Operativo	HP COMPAQ ELITE 8300, WIN 7 PRO		X		
41	Hardware	Gestión Humana	Equipo de Computo	Secretaría Administrativa - Dirección de	Técnico Operativo	DELL OPTIPLEX 3020, WIND7 PRO		X		

Ítem	DATOS DEL ACTIVO DE INFORMACIÓN						3. CRITICIDAD			
	Categoría de Activos	Proceso	Nombre del Activo	Propietario del Activo	Responsable	Descripción	Reservada	Clasificada	Pública	No Clasificada
				Talento Humano						
42	Hardware	Gestión Humana	Equipo de Computo	Secretaría Administrativa - Dirección de Talento Humano	Técnico Operativo	HP COMPAQ PRO 6300, WIN 10 PRO		X		
43	Hardware	Gestión de Infraestructura Tecnológica	Servidor - Plataforma PISAMI	Secretaría de las TIC - Grupo Infraestructura Tecnológica	Profesional Universitario	DELL PowerEdge R510, Linux CentOS 7	X			
44	Hardware	Gestión de Infraestructura Tecnológica	Servidor - Plataforma PISAMIV2 (Soporte	Secretaría de las TIC - Grupo Infraestructura Tecnológica	Profesional Universitario	HP Proliant DL180 GEN9, Windows 2016 Server	X			
45	Hardware	Gestión de Infraestructura Tecnológica	Router	Secretaría de las TIC - Grupo Infraestructura Tecnológica	Técnico Operativo		X			
46	Hardware	Gestión de Infraestructura Tecnológica	Switches - Clientes	Secretaría de las TIC - Grupo Infraestructura Tecnológica	Técnico Operativo	ArubaOS-Switch, ARUBA 2530 24G	X			

Ítem	DATOS DEL ACTIVO DE INFORMACIÓN						3. CRITICIDAD			
	Categoría de Activos	Proceso	Nombre del Activo	Propietario del Activo	Responsable	Descripción	Reservada	Clasificada	Pública	No Clasificada
47	Hardware	Gestión de Infraestructura Tecnológica	Switches - Enlaces Trunk entre SW.	Secretaría de las TIC - Grupo Infraestructura Tecnológica	Técnico Operativo	ArubaOS-Switch, ARUBA 2530 24G	X			
48	Hardware	Gestión de Infraestructura Tecnológica	Switches - CORE	Secretaría de las TIC - Grupo Infraestructura Tecnológica	Técnico Operativo	HUAWEI S5720, v200r010c00spc600b221	X			
49	Hardware	Gestión de Infraestructura Tecnológica	Impresora	Secretaría de las TIC - Grupo Ciencia, Tecnología e Innovación	Profesional Universitario	HP LASERJET M1212NF		X		
50	Hardware	Gestión de Infraestructura Tecnológica	Impresora	Secretaría de las TIC - Grupo Infraestructura Tecnológica	Profesional Universitario	HP LASERJET ENTERPRISE M608		X		
51	Hardware	Gestión Humana	Impresora	Secretaría Administrativa - Despacho	Secretaria de Despacho	HP LASERJET PRO MFP M426FDW		X		
52	Hardware	Gestión de Infraestructura Tecnológica	Impresora	Secretaría de las TIC	Secretaria de Despacho	HP LASERJET P4515x		X		

Ítem	DATOS DEL ACTIVO DE INFORMACIÓN						3. CRITICIDAD			
	Categoría de Activos	Proceso	Nombre del Activo	Propietario del Activo	Responsable	Descripción	Reservada	Clasificada	Pública	No Clasificada
53	Hardware	Gestión Documental	Impresora	Secretaría Administrativa - Despacho - Dirección de Recursos Físicos	Director	LASERJET 600 M603		X		
54	Hardware	Gestión Documental	Impresora	Secretaría Administrativa - Despacho - Dirección de Recursos Físicos	Técnico Operativo	HP OFFICEJET PRO 8600		X		
55	Hardware	Gestión Humana	Impresora	Secretaría Administrativa - Dirección de Talento Humano	Director	HP LASERJET M1522N		X		
56	Hardware	Gestión Humana	Impresora	Secretaría Administrativa - Dirección de Talento Humano	Técnico Operativo	KYOCERA FS-1035MFP		X		
57	Red	Gestión de Infraestructura Tecnológica	Red Local	Secretaría de las TIC - Grupo Infraestructura Tecnológica	Técnico Operativo	Topología de Red Estrella	X			

Ítem	DATOS DEL ACTIVO DE INFORMACIÓN						3. CRITICIDAD			
	Categoría de Activos	Proceso	Nombre del Activo	Propietario del Activo	Responsable	Descripción	Reservada	Clasificada	Pública	No Clasificada
58	Red	Gestión de Infraestructura Tecnológica	Firewalls	Secretaría de las TIC - Grupo Infraestructura Tecnológica	Técnico Operativo	Rendimiento superior de firewall para IPv4 / IPv6, SCTP y multidifusión	X			
59	Red	Gestión de Infraestructura Tecnológica	Wi-fi	Secretaría de las TIC - Grupo Infraestructura Tecnológica	Técnico Operativo	Aruba AP-303	X			
60	Red	Gestión de Infraestructura Tecnológica	Wi-fi	Secretaría de las TIC - Grupo Infraestructura Tecnológica	Técnico Operativo	Aruba AP-303	X			
61	Red	Gestión de Infraestructura Tecnológica	Telefonía IP	Secretaría de las TIC - Grupo Infraestructura Tecnológica	Técnico Operativo	Unify OpenScape Business X8		X		
62	Personal	Alcaldía de Ibagué	Funcionarios de Planta	Secretarios, Directores, Profesionales Universitarios, Técnicos Operativos, Asesores, Auxiliares.	NA	(Provisionalidad, Carrera Administrativa, Libre nombramiento y Remisión			X	

Ítem	DATOS DEL ACTIVO DE INFORMACIÓN						3. CRITICIDAD			
	Categoría de Activos	Proceso	Nombre del Activo	Propietario del Activo	Responsable	Descripción	Reservada	Clasificada	Pública	No Clasificada
63	Personal	Alcaldía de Ibagué	Clientes Externo	NA	NA	Comunidad que efectúa radicación de P.Q.R			X	
64	Personal	Alcaldía de Ibagué	Contratistas	NA	NA	Contrato OPS diferentes dependencias de la Administración Municipal			X	
65	Personal	Alcaldía de Ibagué	Proveedores	NA	NA	Prestación de Servicio de Aseo, Vigilancia, Correo Certificado, Contratos Suministros			X	
66	Instalaciones	Alcaldía de Ibagué	Palacio Municipal	Secretaría de las TIC		Oficinas de Mantenimiento, Desarrollo, Innovación y Despacho			X	
67	Instalaciones	Alcaldía de Ibagué	Palacio Municipal	Secretaría Administrativa		Oficinas Dirección de Recursos Físicos, Dirección de Talento Humano, Despacho.			X	
68	Instalaciones	Alcaldía de Ibagué	Palacio Municipal	Secretaría de las TIC		Ubicación Datacenter y UPS			X	
69	Equipamiento Auxiliar	Gestión de Infraestructura Tecnológica	UPS	Secretaría de las TIC		Marca PEI, 15KVA		X		

Fuente. El Autor

6.2.4 IDENTIFICACIÓN DE AMENAZAS, VULNERABILIDADES Y DIMENSIONES DE SEGURIDAD AFECTADAS:

Una vez identificados los activos, clasificados según su pilar de Seguridad y Criticidad, se procedió a identificar las amenazas existentes en el Sistema de Gestión Documental de la Administración Municipal, vulnerabilidades y sus dimensiones afectadas, para ello es importante conceptualizar las dimensiones de valoración acentuadas en el libro II[53] de la metodología MARGERIT, las cuales nos permites valorar los resultados de la materialización de una amenaza,

Tabla 16 Dimensiones

[D]	Disponibilidad	Propiedad de los activos a los cuales la entidad puede acceder cuando se requiere
[I]	Integridad	Propiedad de los activos en el cual se determina que no ha sido alterado de manera no autorizada.
[C]	Confidencialidad	Propiedad del activo en el cual se establece que la información no se deja a disposición y no se revela a entidades o usuarios no autorizados.
[A]	Autenticidad	Propiedad del activo en la que se establece que el activo es de quien dice ser y su procedencia es garantizada.
[T]	Trazabilidad	Propiedad del activo en la cual se establece que las actuaciones puedes ser efectuadas únicamente por la entidad

Fuente ADMINISTRACIÓN ELECTRÓNICA [Sitio Web] MARGERIT v.3 Metodología de Análisis y Gestión de los Riesgos de los Sistemas de Información. [Consultado: 01 de mayo de 2021]. Disponible en:https://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_Magerit.html

[53] ADMINISTRACIÓN ELECTRÓNICA [Sitio Web] MARGERIT v.3 Metodología de Análisis y Gestión de los Riesgos de los Sistemas de Información. [Consulta: 01 de mayo de 2021]. Disponible en:https://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_Magerit.html

Tabla 17. Amenazas y Dimensiones de los Activos de Información

ACTIVO	VULNERABILIDAD	AMENAZAS			
		[N] Desastres Naturales	**[I] De Origen Industrial**	**[E] Errores y fallos no intencionados.**	**[A] Ataques Intencionados.**
[D] DATOS INFORMACIÓN					
[D] - Datos Correspondencia Interna y Externa	Posible falta de conocimiento en el ingreso de la información en las bases de datos por parte de los funcionarios responsables.	**NA**	**NA**	[E.1] Errores de los Usuarios [I] [C] [D] [E.2] Errores del Administrador [I] [C] [D] [E.4] Errores de Configuración [I] [E.15] Alteración accidental de la información. [I] [E.18] Destrucción de Información [D] [E.19] Fugas de Información. [C]	[A.3] Manipulación de los registros de actividad (Log) [I] [A.4] Manipulación de la Configuración. [I] [C] [D] [A.11] Acceso no Autorizado. [I] [C] [A.13] Repudio [I] [A.15] Modificación deliberada de la Información. [I] [A.18] Destrucción de Información. [D] [A.19] Divulgación de Información [C]
[D] - Copias de Seguridad	Omisión de copias de seguridad en los PC de las diferentes dependencias.				
[D] - Configuración de Equipos Propios de la Administración.	No se implementaron o no se da uso adecuado de los controles de acceso a los Servidores de Bases de Datos.				
[D] - Bases de Datos	Ausencia de actualización de los sistemas de base de datos y de parches de seguridad en los diferentes equipos de cómputo de las dependencias.				
[D] - Contraseñas	Se evidencia falta de validación de las contraseñas, no solicita la combinación de caracteres alfanuméricos en la contraseña				
[D] - Datos de Control de Acceso.	No se cuenta con auditorias periódicas y monitoreo adecuado del estado de la información				
[K] CLAVES CRIPTOGRÁFICAS					
[K] - Protección de la Información Correos Institucionales	No se cuenta con los niveles de seguridad adecuados para la protección de la	**NA**	**NA**	[E.1] Erroresde los Usuarios [C] [D] [I] [E.2] Errores del Administrador.	[A.5] Suplantación de la Identidad del Usuario. A. I.C [A.6] Abuso de

	información financiera.			[C] [I] [D] [E.15] Alteración accidental de la Información. [I]. [E.18] Destrucción de Información [D] [E.19] Fugas de Información. [C]	Privilegios de acceso. [C][I][D] [A.11] Acceso no autorizado. [C][I] [A.15] Modificación deliberada de la Información. [I] [A.18] Destrucción de Información. [D] [A.19] Divulgación de Información
[K] - Protección de las Comunicaciones - Voz IP	La eventual inexperiencia del personal de practica de otras dependencias, encargado de la alimentación de la información en el sistema, puede provocar en el ingreso erróneo de la información				
[K] - Protección de las Comunicaciones - Wifi	Presencia de exceso de privilegios y mala disposición de niveles de acceso para la información.				
		[S] SERVICIOS			
[S] - Servicios de Impresión	Ausencia de Políticas de Control de Acceso correspondiente a los Servidores de Bases de Datos.	**NA**	**NA**	[E.1] Errores de los Usuarios [I] [C] [D] [E.2] Errores del Administrador [I] [C] [D] [E.9] Errores de [re-]encaminamiento. [C] [E.10] Errores de Secuencia. [I] [E.15] Alteración accidental de la información. [I] [E.18] Destrucción de Información [D] [E.19] Fugas de Información. [C] [E.24] Caida del Sistema por Agotamiento de Recursos. [D] [E.25] Pérdida de Equipos. [D][C]	[A.5] Suplantación de la Identidad del Usuario. [A.6] Abuso de Privilegios de acceso. [C][I][D] [A.7] Uso no previsto. [C][I][D] [A.9] [Re-]encaminamiento de mensajes.[C] [A.10] Alteración de Secuencia. [I] [A.11] Acceso no autorizado. [C][I] [A.13] Repudio [I] [A.15] Modificación deliberada de la Información. [I] [A.18] Destrucción de Información. [D] [A.24] Denegación del Servicio. [D]
[S] - Servicio Soporte Técnico	No se cuenta con auditorias periódicas y monitoreo adecuado del estado de las Bases de Datos.				
[S] - Servicios Pagina Web Institucional (1)	Configuración insuficiente de servidor. Configuración errónea de los parámetros de autenticación.				
[S] - Servicio Correo Electronico - Google Sites (1)	Ineficiente sistema de autenticación y gestor de permisos y permisos.				
[S] - Transferencia de Archivos	Vulnerabilidad presentada en los servidores de Godaddy, frente a un control inadecuado de un alto tráfico.				
[S] - Gestión de usuarios y Contraseñas	Gestión y disposición errónea de las				

	cuentas para los usuarios.				
[SW] APLICACIONES (SOFTWARE)					
[SW] - Plataforma PISAMI (1)	Ausencia de capacitación (Ingeniería Social), concientización y plan de seguridad para los usuarios; que permita un uso adecuado y seguro del servicio.	**NA**	[I.5] Averia de Origen físico o Lógico [D]	[E.1] Errores de los Usuarios. [D][I][C] [E.2] Errores del Administrador [D][I][C] [E.8] Difusión de Software dañino [D][I][C] [E.9] Errores de [re-]encaminamiento. [C] [E.10] Errores de Secuencia. [I] [E.15] Alteración accidental de la Información. [I] [E.18] Destrucción de Información. [D] [E.19] Fugas de Información. [C] [E.20] Vulnerabilidades de los Programas. [I][D][C] [E.21] Errores de Mantenimiento / Actualización (Software). [I][D]	[A.5] Suplantación de la Identidad del Usuario. [C][A][I]. [A.6] Abuso de Privilegios de acceso. [C][I][D]. [A.7] Uso no previsto. [C][I][D] [A.8] Difusión de Software Dañino. [C][I][C]. [A.9] [Re-]encaminamiento de mensajes.[C] [A.10] Alteración de Secuencia. [I] [A.11] Acceso no autorizado. [C][I] [A.15] Modificación deliberada de la Información. [I] [A.18] Destrucción de Información. [D] [A.19] Divulgación de Información. [C] [A.22] Manipulación de Programas. [C][I][D]
[SW] - PHP y Larabel (1)	Daños generados por uso inadecuado del servicio por falta de capacitación del uso adecuado de las herramientas tecnológicas.				
[SW] - Apache (1)	Gestión de la configuración, disposición de accesos al servicio y gestión de capacitaciones para el uso adecuado del servicio				
[SW] - Windows 2016 Server Linux Centos 7	No se realizan las actualizaciones correspondientes y actuales al sistema. No se realiza un eficiente mantenimiento al sistema.				
[SW] - Joomla V.2.5	Instalación ineficiente, deficiente mantenimiento de los equipos.				
[SW] - Bases de Datos MySQL (1)	Configuración inadecuada o errada del protocolo.				
[SW] - Oracle 10G (1)	No se cuentan con los recursos suficientes para cubrir con lo requerido por la organización				
[SW] - Avira	Ineficientes medidas de seguridad implementadas; ausencia en la configuración UTM				

	para la detección de Intrusiones, zona desmilitarizada para la protección de los servidores.				
[SW] - Windows 10 Pro	Incorrecta configuración de usuarios y contraseñas. Uso de contraseñas genéricas.				
[HW] EQUIPOS INFORMÁTICOS (HARDWARE)					
[HW] - Servidor de Archivos FTP - Marca: DELL en Torre PowerEdge T130 (1)	No se cuentan disponibilidad suficiente, recursos físicos, humano necesario para cubrir con los casos de soporte requeridos por los usuarios organización	[N.1] Fuego [D] [N.2] Daños por Agua [D] [N.10]]Inundación [D]	[I.1] Fuego [D] [I.2] Daños por agua [D] [I.5] Avería de Origen físico o Lógico [D] [I.6] Corte del Suministro eléctrico [D] [I.7] Condiciones inadecuadas de temperatura o humedad [D] [I.11] Emanaciones Electromagnéticas.[C]	[E.2] Errores de Administrador [D] [I] [C] [E.23] Errores de Mantenimiento/Actualización de equipos [D] [E.24] Caída del Sistema por agotamiento de Recursos.[D] [E.25] Perdida de Equipos. [D]	[A.6] Abuso de Privilegios de Acceso [D] [I] [C] [A.7] Uso no previsto [D] [I] [C] [A.11] Acceso no autorizado [C] [I] [A.23] Manipulación de Equipos [C] [D] [A.24] Denegación de Servicio. [D] [A.25] Robo [C] [D] [A.26] Ataque Destructivo [D]
[HW] - Servidor DHCP - Marca: Dell en Torre PowerEdge T440 (1)	Ausencia de configuración de privilegios de aceptación o denegación de conectividad firewall, Ineficiente medidas de seguridad.				
[HW] - Servidor DHCP - Marca: Dell en Torre PowerEdge T440 (1)	Uso inadecuado. Ausencia de conocimiento sobre la operabilidad y uso del sistema operativo.				
[HW] - Equipos de Cómputo (1)	Fallos o vulnerabilidades presentes en la seguridad del sistema. Ausencia de plan de seguridad.				
[HW] - Equipos de Cómputo (6)	No se realizan las actualizaciones correspondientes y actuales al sistema. No se realiza un eficiente mantenimiento al sistema.				
[HW] - Equipos de Cómputo (2)	Fallos en la configuración de seguridad del sistema				

	operativo, ausencia de antivirus actualizado
[HW] - Equipos de Cómputo (1)	Fallos o vulnerabilidades presentes en la seguridad del sistema. Ausencia de plan de seguridad.
[HW] - Equipos de Cómputo (8)	Ausencia en el control de actualizaciones del sistema de seguridad e implantación de parches. No se realiza un eficiente mantenimiento al sistema.
[HW] - Grupo de Talento Humano (7)	Configuraciones erradas que generan deficiencias en el funcionamiento adecuado del software.
[HW] - Impresora Marca: HP LASERJET M1212NF (1)	Fallos o vulnerabilidades presentes en la seguridad del sistema. Ausencia de plan de seguridad.
[HW] - Impresora Marca: HP LASERJET ENTERPRISE M608 (1)	Ausencia en el control de actualizaciones del sistema de seguridad e implantación de parches. No se realiza un eficiente mantenimiento al sistema.
[HW] - Impresora Marca: HP LASERJET PRO MFP M426FDW (1)	Configuraciones erradas que generan deficiencias en el funcionamiento adecuado del software.
[HW] - Impresora Marca: HP LASERJET P4515x (1)	Fallos o vulnerabilidades presentes en la seguridad del sistema. Ausencia de plan de seguridad.

[HW] - Impresora Marca: LASERJET 600 M603 (1)	Ausencia en el control de actualizaciones del sistema de seguridad e implantación de parches. No se realiza un eficiente mantenimiento al sistema.	
[HW] - Impresora Marca: HP OFFICEJET PRO 8600 (1)	Configuraciones erradas que generan deficiencias en el funcionamiento adecuado del software.	
[HW] - Impresora Marca: HP LASERJET M1522N (1)	Ausencia en el control de actualizaciones del sistema de seguridad e implantación de parches. No se realiza un eficiente mantenimiento al sistema.	
[HW] - Impresora Marca: KYOCERA FS-1035MFP (1)	Ausencia en la configuración adecuada de permisos para la aceptación o denegación de conexiones.	
[HW] - Puntos de Acceso Alámbricos	Fallos o vulnerabilidades presentes en la seguridad del sistema. Ausencia de plan de seguridad.	
[HW] - Swtches: Marca ArubaOS-Switch, ARUBA 2530 24G (6)	Ausencia en el control de actualizaciones del sistema de seguridad e implantación de parches. No se realiza un eficiente mantenimiento al sistema.	
[HW] - Cortafuegos Cisco ASA 5505 (1)	Configuraciones erradas que generan deficiencias en el funcionamiento adecuado del software.	

[HW] - Puntos de Acceso (2)	Fallos o vulnerabilidades presentes en la seguridad del sistema. Ausencia de plan de seguridad.				
[HW] - Teléfono IP (6)	Ausencia en el control de actualizaciones del sistema de seguridad e implantación de parches. No se realiza un eficiente mantenimiento al sistema.				
[COM] REDES DE COMUNICACIONES					
[ISDN] Sistema Comunicación Voz IP	Configuraciones erradas que generan deficiencias en el funcionamiento adecuado del software.				[A.5] suplantación de la Identidad del Usuario. [C][A][I] [A.6] Abuso de Privilegios de Acceso [D] [I] [C] [A.7] Uso no previsto [D] [I] [C] [A.9] [Re-]encaminamiento de mensajes.[C] [A.10] Alteración de Secuencia. [I] [A.11] Acceso no autorizado. [C][I] [A.12] Análisis de tráfico. [C]. [A.14] Interceptación de Información (Escucha) [A.15] Modificación deliberada de la Información. [I] [A.19] Divulgación de Información. [C]. [A.24] Denegación de Servicio. [D]
[wifi] Red Inalámbrica - Institucional	Ausencia de sistema de Seguridad adecuado				
[LAN] Red Local Institucional	Ausencia de encapsulamiento de protocoles.				
[Internet] Internet Palacio	Fallas relacionadas con el internet, intermitencia, por daños en la infraestructura o inutilidad del mismo.		[I.8] Fallo de Servicios de Comunicaciones. D	[E.2] Errores del Administrador [D][I][C] [E.9] Errores de [re-]encaminamiento. [C] [E.10] Errores de Secuencia. [I] [E.15] Alteración accidental de la Información. [I] [E.18] Destrucción de Información. [D] [E.19] Fugas de Información. [C]	
[Media] SOPORTES DE INFORMACIÓN					

[vdisk] Plus	Cloud	Intermitencia del servicio por fallas.	[N.1] Fuego [D] [N.2] Daños por Agua [D] [N.10]]Inundación [D]	[I.1] Fuego [D] [I.2] Daños por agua [D] [I.5] Avería de Origen físico o Lógico [D] [I.6] Corte del Suministro eléctrico [D] [I.7] Condiciones inadecuadas de temperatura o humedad [D] [I.10] Degradación de los soportes de almacenamiento de la información [D] [I.11] Emanaciones Electromagnéticas.[C]	[E.1] Errores de los Usuarios. [D][I][C] [E.2] Errores del Administrador [D][I][C] [E.15] Alteración accidental de la Información. [I] [E.18] Destrucción de Información. [D] [E.19] Fugas de Información. [C] [E.23] Errores de Mantenimiento/Actualización de equipos [D] [E.25] Pérdida de Equipos. [D][C]	[A.7] Uso no previsto [D] [I] [C] [A.11] Acceso no autorizado. [C][I] [A.15] Modificación deliberada de la Información. [I] [A.18] Destrucción de Información. [D] [A.23] Manipulación de Equipos [C] [D]. [A.25] Robo [C] [D] [A.26] Ataque Destructivo [D]
[AUX] EQUIPAMIENTO AUXILIAR						
[AUX] - UPS del Alcaldía		Falta de conocimiento en la manipulación de los dispositivos	[N.1] Fuego [D] [N.2] Daños por Agua [D] [N.10]]Inundación [D]	[I.1] Fuego [D] [I.2] Daños por agua [D] [I.5] Avería de Origen físico o Lógico [D]	[E.23] Errores de Mantenimiento/Actualización de equipos [D] [E.24] Caída del Sistema por Agotamiento de Recursos. [D]	[A.7] Uso no previsto [D] [I] [C] [A.11] Acceso no autorizado. [C][I] [A.23] Manipulación de Equipos [C] [D] [A.25] Robo [C] [D]
[AUX] - Cableado Eléctrico		Deterioro total o parcial del cableado incluido equipos conectados al mismo.				

[AUX] - Cableado Estructurado	Daños por uso e instalación inadecuado.		[I.6] Corte del Suministro eléctrico [D] [I.7] Condiciones inadecuadas de temperatura o humedad [D] [I.9] Interrupción de Otros Servicios Suministros [D]. [I.11] Emanaciones Electromagnéticas.[C]	[E.25] Pérdida de Equipos. [D][C]	[A.26] Ataque Destructivo [D]
[L] INSTALACIONES					
[L] - Instalaciones Palacio	Falta de un Sistema Biométrico o de monitoreo para el acceso a las Instalaciones y dependencias de acceso restringido.	[N.1] Fuego [D] [N.2] Daños por Agua [D] [N.10]]Inundación [D]	[I.1] Fuego [D] [I.2] Daños por agua [D] [I.11] Emanaciones Electromagnéticas.[C]	[E.15] Alteración accidental de la Información. [I] [E.18] Destrucción de Información. [D] [E.19] Fugas de Información. [C]	[A.7] Uso no previsto [D] [I] [C] [A.11] Acceso no autorizado. [C][I] [A.15] Modificación deliberada de la Información. [I] [A.18] Destrucción de Información. [D]. [A.19] Divulgación de Información. [C]. [A.26] Ataque Destructivo [D]. [A.27] Ocupación Enemiga. [D][C]
[P] PERSONAL					
[P] - Funcionarios de Planta y Contratistas (75)	Susceptibilidad de los servidores públicos a ser obligados para ejecutar actos inicuos en contra la			[E.7] Deficiencias en la Organización. [D] [E.15] Alteración accidental de la	[A.28] Indisponibilidad del Personal [D] [A.29] Extorsión. [C][I][D]

	Administración Municipal.		Información. [I] [E.19] Fugas de Información. [C] [E.28] Indisponibilidad del Personal. [D]	[A.30] Ingeniería Social. [C][I][D].
[P] - Funcionarios de Planta y Contratistas (75)	Deficiencia en el monitoreo sobre el uso adecuado de la información publicada en la Plataforma PISAMI y el control de acceso a los datos, carencia de LOGS de auditoría.			
[P] - Funcionarios de Planta y Contratistas (75)	Ausencia del personal por incapacidades medicas a a causa del COVID 19, y deficiencia en los procesos contractuales para la contratación de nuevo personal.			
[P] - Técnicos/Ausxiliares de Mantenimiento (2)	Ausencia del personal por incapacidades medicas a a causa del COVID 19, y deficiencia en los procesos contractuales para la contratación de nuevo personal.			
[P] - Técnicos/Ausxiliares de Mantenimiento (2)	Susceptibilidad de los servidores públicos a ser obligados para ejecutar actos inicuos en contra la Administración Municipal.			
[P] - Profesionales	Susceptibilidad de los servidores públicos a ser obligados para ejecutar actos inicuos en contra la Administración Municipal.			
[P] - Profesionales	Ausencia del personal por incapacidades medicas a a causa del COVID 19, y deficiencia en los procesos contractuales para la			

	contratación de nuevo personal.
[P] - Servicio Web: MEDIA COMMERCE PARTNERS (1)	Suministro de información a terceros mediante amenazas.
[P] - Servicio Correo Institucional: ITO SOFTWARE SAS (1)	Entrega de información confidencial a terceros por presión mediante extorsión

Fuente 1. El Autor

6.2.5 VALORACIÓN DE AMENAZAS

Basados en la identificación de amenazas de cada uno de los activos de información, se efectúa el respectivo análisis y valoración cuantitativa y cualitativa, ello basado en la aplicación de la metodología MARGERIT, la cual establece estándares como los descritos en los cuadro 1, 2, 3 y 4.

Cuadro 1. Probabilidad de Riesgo

	Nomenclatura	Categoría	Valoración
Probabilidad	MA	**Prácticamente seguro**	5
	A	**Probable**	4
	M	**Posible**	3
	B	**Poco probable**	2
	MB	**Muy raro**	1
Fuente. El Autor			

Cuadro 2. Impacto de Riesgo

	Nomenclatura	Categoría	Valoración
Impacto	MA	**Muy Alto**	5
	A	**Alto**	4
	M	**Medio**	3
	B	**Bajo**	4

	MB	**Muy Bajo**	1
Fuente. El Autor			

Cuadro 3. Valoración del Riesgo

IMPACTO	**MA**					
	A					
	M					
	B					
	MB					
RIESGO		**MB**	**B**	**M**	**A**	**MA**
		PROBABILIDAD				
Fuente. El Autor						

Cuadro 4. Valoración del Riesgo 2

	Nomenclatura	**Categoría**	**Valoración**
Valoración del riesgo	MA	**Critico**	21 a 25
	A	**Importante**	16 a 20
	M	**Apreciable**	10 a 15
	B	**Bajo**	5 a 9
	MB	**Despreciable**	1 a 4
Fuente. El Autor			

6.2.5.1 Valoración Cualitativa*:*

Una vez identificado los Activos de la información y establecido los criterios de evaluación tanto la valoración como el impacto del riesgo a continuación se relaciona la valoración cualitativa por cada una de sus dimensiones, información que se podrá evidenciar en la Metodología MARGERIT. Ver. Anexo: I.” Anexo I - Matriz Metodología – MARGERIT”

Tabla 18. Valoración Activos

DATOS DEL ACTIVO DE INFORMACIÓN				DIMENSIÓN				
No.	Nombre del activo de información	Proceso propietario del activo	Responsable	Dimensión Autenticidad(B / M /A / MA/ MB)	Dimensión Trazabilidad (B / M /A / MA/ MB)	Dimensión Confidencialidad (B / M /A / MA/ MB)	Dimensión Integridad (B / M /A / MA/ MB)	Dimensión Disponibilidad (B / M /A / MA/ MB)
1	[D] - Datos Correspondencia Interna y Externa	Secretaría de la TIC, Grupo Ciencia, Tecnología e Innovación	Profesional Universitario	B	B	B	B	B
2	[D] - Copias de Seguridad	Secretaría de la TIC, Ciencia, Tecnología e Innovación	Profesional Universitario	B	B	MA	MA	MA
3	[D] - Configuración de Equipos Propios del Palacio	Secretaría de la TIC, Ciencia, Tecnología e Innovación	Técnico Operativo	B	B	B	B	B
4	[D] - Bases de Datos	Secretaría de la TIC, Ciencia, Tecnología e Innovación	Profesional Universitario	B	B	MA	MA	MA
5	[D] - Contraseñas	Secretaría de la TIC, Ciencia, Tecnología e Innovación	Profesional Universitario	B	B	B	B	B
6	[D] - Datos de Control de Acceso.	Secretaría de la TIC, Ciencia, Tecnología e Innovación	Profesional Universitario	B	B	B	B	B
7	[K] - Protección de la Información Correos Institucionales	Secretaría de la TIC, Grupo de Infraestructura Tecnológica	Profesional Universitario	B	B	B	B	B
8	[K] - Protección de las Comunicaciones - Voz IP	Secretaría de la TIC, Grupo de Infraestructura Tecnológica	Profesional Universitario	B	B	B	B	B
9	[K] - Protección de las Comunicaciones - Wifi	Secretaría de la TIC, Grupo de Infraestructura Tecnológica	Profesional Universitario	B	B	B	B	B
10	[S] - Servicios de Impresión	Secretaría de la TIC, Grupo de Infraestructura Tecnológica	Técnico Operativo	B	B	B	B	B
11	[S] - Servicio Soporte Técnico	Secretaría de la TIC, Grupo de Infraestructura Tecnológica	Técnico Operativo	B	B	B	B	B
12	[S] - Servicios Pagina Web Institucional (1)	Secretaría de la TIC, Grupo de Infraestructura Tecnológica	Profesional Universitario	A	B	MA	MA	MA

DATOS DEL ACTIVO DE INFORMACIÓN				DIMENSIÓN				
No.	Nombre del activo de información	Proceso propietario del activo	Responsable	Dimensión Autenticidad(B / M /A / MA/ MB)	Dimensión Trazabilidad (B / M /A / MA/ MB)	Dimensión Confidencialidad (B / M /A / MA/ MB)	Dimensión Integridad (B / M /A / MA/ MB)	Dimensión Disponibilidad (B / M /A / MA/ MB)
13	[S] - Servicio Correo Electrónico - Google Sites (1)	Secretaría de la TIC, Grupo de Infraestructura Tecnológica	Profesional Universitario	M	MB	A	A	M
14	[S] - Transferencia de Archivos	Secretaría de la TIC, Grupo de Infraestructura Tecnológica	Técnico Operativo	MB	MB	MA	MA	MA
15	[S] - Gestión de usuarios y Contraseñas	Secretaría de la TIC, Grupo de Infraestructura Tecnológica	Técnico Operativo	B	B	A	MA	MA
16	[SW] - Plataforma PISAMI (1)	Secretaría de la TIC, Ciencia, Tecnología e Innovación	Profesional Universitario	B	B	A	MA	MA
17	[SW] - PHP y Larabel (1)	Secretaría de la TIC, Ciencia, Tecnología e Innovación	Profesional Universitario	B	B	A	MA	MA
18	[SW] - Apache (1)	Secretaría de la TIC, Ciencia, Tecnología e Innovación	Profesional Universitario	B	B	MA	MA	MA
19	[SW] - Windows 2016 Server Linux Centos 7	Secretaría de la TIC, Ciencia, Tecnología e Innovación	Técnico Operativo	MB	MB	MA	MA	MA
20	[SW] - Joomla V.2.5	Secretaría de la TIC, Ciencia, Tecnología e Innovación	Profesional Universitario	MB	MB	MA	MA	MA
21	[SW] - Bases de Datos MySQL (1)	Secretaría de la TIC, Ciencia, Tecnología e Innovación	Profesional Universitario	B	B	A	MA	MA
22	[SW] - Oracle 10G (1)	Secretaría de la TIC, Ciencia, Tecnología e Innovación	Profesional Universitario	B	B	A	MA	MA
23	[SW] - Avira	Secretaría de la TIC, Ciencia, Tecnología e Innovación	Técnico Operativo	B	B	MA	MA	MA
24	[SW] - Windows 10 Pro	Secretaría de la TIC, Ciencia, Tecnología e Innovación	Técnico Operativo	MB	MB	MA	MA	MA
25	[HW] - Servidor de Archivos FTP - Marca:	Antigua Oficina de Sistemas	Profesional Universitario	B	B	A	A	MA

	DATOS DEL ACTIVO DE INFORMACIÓN			DIMENSIÓN				
No.	Nombre del activo de información	Proceso propietario del activo	Responsable	Dimensión Autenticidad(B / M /A / MA/ MB)	Dimensión Trazabilidad (B / M /A / MA/ MB)	Dimensión Confidencialidad (B / M /A / MA/ MB)	Dimensión Integridad (B / M /A / MA/ MB)	Dimensión Disponibilidad (B / M /A / MA/ MB)
	DELL en Torre PowerEdge T130 (1)							
26	[HW] - Servidor DHCP - Marca: Dell en Torre PowerEdge T440 (1)	Antigua Oficina de Sistemas	Profesional Universitario	B	B	A	A	MA
27	[HW] - Servidor DHCP - Marca: Dell en Torre PowerEdge T440 (1)	Antigua Oficina de Sistemas	Profesional Universitario	B	B	A	A	MA
28	[HW] - Equipos de Computo (1)	Secretaría de las TIC - Despacho	Secretaria de Despacho	MB	MB	A	A	MA
29	[HW] - Equipos de Computo (6)	Grupo de Ciencia, Tecnología e Innovación	Funcionarios Dependencia	B	B	B	B	MA
30	[HW] - Equipos de Computo (2)	Grupo de Infraestructura Tecnología	Funcionarios Dependencia	B	B	B	B	MA
31	[HW] - Equipos de Computo (1)	Secretaría Administrativa	Secretaria de Despacho	B	B	B	B	MA
32	[HW] - Equipos de Computo (8)	Grupo de Recursos Físicos	Funcionarios Dependencia	B	B	B	B	MA
33	[HW] - Grupo de Talento Humano (7)	Grupo de Talento Humano	Funcionarios Dependencia	B	B	B	B	MA
34	[HW] - Impresora Marca: HP LASERJET M1212NF (1)	Secretaría de las TIC - Grupo Ciencia, Tecnología e Innovación	Funcionarios Dependencia	MB	MB	MB	MB	MA
35	[HW] - Impresora Marca: HP LASERJET ENTERPRISE M608 (1)	Secretaría de las TIC - Grupo Infraestructura Tecnológica	Funcionarios Dependencia	MB	MB	MB	MB	MA
36	[HW] - Impresora Marca: HP LASERJET PRO MFP M426FDW (1)	Secretaría Administrativa - Despacho	Secretaria de Despacho	MB	MB	MB	MB	MA
37	[HW] - Impresora Marca: HP LASERJET P4515x (1)	Secretaría de las TIC	Funcionarios Dependencia	MB	MB	MB	MB	MA

	DATOS DEL ACTIVO DE INFORMACIÓN			DIMENSIÓN				
No.	Nombre del activo de información	Proceso propietario del activo	Responsable	Dimensión Autenticidad(B / M /A / MA/ MB)	Dimensión Trazabilidad (B / M /A / MA/ MB)	Dimensión Confidencialidad (B / M /A / MA/ MB)	Dimensión Integridad (B / M /A / MA/ MB)	Dimensión Disponibilidad (B / M /A / MA/ MB)
38	[HW] - Impresora Marca: LASERJET 600 M603 (1)	Secretaría Administrativa - Despacho - Dirección de Recursos Físicos	Funcionarios Dependencia	MB	MB	MB	MB	MA
39	[HW] - Impresora Marca: HP OFFICEJET PRO 8600 (1)	Secretaría Administrativa - Despacho - Dirección de Recursos Físicos	Funcionarios Dependencia	MB	MB	MB	MB	MA
40	[HW] - Impresora Marca: HP LASERJET M1522N (1)	Secretaría Administrativa - Dirección de Talento Humano	Funcionarios Dependencia	MB	MB	MB	MB	MA
41	[HW] - Impresora Marca: KYOCERA FS-1035MFP (1)	Secretaría Administrativa - Dirección de Talento Humano	Funcionarios Dependencia	MB	MB	MB	MB	MA
42	[HW] - Puntos de Acceso Alámbricos	Red de Datos - Palacio	Técnico Operativo	B	B	A	A	MA
43	[HW] - Switches: Marca ArubaOS-Switch, ARUBA 2530 24G (6)	Red de Datos - Secretaría Administrativa	Técnico Operativo	B	B	A	A	MA
44	[HW] - Cortafuegos Cisco ASA 5505 (1)	Secretaría de las TIC	Técnico Operativo	MB	MB	A	A	MA
45	[HW] - Puntos de Acceso (2)	Secretaría de las TIC	Técnico Operativo	B	B	A	A	MA
46	[HW] - Teléfono IP (6)	Dependencias	Técnico Operativo	B	B	A	A	A
47	[COM] - Sistema Comunicación Voz IP	Palacio Municipal de Ibagué	Técnico Operativo	B	B	A	A	MA
48	[COM] - Red Inalámbrica - Institucional	Palacio Municipal de Ibagué	Técnico Operativo	B	B	A	B	A
49	[COM] - Red Local Institucional	Palacio Municipal de Ibagué	Técnico Operativo	B	B	MA	MA	MA
50	[COM] - Internet Palacio	Palacio Municipal de Ibagué	Técnico Operativo	B	B	MA	MA	MA

	DATOS DEL ACTIVO DE INFORMACIÓN			DIMENSIÓN				
No.	Nombre del activo de información	Proceso propietario del activo	Responsable	Dimensión Autenticidad(B / M /A / MA/ MB)	Dimensión Trazabilidad (B / M /A / MA/ MB)	Dimensión Confidencialidad (B / M /A / MA/ MB)	Dimensión Integridad (B / M /A / MA/ MB)	Dimensión Disponibilidad (B / M /A / MA/ MB)
51	[Media] - Cloud Plus	Departamento de Sistemas	Técnico Operativo	B	B	MA	MA	MA
52	[AUX] - UPS del Palacio	Datacenter	Técnico Operativo	B	B	B	B	MA
53	[AUX] - Cableado Eléctrico	Palacio Municipal de Ibagué	Técnico Operativo	B	B	B	B	MA
54	[AUX] - Cableado Estructurado	Palacio Municipal de Ibagué	Técnico Operativo	B	B	B	B	MA
55	[L] - Instalaciones Palacio	Palacio Municipal de Ibagué	Funcionarios Dependencia	B	B	A	A	A
57	[P] - Funcionarios de Planta y Contratistas (75)	Palacio Municipal de Ibagué	NA	B	B	A	A	MA
58	[P] - Técnicos/Auxiliares de Mantenimiento (2)	Secretaría de las TIC, Grupo Infraestructura Tecnología	NA	B	B	A	A	MA
59	[P] - Profesionales	Secretaría de las TIC, Grupo de Ciencia, Tecnología e Innovación	NA	B	B	A	A	MA
60	[P] - Servicio Web: MEDIA COMMERCE PARTNERS (1)	Secretaría de las TIC	NA	B	B	MA	MA	MA
61	[P] - Servicio Correo Institucional: ITO SOFTWARE SAS (1)	Secretaría de las TIC	NA	B	B	MA	MA	MA

Fuente. El Autor

6.2.5.2 Valoración Cuantitativa:

Teniendo en cuenta la importancia de los activos de la entidad, y con el fin de identificar el nivel de riesgo de cada uno de ellos, se procede a efectuar la valoración cuantitativa de cada uno de ellos, reflejada en la tabla 19. Ver. Anexo: H.” Matriz Metodología – MARGERIT”

Tabla 19. Valoración Cuantitativa.

NOMBRE	RIESGO	AUTENTICIDAD	TRAZABILIDAD	CONFIDENCIALIDAD	INTEGRIDAD	DISPONIBILIDAD	VALOR
[D] - Datos Correspondencia Interna y Externa	BAJO	9	9	9	9	9	9
[D] - Copias de Seguridad	IMPORTANTE	9	9	25	25	25	19
[D] - Configuración de Equipos Propios del Palacio	BAJO	9	9	9	9	9	9
[D] - Bases de Datos	IMPORTANTE	9	9	25	25	25	19
[D] - Contraseñas	BAJO	9	9	9	9	9	9
[D] - Datos de Control de Acceso.	BAJO	9	9	9	9	9	9
[K] - Protección de la Información Correos Institucionales	BAJO	9	9	9	9	9	9
[K] - Protección de las Comunicaciones - Voz IP	BAJO	9	9	9	9	9	9
[K] - Protección de las Comunicaciones - Wifi	BAJO	9	9	9	9	9	9
[S] - Servicios de Impresión	BAJO	9	9	9	9	9	9
[S] - Servicio Soporte Técnico	BAJO	9	9	9	9	9	9
[S] - Servicios Pagina Web Institucional (1)	CRITICO	20	9	25	25	25	21
[S] - Servicio Correo Electrónico - Google Sites (1)	APRECIABLE	15	4	20	20	15	15
[S] - Transferencia de Archivos	IMPORTANTE	4	4	25	25	25	17
[S] - Gestión de usuarios y Contraseñas	IMPORTANTE	9	9	20	25	25	18

NOMBRE	RIESGO	AUTENTICIDAD	TRAZABILIDAD	CONFIDENCIALIDAD	INTEGRIDAD	DISPONIBILIDAD	VALOR
[SW] - Plataforma PISAMI (1)	IMPORTANTE	9	9	20	25	25	18
[SW] - PHP y Larabel (1)	IMPORTANTE	9	9	20	25	25	18
[SW] - Apache (1)	IMPORTANTE	9	9	25	25	25	19
[SW] - Windows 2016 Server Linux Centos 7	IMPORTANTE	4	4	25	25	25	17
[SW] - Joomla V.2.5	IMPORTANTE	4	4	25	25	25	17
[SW] - Bases de Datos MySQL (1)	IMPORTANTE	9	9	20	25	25	18
[SW] - Oracle 10G (1)	IMPORTANTE	9	9	20	25	25	18
[SW] - Avira	IMPORTANTE	9	9	25	25	25	19
[SW] - Windows 10 Pro	IMPORTANTE	4	4	25	25	25	17
[HW] - Servidor de Archivos FTP - Marca: DELL en Torre PowerEdge T130 (1)	IMPORTANTE	9	9	20	20	25	17
[HW] - Servidor DHCP - Marca: Dell en Torre PowerEdge T440 (1)	IMPORTANTE	9	9	20	20	25	17
[HW] - Servidor DHCP - Marca: Dell en Torre PowerEdge T440 (1)	IMPORTANTE	9	9	20	20	25	17
[HW] - Equipos de Cómputo (1)	APRECIABLE	4	4	20	20	25	15
[HW] - Equipos de Cómputo (6)	APRECIABLE	9	9	9	9	25	12
[HW] - Equipos de Cómputo (2)	APRECIABLE	9	9	9	9	25	12
[HW] - Equipos de Cómputo (1)	APRECIABLE	9	9	9	9	25	12
[HW] - Equipos de Cómputo (8)	APRECIABLE	9	9	9	9	25	12
[HW] - Grupo de Talento Humano (7)	APRECIABLE	9	9	9	9	25	12
[HW] - Impresora Marca: HP LASERJET M1212NF (1)	BAJO	4	4	4	4	25	8
[HW] - Impresora Marca: HP LASERJET ENTERPRISE M608 (1)	BAJO	4	4	4	4	25	8
[HW] - Impresora Marca: HP LASERJET PRO MFP M426FDW (1)	BAJO	4	4	4	4	25	8

NOMBRE	RIESGO	AUTENTICIDAD	TRAZABILIDAD	CONFIDENCIALIDAD	INTEGRIDAD	DISPONIBILIDAD	VALOR
[HW] - Impresora Marca: HP LASERJET P4515x (1)	BAJO	4	4	4	4	25	8
[HW] - Impresora Marca: LASERJET 600 M603 (1)	BAJO	4	4	4	4	25	8
[HW] - Impresora Marca: HP OFFICEJET PRO 8600 (1)	BAJO	4	4	4	4	25	8
[HW] - Impresora Marca: HP LASERJET M1522N (1)	BAJO	4	4	4	4	25	8
[HW] - Impresora Marca: KYOCERA FS-1035MFP (1)	APRECIABLE	4	4	20	20	25	15
[HW] - Puntos de Acceso Alámbricos	IMPORTANTE	9	9	20	20	25	17
[HW] - Switches: Marca ArubaOS-Switch, ARUBA 2530 24G (6)	IMPORTANTE	9	9	20	20	20	16
[HW] - Cortafuegos Cisco ASA 5505 (1)	IMPORTANTE	9	9	20	20	25	17
[HW] - Puntos de Acceso (2)	IMPORTANTE	9	9	20	20	25	17
[HW] - Teléfono IP (6)	IMPORTANTE	9	9	20	20	25	17
[COM] - Sistema Comunicación Voz IP	BAJO	4	4	4	4	25	8
[COM] - Red Inalámbrica - Institucional	IMPORTANTE	9	9	20	20	25	17
[COM] - Red Local Institucional	IMPORTANTE	9	9	20	20	25	17
[COM] - Internet Palacio	APRECIABLE	4	4	20	20	25	15
[Media] - Cloud Plus	IMPORTANTE	9	9	20	20	25	17
[AUX] - UPS del Palacio	IMPORTANTE	9	9	20	20	20	16
[AUX] - Cableado Eléctrico	IMPORTANTE	9	9	20	20	25	17
[AUX] - Cableado Estructurado	APRECIABLE	9	9	20	9	20	13
[L] - Instalaciones Palacio	IMPORTANTE	9	9	25	25	25	19
[P] - Funcionarios de Planta y Contratistas (75)	IMPORTANTE	9	9	25	25	25	19
[P] - Técnicos/Auxiliares de Mantenimiento (2)	IMPORTANTE	9	9	25	25	25	19
[P] - Profesionales	APRECIABLE	9	9	9	9	25	12
[P] - Servicio Web: MEDIA COMMERCE PARTNERS (1)	APRECIABLE	9	9	9	9	25	12
[P] - Servicio Correo Institucional: ITO SOFTWARE SAS (1)	APRECIABLE	9	9	9	9	25	12

Fuente El Autor

6.2.5.3 Resultado Valoración de Amenazas:

Con el fin de valorar las amenazas identificadas, se identifica la criticidad neta de cada una de las amenazas del Sistema de Gestión, el cual se determina teniendo los parámetros determinados en la metodología MARGERIT, anexo H, del presente trabajo.

Tabla 20. Valoración Criticidad

Categoría	Valoración
Critico	21 a 25
Importante	16 a 20
Apreciable	10 a 15
Bajo	5 a 9
Despreciable	1 a 4

Fuente 2Fuente. Anexo H. Matriz Metodología – MARGERIT

Basados en lo detallado previamente, y los resultados generados en la matriz, a continuación de presenta un breve análisis de los resultados obtenidos.

Tabla 21. Resultado Valoración NETA

Categoría	Cantidad de amenazas por categoría
Critico	63
Importante	3
Apreciable	0
Bajo	0
Despreciable	0

Fuente. Anexo H. Matriz Metodología – MARGERIT

Como resultado de la evaluación efectuada sobre las 63 amenazas, que se encuentran relacionadas directamente sobre los activos anticipadamente identificados que hacen parte del Sistema de Gestión Documental de la Administración Municipal de Ibagué.

Adicionalmente se aplica el análisis según lo definitivo por el mapa de calor de la 'Matriz de análisis de riesgos' Anexo: H." Matriz Metodología – MARGERIT" en el cual se ve relacionado el nivel de impacto que se encuentra relacionado con cada uno de los activos, permitiendo una imagen visual, completa y sencilla con respecto a los riesgos que representan un mayor o menor impacto y así respectivamente cuales requieren por nuestra parte de un mayor enfoque:

Cuadro 5. Mapa de Calor - Riesgos

		IMPACTO				
		Insignificante	**Menor**	**Moderado**	**Mayor**	**Catastrófico**
IMPACTO	**MUY ALTA**		, R76, R69, R34, R33, R32, R31, R30, R29, R19, R17, R16, R6, R4, R2, R1	, R78, R77, R73, R72, R71, R70, R66, R65, R64, R63, R61, R60, R59, R58, R57, R56, R50, R36, R35, R28, R27, R26, R25, R23, R22, R21, R20, R18, R11, R10, R9, R8, R7, R5	, R79, R74, R68, R67, R62, R55, R53, R52, R49, R48, R46, R45, R44, R43, R42, R41, R40, R39, R38, R37, R24, R12	, R40, R40, R38, R37, R35, R34, R32, R31, R30, R29, R28, R27, R19, R14, R13, R12, R8
	ALTA		, R3			
	MEDIA					
	BAJA					
	MUY BAJA					
RIESGO		**MUY BAJA**	**BAJA**	**MEDIA**	**ALTA**	**MUY ALTA**
		PROBABILIDAD				

Fuente. Autor

Tabla 22. Impacto de Riesgo

Impacto	Riesgos identificados	Cantidad de riesgos
Catastrófico	R40, R40, R38, R37, R35, R34, R32, R31, R30, R29, R28, R27, R19, R14, R13, R12, R8	17
Mayor	, R79, R74, R68, R67, R62, R55, R53, R52, R49, R48, R46, R45, R44, R43, R42, R41, R40, R39, R38, R37, R24, R12	22
Moderado	, R78, R77, R73, R72, R71, R70, R66, R65, R64, R63, R61, R60, R59, R58, R57, R56, R50, R36, R35, R28, R27, R26, R25, R23, R22, R21, R20, R18, R11, R10, R9, R8, R7, R5	34
Menor	, R76, R69, R34, R33, R32, R31, R30, R29, R19, R17, R16, R6, R4, R2, R1	15
Insignificante		0

6.2.6 IDENTIFICACIÓN SALVAGUARDAS:

La Administración Municipal de Ibagué, cuenta con determinadas salvaguardas; sin embargo, son estimados como un punto de partida debido a que primeramente se encuentran conexos a fallos, aspectos mal configurados y otras vulnerabilidades por las cuales primero deben ser rectificadas y posteriormente evaluar la necesidad de ejecución de nuevos o adicionales salvaguardas.

De esta manera se relaciona las salvaguardas identificadas:

- Cortafuegos: Cisco ASA 5505.
- Antivirus: Avira.
- Servidor FTP.
- Soporte a la infraestructura tecnológica: 9/5 – El soporte brindado por el personal de la administración municipal es basado en la jornada laboral, el cual corresponde a: lunes a viernes de 07:00 a 12:00 m y 02: 00 a 06:00 p.m

Así mismo, teniendo en cuenta los controles existentes en la Administración Municipal, a continuación, se detalla los cambios efectuados en la criticidad de las amenazas.

Tabla 23. Valoración Residual de Amenazas Identificadas

Categoría	Cantidad de amenazas por categoría
Critico	**46**
Importante	13
Apreciable	1
Bajo	6
Despreciable	0

Fuente . Anexo H. Matriz Metodología – MARGERIT

Basados en la información obtenida, se efectúa valoración de la aceptación del riesgo la cual se encuentra relacionada en cada una de las amenazas residuales, la cual se evidencia en la siguiente tabla:

Tabla 24. Aceptación del Riesgo

ACEPTACIÓN DEL RIESGO	
Niveles	
Aceptable	0
Moderado	7
Inaceptable	59

Fuente El Autor

7 PROPONER MECANISMOS DE CONTROL Y GESTIÓN QUE REDUZCAN LAS VULNERABILIDADES IDENTIFICADAS EN EL ANÁLISIS REALIZADO

Con el fin de proponer Mecanismos de Control adecuados para la Administración Municipal, que conlleven a mejorar la protección de sus activos tanto físicos como electrónicos a continuación, se detalla los dominios, objetivos y controles que establece la Norma ISO/IEC 27002:2013.

Tabla 25. Controles - Norma ISO[54]

Dominios	Objetivos	Controles
5. Políticas de seguridad	5.1 Directrices de la Dirección en seguridad de la información	5.1.1 conjunto de políticas de la seguridad de la información
		5.1.2 Revisión de las políticas para la seguridad de la información
6. Aspectos organizativos de la seguridad de la información	6.1 Organización Interna	6.1.1 Asignación de responsabilidades para la seguridad de la información
		6.1.2 Segregación de tareas
		6.1.3 Contacto con las autoridades
		6.1.4 Contacto con grupos de interés especial
		6.1.5 seguridad de la información en la gestión de proyectos
	6.2 Dispositivos para movilidad y teletrabajo	6.2.1 Política de uso de dispositivos para movilidad
		6.2.2 Teletrabajo
7. Seguridad ligada a los recursos humanos	7.1 Antes de la contratación	7.1.1 Investigación de antecedentes
		7.1.2 Términos y condiciones de contratación
	7.2 Durante la contratación	7.2.1 Responsabilidad de gestión
		7.2.2 Concienciación, educación y capacitación en seguridad de la información
		7.2.3 Proceso disciplinario
	7.3 Cese o cambio de puesto de trabajo	7.3.1 Cese o cambio de puesto de trabajo
8. Gestión Activos	8.1 Responsabilidad sobre los activos	8.1.1 Inventario de activos
		8.1.2 Propiedad de los activos
		8.1.3 Uso aceptable de los activos
		8.1.4 Devolución de activos
		8.2.1 Directrices de clasificación

[54] ISO.es. Controles ISO 27002-2013. [Sitio Web] https://www.iso27000.es [Consulta: 29 de septiembre de 2021]. Disponible en: https://www.iso27000.es/assets/files/ControlesISO27002-2013.pdf

Dominios	Objetivos	Controles
	8.2 Clasificación de la información	8.2.2 Etiquetado y manipulado de la información
		8.2.3 Manipulación de activos
	8.3 Manejo de los soportes de almacenamiento	8.3.1 Gestión de soportes extraíbles
		8.3.2 Eliminación de soportes
		8.3.3 Soportes físicos en transito
9. control de acceso	9.1 Requisitos de negocio para el control de accesos	9.1.1 Política de control de accesos
		9.1.2 Control de accesos a las redes y servicios asociados
	9.2 Gestión de acceso de usuario	9.2.1 Gestión de altas/bajas en el registro de usuarios
		9.2.2 Gestión de derechos de accesos asignados a usuarios
		9.2.3 Gestión de derechos de accesos con privilegios especiales
		9.2.4 Gestión de información confidencial de autenticación de usuarios
		9.2.5 Revisión de los derechos de acceso de los usuarios
		9.2.6 Retirada o adaptación de los derechos de acceso
	9.3 Responsabilidades del usuario	9.3.1 Uso de información confidencial para la autenticación
	9.4 Control de acceso a sistemas y aplicaciones	9.4.1 Restricción del acceso a la información
		9.4.2 Procedimientos seguros de inicio de sesión
		9.4.3 Gestión de contraseñas de usuario
		9.4.4 Uso de herramientas de administración de sistemas
		9.4.5 Control de acceso al código fuerte de los programas
10. cifrado	10.1 Controles Criptográficos	10.1.1 Políticas de uso de los controles criptográficos
		10.1.2 Gestión de claves
11. seguridad física y ambiental	11.1 Áreas seguras	11.1.1 Perímetro de seguridad física
		11.1.2 Controles físicos de entrada
		11.1.3 Seguridad de oficinas, despachos y recursos
		11.1.4 Protección contra las amenazas externas y ambientales
		11.1.5 El trabajo en áreas seguras

Dominios	Objetivos	Controles
		11.1.6 Áreas de acceso público, carga y descarga
	11.2 Seguridad de los Equipos	11.2.1 Emplazamiento y protección de equipos
		11.2.2 Instalación de suministro
		11.2.3 Seguridad del cableado
		11.2.4 Mantenimiento de los equipos
		11.2.5 Salida de activos fuera de las dependencias de la empresa
		11.2.6 Seguridad de los equipos y activos fuera de las instalaciones
		11.2.7 Reutilización o retirada segura de dispositivos de almacenamiento
		11.2.8 Equipo informático de usuario desatendido
		11.2.9 Política de puesto de trabajo despejado y bloqueo de pantalla
12. Seguridad en la operatividad	12.1 Responsabilidades y procedimientos de operación	12.1.1 Documentación de procedimientos de operación
		12.1.2 Gestión de cambios
		12.1.3 Gestión de capacidades
		12.1.4 Separación de entornos de desarrollo prueba y producción
	12.2 Protección contra código malicioso	12.2.1 Controles contra código malicioso
	12.3 Copias de seguridad	12.3.1 Copias de seguridad de la información
	12.4 Registro de actividad y supervisión	12.4.1 Registro y gestión de eventos de actividad
		12.4.2 Protección de los registros de información
		12.4.3 Registros de actividad del administrador y operador del sistema
		12.4.4 Sincronización de relojes
	12.5 Control del software en explotación	12.5.1 instalación de software en sistemas en producción
	12.6 Gestión de la vulnerabilidad técnica	12.6.1 Gestión de las vulnerabilidades técnicas
		12.6.2 Restricciones en la instalación de software
	12.7 Consideraciones de las auditorias de los sistemas de información	12.7.1 Controles de auditorías de los sistemas de información
13. Seguridad en las telecomunicaciones	13.1 Gestión de la seguridad en las redes	13.1.1 Controles de red
		13.1.2 Mecanismos de seguridad asociada a servicios en red

Dominios	Objetivos	Controles
		13.1.3 Segregación de redes
	13.2 Intercambio de información con partes externas	13.2.1 Políticas y procedimientos de intercambio de información
		13.2.2 Acuerdos de intercambio
		13.2.3 Mensajería electrónica
		13.2.4 Acuerdos de confidencialidad y secreto
14. Adquisición, desarrollo y mantenimiento de los sistemas de información	14.1 Requisitos de seguridad de los sistemas de información	14.1.1 Análisis y especificación de los requisitos de seguridad
		14.1.2 Seguridad en las comunicaciones en servicios accesibles por redes públicas
		14.1.3 Protección de las transacciones por redes telemáticas
	14.2 Seguridad en los procesos de desarrollo y soporte	14.2.1 Políticas de desarrollo seguro de software
		14.2.2 Procedimientos de control de cambios en los sistemas
		14.2.3 Revisión técnica de las aplicaciones tras efectuar cambios en el sistema operativo
		14.2.4 Restricciones a los cambios en los paquetes de software
		14.2.5 Uso de principios de ingeniería en protección de sistemas
		14.2.6 Seguridad en entornos de desarrollo
		14.2.7 Externalización del desarrollo de software
		14.2.8 Pruebas de funcionalidad durante el desarrollo de los sistemas
		14.2.9 Pruebas de aceptación
	14.3 Datos de prueba	14.3.1 Protección de los datos utilizados en pruebas
15. Relaciones con suministradores	15.1 Seguridad de la información en las relaciones con suministradores	15.1.1 Política de seguridad de la información para suministradores
		15.1.2 Tratamiento del riesgo dentro de acuerdos de suministradores
		15.1.3 Cadena de suministro en tecnologías de la información y comunicaciones
	15.2 Gestión de la prestación del servicio por suministradores	15.2.1 Supervisión de los servicios prestados por terceros
		15.2.2 Gestión de cambio en los servicios prestados por terceros

Dominios	Objetivos	Controles
16. Gestión de incidentes en la seguridad de la información	16.1 Gestión de incidentes de seguridad de la información y mejoras	16.1.1 Responsabilidades y procedimientos
		16.1.2 Notificación de los eventos de seguridad de la información
		16.1.3 Notificación de puntos débiles de la seguridad
		16.1.4 Valoración de eventos de seguridad de la información y toma de decisiones
		16.1.5 Respuesta a los incidentes de seguridad
		16.1.6 Aprendizaje de los incidentes de seguridad
		16.1.7 Recopilación de evidencias
17. Aspectos de seguridad de la información en la gestión de la continuidad del negocio	17.1 Continuidad de la información	17.1.1 Planificación de la continuidad de la seguridad de la información
		17.1.2 Implantación de la continuidad de la seguridad de la información
		17.1.3 Verificación, revisión y evaluación de la continuidad de la seguridad de la información
	17.2 Redundancias	17.2.1 Disponibilidad de instalaciones para el procesamiento de la información
18. Cumplimiento	18.1 Cumplimiento de los requisitos legales y contractuales	18.1.1 Identificación de la legislación aplicable
		18.1.2 Derechos de propiedad intelectual (DPI)
		18.1.3 Protección de requisitos de la organización
		18.1.4 Protección de datos y privacidad de la información personal
		18.1.5 Regulación de controles criptográficos
	18.2 revisiones de seguridad de la información	18.2.1 Revisión independiente de la seguridad de la información
		18.2.2 Cumplimiento de las políticas y normas de seguridad
		18.2.3 Comprobación del cumplimiento

Fuente. ISO.es. Controles ISO 27002-2013. [Sitio Web] https://www.iso27000.es [Consulta 29 de septiembre de 2021]. Disponible en: https://www.iso27000.es/assets/files/ControlesISO27002-2013.pd

De esta manera, tomando como línea base lo citado en la norma ISO/IEC 27001:2013 y una vez realizado el proceso de inspección documental, ocular al sistema de información y verificación de las áreas de trabajo, a continuación, se proponen la aplicación de una serie de controles, que permitirán mejorar de manera significativa el nivel de seguridad de la entidad.

No obstante, es de aclarar, que la Administración Municipal viene desarrollando actividades constantes en pro de mejorar su nivel de seguridad, puesto que se encuentra Certificada por en el Norma ISO 9001 “Sistema de Gestión de Calidad“ la cual los forja a brindar un servicio de alta calidad, garantizando la disponibilidad, confidencialidad e integridad de la información, tanto del cliente interno como externo.

De esta manera los controles que se plantean son los siguientes:

Tabla 26. Controles Identificados

Dominio	Control		Descripción	Justificación
A6 Administración Municipal de la seguridad de la información	A6.1 Administración Municipal Interna	A6.1.1 Roles y responsabilidades para la seguridad de la información.	Control: Se deben definir y asignar todas las responsabilidades de la seguridad de la información.	En la Administración Municipal es necesario implementarlo para controlar la implementación y operación de la seguridad informática teniendo en cuenta los roles y responsabilidades con las que cuenta cada aspecto de la seguridad de la información, pese a que se cuenta con un Manual de Funciones, no es aplicado en su totalidad.
		A6.1.2 Separación de deberes	Control: Los deberes y áreas de responsabilidad en conflicto se deben separar para reducir las posibilidades de modificación no autorizada o no intencional, o el uso indebido de los activos de la Administración Municipal	
A8 Gestión de activos	A8.2 Clasificación de la información	A8.2.3 Manejo de activos	Control: Se deben desarrollar e implementar procedimientos para el manejo de activos, de acuerdo con el esquema de clasificación de información adoptado por la Administración Municipal	Este permitirá a la Administración Municipal contar con información completa certeza frente al nivel que de seguridad que recibe cada uno de los activos de la Administración Municipal y si estos niveles son pertinentes.
A9. Control de acceso	A9.1 Requisitos de negocio para el control de accesos	A9.1.1 Política de control de acceso	Control: Se debe establecer, documentar y revisar una política	El manejo y control de acceso es de vital importancia

Dominio	Control		Descripción	Justificación
			de control de acceso con base en los requisitos del negocio y de la seguridad de la información.	para la protección de la información. Logrando tener en cuenta con convicción
		A9.1.2 Acceso a redes y a servicios de red	Control: Solo se debe permitir acceso de los usuarios a la red y a los servicios de red para los que hayan sido autorizados específicamente.	quienes acceden a la información y si realmente requieren de tener acceso a dicha información.
	A9.2 Gestión de acceso de usuario	A9.2.2 Suministro de acceso de usuarios	Control: Se debe implementar un proceso de suministro de acceso formal de usuarios para asignar o revocar los derechos de acceso para todo tipo de usuarios para todos los sistemas y servicios	Este es un parámetro que se tiene desatendido en la Administración Municipal en el acceso de la red y falta de segmentación, motivo por el cual se requiere de estos controles relacionados.
		A9.2.4 Gestión de la autenticidad secreta de usuarios.	Control: La asignación de información de autenticación secreta se debe controlar por medio de un proceso de gestión formal.	
		A9.2.5 Revisión de los derechos de acceso de los usuarios	Control: Los propietarios de los activos deben revisar los derechos de acceso de los usuarios, a intervalos regulares.	
	A9.4 Control de	A9.4.3 Sistema	Control: Los	

Dominio	Control		Descripción	Justificación
	acceso a sistemas y aplicaciones	de gestión de contraseñas	sistemas de gestión de contraseñas deben ser interactivos y deben asegurar la calidad de las contraseñas.	
A11. Seguridad física y del entorno	A11.1 Áreas seguras	A11.1.1 Perímetro de seguridad física	Control: Se deben definir y usar perímetros de seguridad, y usarlos para proteger áreas que contengan información confidencial o critica, e instalaciones de manejo de información	Según lo evidenciado en el caso no se identifican controles suficientes destinados a la seguridad física en la Administración Municipal, por lo cual se requiere la implementación de controles de seguridad física y del entorno logrando prevenir el acceso físico no autorizado, daños, interferencias sobre la información en la Administración Municipal.
		A11.1.2 Controles de acceso físicos.	Control: Las áreas seguras deben estar protegidas con controles de acceso apropiados para asegurar que sólo se permite el acceso a personal autorizado.	
		A11.1.4 Protección contra amenazas externas y ambientales.	Control: Se deben diseñar y aplicar protección física contra desastres naturales, ataques maliciosos o accidentes.	
		A11.1.6 Áreas de carga, despacho y acceso público.	Control: Se deben controlar los puntos de acceso tales como las áreas de despacho y carga y otros puntos por donde pueden	

Dominio	Control		Descripción	Justificación
			entrar personas no autorizadas y, si es posible, aislarlos de las instalaciones de procesamiento de información para evitar el acceso no autorizado.	
	A11.2 Seguridad de los equipos	A11.2.1 Ubicación y la protección de los equipos	Control: Los equipos deben de estar ubicados y protegidos para reducir los riesgos de amenazas y peligros del entorno, y las posibilidades de acceso no autorizado.	
		A11.2.2 Los servicios de suministro.	Control: Los equipos se deben proteger contra fallas de energía y otras interrupciones causadas por fallas en los servicios de suministro.	
A12. Seguridad de las operaciones	A12.1 Responsabilidades y procedimientos de operación	A12.1.4 Separación de los ambientes de desarrollo, pruebas y operación.	Control: Se deben separar los ambientes de desarrollo, pruebas y operación, para reducir los riesgos de acceso o cambios no autorizados al ambiente de operación.	Estos controles son necesarios para minimizar los riesgos existentes referentes a la ausencia de separación del área de desarrollo con respecto a los de operación. Es

Dominio	Control		Descripción	Justificación
		A12.6.1 Gestión de las vulnerabilidades técnicas	Control: Se debe obtener oportunamente información acerca de las vulnerabilidades técnicas de los sistemas de información que se usen; evaluar la exposición de la Administración Municipal a estas vulnerabilidades, y tomar las medidas apropiadas para tratar el riesgo asociado.	necesario que la seguridad este firmemente establecida, así como la distribución de sus áreas
A13. Seguridad de las comunicaciones	A13.1 Gestión de la seguridad en las redes.	A13.1.2 Seguridad de los servicios	Control: Se deben identificar los mecanismos de seguridad, los niveles de servicio y los requisitos de gestión de todos los servicios de red, e incluirlos en los acuerdos de servicio de red, ya sea que los servicios se presten internamente o se contraten externamente	Se evidencia la ausencia de segmentación de la red, motivo por el cual se identifican los riesgos relacionados a la exposición de los equipos y servidores frente a un tipo de vulneración u ataque, motivo por el cual se requiere de la implementación de estos controles que a su vez cuenten con instalaciones de procesamiento de la información de soporte.
		A.13.1.3 Separación en las redes	Control: Los grupos de servicios de información, usuarios y sistemas de información se deben separar en las redes	
A14. Adquisición, desarrollo y el	A14.1 Requisitos de seguridad de los sistemas de	A14.1.1 Análisis y especificaciones	Control: Los requisitos relacionados con	Es necesario asegurar la seguridad de la

Dominio	Control		Descripción	Justificación
mantenimiento de sistemas	información	de requisitos de seguridad de la información	seguridad de la información se deben incluir en los requisitos para nuevos sistemas de información o para mejoras a los sistemas de información existentes.	información donde se cuente con la integridad de sus sistemas de información, requisitos para sistemas de información y desarrollo de los sistemas de información.
	A14.2 Seguridad en los procesos de desarrollo y soporte	A14.2.7 Desarrollo contratado externamente	Control: La Administración Municipal debe supervisar y hacer seguimiento de la actividad de desarrollo de sistemas contratados externamente.	Esto se encuentra relacionado con el sistema de registro y control que emplea la Administración Municipal debido a la ausencia de pruebas de sus seguridad y evidentes vulnerabilidades relacionadas.
		A14.2.8 Pruebas de seguridad	Control: Durante el desarrollo se deben llevar a cabo pruebas de funcionalidad de la seguridad.	
A16. Gestión de incidentes de seguridad de la información	A16.1 Gestión de incidentes de seguridad de la información y mejoras	A16.1.1 Responsabilidades y procedimientos	Control: Se deben establecer las responsabilidades y procedimientos de gestión para asegurar una respuesta rápida, eficaz y ordenada a los incidentes de seguridad de la información.	Se requiere contar con una disposición de responsabilidades y procedimientos estipulados para llevar a cabo en cuestiones de que se vea algún incidente, identificando los

Dominio	Control		Descripción	Justificación
		A16.1.6 Aprendizaje obtenido de los incidentes de seguridad de la información	Control: El conocimiento adquirido al analizar y resolver incidentes de seguridad de la información se debe usar para reducir la posibilidad o impacto de incidentes futuros.	pasados y posibles que se presenten dándole un tratamiento adecuado según la aplicación de estos controles.
A17. Aspectos de seguridad de la información en la gestión de la continuidad del negocio	A17.1 Continuidad de la información	A17.1.3 Verificación, revisión y evaluación de la continuidad de la seguridad de la información	Control: La Administración Municipal debe verificar a intervalos regulares los controles de continuidad de la seguridad de la información establecidos e implementados, con el fin de asegurar que son válidos y eficaces durante situaciones adversas.	Estos controles se encuentran relacionados para suplir la ausencia actual donde se plantearán los parámetros de alta disponibilidad o de respaldo como servidores alternos o medidas de respaldo en caso de que sean necesaria. Adicionalmente manteniendo la seguridad incluyendo las pruebas de eficiencia sobre los sistemas de seguridad.
	A17.2 Redundancias	A.17.2.1 Disponibilidad de instalaciones de procesamiento de información	Control: Las instalaciones de procesamientos de información se deben implementar con redundancia suficiente para cumplir los requisitos de disponibilidad.	
A18 Cumplimiento	A18.1 Cumplimiento de los requisitos legales y contractuales	A18.1.1 identificación de la legislación que es aplicable	Control: Todos los requisitos estatutarios, reglamentarios y contractuales pertinentes y el	Esto es necesario la normatividad y aspectos legales arraigados a los documentos e

Dominio	Control	Descripción	Justificación
		enfoque de la Administración Municipal para cumplirlos, se deben identificar y documentar explícitamente y mantenerlos actualizados para cada sistema de información y para la Administración Municipal.	información de la Administración Municipal identificando protocolos y procesos a tener en cuenta para la información sensible de la Administración Municipal. Estos debido a que se pueden presentar errores o vulnerabilidades relacionadas con el óptimo funcionamiento e implicaciones legales al hacer uso o cuando la información se encuentra relacionada con métodos criptográficos.
	A18.1.2 Derechos de propiedad intelectual	Control: Se deben implementar procedimientos apropiados para asegurar el cumplimiento de los requisitos legislativos, de reglamentación y contractuales relacionados con los derechos de propiedad intelectual y el uso de productos de software patentados.	
	A18.1.4. Privacidad y protección de información de datos personales	Control: Se deben asegurar la privacidad y la protección de la información de datos personales, como se exige e la legislación y la reglamentación pertinentes, cuando sea aplicable	
	A18.1.5 Reglamentación de controles criptográficos.	Control: Se deben usar controles criptográficos, en cumplimiento de todos los	

Dominio	Control		Descripción	Justificación
			acuerdos, legislación y reglamentación pertinentes.	
	A18.2 Revisiones de la seguridad de la información.	A18.2.1 Revisión independiente de la seguridad de la información	Control: El enfoque de la Administración Municipal para la gestión de la seguridad de la información y su implementación (es decir los objetivos de control, los controles, las políticas, los procesos y los procedimientos para seguridad de la información), se deben revisar independientemente a intervalos planificados o cuando ocurran cambios significativos.	
		A18.2.2 Cumplimiento con las políticas y normas de seguridad.	Control: Los directores deben revisar con regularidad el cumplimiento del procesamiento y procedimientos de información dentro de su área de responsabilidad, con las políticas y normas de seguridad apropiadas, y cualquier otro requisito de seguridad.	

Dominio	Control	Descripción	Justificación
	A18.2.3 Revisión del cumplimiento técnico.	Control: Los sistemas de información se deben revisar periódicamente para determinar el cumplimiento con las políticas y normas de seguridad de la información	

Fuente. Autor

8 ELABORAR INFORME DE HALLAZGOS Y RECOMENDACIONES QUE PERMITA PRECISAR UN SISTEMA DE SEGURIDAD DE LA INFORMACIÓN CONCRETA A LA REALIDAD DE LA ALCALDÍA MUNICIPAL DE IBAGUÉ.

Con el fin de mostrar una información concreta de las amenazas y vulnerabilidades del Sistema de Gestión Documental del Palacio Municipal, a continuación, se detalla “GESTIÓN DE RIESGOS: ANÁLISIS DE RIESGOS".

Tabla 27. Informe Hallazgos

Activos de Información	**No. De Amenazas y**	**Nombre del activo de información**	**VALORACIÓN DEL RIESGO DE LOS**	**Amenazas Metodología Magerit**	**Vulnerabilidades**	**Probabilidad de vulneración** (1 **Calculo del riesgo neto**		**Criticidad neta** (1 a 4 despreciable **Calificación de Gestión** (1 control		**Si la opción es 2 - 3 o 4 Indique el Control aplicado actual**	**Riesgo residual** (riesgo neto **Criticidad residual** (1 a 4		**Niveles de aceptación del riesgo**
[D] DATOS	1	[D] - Datos Corresponde ncia Interna y Externa	9	[E1] Errores de los usuarios	Posible falta de conocimiento en el ingreso de la información en las bases de datos por parte de los funcionarios responsables.	3	27	C	1		27	C	I
[D] DATOS	2	[D] - Copias de Seguridad	19	[E2] Errores del administrador	Omisión de copias de seguridad en los PC de las diferentes dependencias.	4	76	C	1		76	C	I
[D] DATOS	3	[D] - Configuración de Equipos Propios del Palacio	9	[A11] Acceso no autorizado	No se implementaron o no se da uso adecuado de los controles de acceso a los Servidores de Bases de Datos.	2	18	I	1		18	I	I
[D] DATOS	4	[D] - Bases de Datos	19	[E1] Errores de los usuarios	Ausencia de actualización de los sistemas de base de datos y de parches de seguridad en los diferentes	5	95	C	1		95	C	I

Activos de Información	No. De Amenazas y	Nombre del activo de información	VALORACIÓN DEL RIESGO DE LOS	Amenazas Metodología Magerit	Vulnerabilidades	Probabilidad de vulneración (1 Calculo del riesgo neto		Criticidad neta (1 a 4 despreciable	Calificación de Gestión (1 control	Si la opción es 2 - 3 o 4 Indique el Control aplicado actual	Riesgo residual (riesgo neto	Criticidad residual (1 a 4	Niveles de aceptación del riesgo
					equipos de computo de las dependencias.								
[D] DATOS	5	[D] - Contraseñas	9	[E2] Errores del administrador	Se evidencia falta de validación de las contraseñas, no solicita la combinación de caracteres alfanuméricos en la contraseña	3	27	C	1		27	C	I
[D] DATOS	6	[D] - Datos de Control de Acceso.	9	[A15] Modificación deliberada de la información	No se cuenta con auditorias periódicas y monitoreo adecuado del estado de la información	3	27	C	1		27	C	I
[K] CLAVES CRIPTOGRÁFICAS	7	[K] - Protección de la Información Correos Institucionales	9	[E18] Destrucción de información	No se cuenta con los niveles de seguridad adecuados para la protección de la información financiera.	3	27	C	1		27	C	I
[K] CLAVES CRIPTOGRÁFICAS	8	[K] - Protección de las Comunicaciones - Voz IP	9	[E1] Errores de los usuarios	La eventual inexperiencia del personal de practica de otras dependencias, encargado de la alimentación de la información en el sistema, puede provocar en el ingreso erróneo de la información	5	45	C	1		45	C	I

Activos de Información	No. De Amenazas y	Nombre del activo de información	VALORACIÓN DEL RIESGO DE LOS	Amenazas Metodología Magerit	Vulnerabilidades	Probabilidad de vulneración (1	Calculo del riesgo neto	Criticidad neta (1 a 4 despreciable	Calificación de Gestión (1 control	Si la opción es 2 - 3 o 4 Indique el Control aplicado actual	Riesgo residual (riesgo neto	Criticidad residual (1 a 4	Niveles de aceptación del riesgo
[K] CLAVES CRIPTOGRÁFICAS	9	[K] - Protección de las Comunicaciones - Wifi	9	[E2] Errores del administrador	Presencia de exceso de privilegios y mala disposición de niveles de acceso para la información.	4	36	C	1		36	C	I
[S] SERVICIOS	10	[S] - Servicios de Impresión	9	[A11] Acceso no autorizado	Ausencia de Políticas de Control de Acceso correspondiente a los Servidores de Bases de Datos.	3	27	C	1		27	C	I
[S] SERVICIOS	11	[S] - Servicio Soporte Técnico	9	[A15] Modificación deliberada de la información	No se cuenta con auditorias periódicas y monitoreo adecuado del estado de las Bases de Datos.	4	36	C	1		36	C	I
[S] SERVICIOS	12	[S] - Servicios Pagina Web Institucional (1)	21	[E2] Errores del administrador	Configuración insuficiente de servidor. Configuración errónea de los parámetros de autenticación.	5	105	C	1		105	C	I
[S] SERVICIOS	13	[S] - Servicio Correo Electrónico - Google Sites (1)	15	[A11] Acceso no autorizado	Ineficiente sistema de autenticación y gestor de permisos y permisos.	5	75	C	1		75	C	I
[S] SERVICIOS	14	[S] - Transferencia de Archivos	17	[A24] Denegación de servicio	Vulnerabilidad presentada en los servidores de Godaddy, frente a un control	5	85	C	1		85	C	I

Activos de Información	No. De Amenazas y	Nombre del activo de información	VALORACIÓN DEL RIESGO DE LOS	Amenazas Metodología Magerit	Vulnerabilidades	Probabilidad de vulneración (1	Calculo del riesgo neto	Criticidad neta (1 a 4 despreciable	Calificación de Gestión (1 control	Si la opción es 2 - 3 o 4 Indique el Control aplicado actual	Riesgo residual (riesgo neto	Criticidad residual (1 a 4	Niveles de aceptación del riesgo
					inadecuado de un alto tráfico.								
[S] SERVICIOS	15	[S] - Gestión de usuarios y Contraseñas	18	[E2] Errores del administrador	Gestión y disposición errónea de las cuentas para los usuarios.	2	36	C	1		36	C	I
[SW] SOFTWARE	16	[SW] - Plataforma PISAMI (1)	18	[A5] Suplantación de la identidad del usuario	Ausencia de capacitación (Ingeniería Social), concientización y plan de seguridad para los usuarios; que permita un uso adecuado y seguro del servicio.	3	54	C	1		54	C	I
[SW] SOFTWARE	17	[SW] - PHP y Larabel (1)	18	[E1] Errores de los usuarios	Daños generados por uso inadecuado del servicio por falta de capacitación del uso adecuado de los herramientas tecnológicas.	3	54	C	1		54	C	I
[SW] SOFTWARE	18	[SW] - Apache (1)	19	[E2] Errores del administrador	Gestión de la configuración, disposición de accesos al servicio y gestión de capacitaciones para el uso adecuado del servicio	3	57	C	1		57	C	I

Activos de Información	No. De Amenazas y	Nombre del activo de información	VALORACIÓN DEL RIESGO DE LOS	Amenazas Metodología Magerit	Vulnerabilidades	Probabilidad de vulneración (1	Calculo del riesgo neto	Criticidad neta (1 a 4 despreciable	Calificación de Gestión (1 control	Si la opción es 2 - 3 o 4 Indique el Control aplicado actual	Riesgo residual (riesgo neto	Criticidad residual (1 a 4	Niveles de aceptación del riesgo
[SW] SOFTWARE	19	[SW] - Windows 2016 Server Linux Centos 7	17	[E21] Errores de mantenimiento / actualización de programas (software)	No se realizan las actualizaciones correspondientes y actuales al sistema. No se realiza un eficiente mantenimiento al sistema.	5	85	C	1		85	C	I
[SW] SOFTWARE	20	[SW] - Joomla V.2.5	17	[E23] Errores de mantenimiento / actualización de equipos (hardware)	Instalación ineficiente, deficiente mantenimiento de los equipos.	4	68	C	1		68	C	I
[SW] SOFTWARE	21	[SW] - Bases de Datos MySQL (1)	18	[E2] Errores del administrador	Configuración inadecuada o errada del protocolo.	3	54	C	1		54	C	I
[SW] SOFTWARE	22	[SW] - Oracle 10G (1)	18	[E24] Caída del sistema por agotamiento de recursos	No se cuentan con los recursos suficientes para cubrir con lo requerido por la organización	2	36	C	1		36	C	I
[SW] SOFTWARE	23	[SW] - Avira	19	[A24] Denegación de servicio	Ineficientes medidas de seguridad implementadas; ausencia en la configuración UTM para la detección de Intrusiones, zona desmilitarizada para la	3	57	C	1		57	C	I

Activos de Información	No. De Amenazas y	Nombre del activo de información	VALORACIÓN DEL RIESGO DE LOS	Amenazas Metodología Magerit	Vulnerabilidades	Probabilidad de vulneración (1 Calculo del riesgo neto		Criticidad neta (1 a 4 despreciable	Calificación de Gestión (1 control	Si la opción es 2 - 3 o 4 Indique el Control aplicado actual	Riesgo residual (riesgo neto	Criticidad residual (1 a 4	Niveles de aceptación del riesgo
					protección de los servidores.								
[SW] SOFTWARE	24	[SW] - Windows 10 Pro	17	[E2] Errores del administrador	Incorrecta configuración de usuarios y contraseñas. Uso de contraseñas genéricas.	3	51	C	3	El Departamento de Sistemas - de sistema brinda: Apoyo al Registro y Control Académico	17	I	I
[HW] EQUIPAMIENTO INFORMÁTICO	25	[HW] - Servidor de Archivos FTP - Marca: DELL en Torre PowerEdge T130 (1)	17	[E24] Caída del sistema por agotamiento de recursos	No se cuentan disponibilidad suficiente, recursos físico, humano necesario para cubrir con los casos de soporte requeridos por los usuarios organización	2	34	C	1		34	C	I
[HW] EQUIPAMIENTO INFORMÁTICO	26	[HW] - Servidor DHCP - Marca: Dell en Torre PowerEdge T440 (1)	17	[A24] Denegación de servicio	Ausencia de configuración de privilegios de aceptación o denegación de conectividad firwall, Ineficiente medidas de seguridad.	3	51	C	1		51	C	I

Activos de Información	No. De Amenazas y	Nombre del activo de información	VALORACIÓN DEL RIESGO DE LOS	Amenazas Metodología Magerit	Vulnerabilidades	Probabilidad de vulneración (1 Calculo del riesgo neto		Criticidad neta (1 a 4 despreciable	Calificación de Gestión (1 control	Si la opción es 2 - 3 o 4 Indique el Control aplicado actual	Riesgo residual (riesgo neto	Criticidad residual (1 a 4	Niveles de aceptación del riesgo
[HW] EQUIPAMIENTO INFORMÁTICO	27	[HW] - Servidor DHCP - Marca: Dell en Torre PowerEdge T440 (1)	17	[E1] Errores de los usuarios	Uso inadecuado. Ausencia de conocimiento sobre la operabilidad y uso del sistema operativo.	5	85	C	4	El Departamento de Sistemas - Área de Soporte es la encargada velar por el optimo funcionamiento del equipo tecnológico en cuanto el Sistema Operativo	21	C	I
[HW] EQUIPAMIENTO INFORMÁTICO	28	[HW] - Equipos de Computo (1)	15	[E20] Vulnerabilidades de los programas (software)	Fallos o vulnerabilidades presentes en la seguridad del sistema. Ausencia de plan de seguridad.	5	75	C	4	El Departamento de Sistemas - Área de Soporte es la encargada velar por el optimo funcionamiento del equipo tecnológico en cuanto el Sistema Operativo	19	I	I
[HW] EQUIPAMIENTO INFORMÁTICO	29	[HW] - Equipos de Computo (6)	12	[E21] Errores de mantenimiento / actualizació	No se realizan las actualizaciones correspondientes y actuales al	5	60	C	1		60	C	I

Activos de Información	No. De Amenazas y	Nombre del activo de información	VALORACIÓN DEL RIESGO DE LOS	Amenazas Metodología Magerit	Vulnerabilidades	Probabilidad de vulneración (1	Calculo del riesgo neto	Criticidad neta (1 a 4 despreciable	Calificación de Gestión (1 control	Si la opción es 2 - 3 o 4 Indique el Control aplicado actual	Riesgo residual (riesgo neto	Criticidad residual (1 a 4	Niveles de aceptación del riesgo
				n de programas (software)	sistema. No se realiza un eficiente mantenimiento al sistema.								
[HW] EQUIPAMIENTO INFORMÁTICO	30	[HW] - Equipos de Computo (2)	12	[A8] Difusión de software dañino	Fallos en la configuración de seguridad del sistema operativo, ausencia de antivirus actualizado	5	60	C	2	La organización cuenta con un Sistema de Antivirus, pero presenta deficiencia en el seguimiento a sus actualizaciones o estado.	30	C	I
[HW] EQUIPAMIENTO INFORMÁTICO	31	[HW] - Equipos de Computo (1)	15	[E20] Vulnerabilidades de los programas (software)	Fallos o vulnerabilidades presentes en la seguridad del sistema. Ausencia de plan de seguridad.	5	75	C	1		75	C	I
[HW] EQUIPAMIENTO INFORMÁTICO	32	[HW] - Equipos de Computo (8)	12	[E21] Errores de mantenimiento / actualización de programas (software)	Ausencia en el control de actualizaciones del sistema de seguridad e implantación de parches. No se realiza un eficiente mantenimiento al sistema.	5	60	C	1		60	C	I

Activos de Información	No. De Amenazas y	Nombre del activo de información	VALORACIÓN DEL RIESGO DE LOS	Amenazas Metodología Magerit	Vulnerabilidades	Probabilidad de vulneración (1	Calculo del riesgo neto	Criticidad neta (1 a 4 despreciable	Calificación de Gestión (1 control	Si la opción es 2 - 3 o 4 Indique el Control aplicado actual	Riesgo residual (riesgo neto	Criticidad residual (1 a 4	Niveles de aceptación del riesgo
[HW] EQUIPAMIENTO INFORMÁTICO	33	[HW] - Grupo de Talento Humano (7)	12	[E2] Errores del administrador	Configuraciones erradas que generan deficiencias en el funcionamiento adecuado del software.	3	36	C	3	El Departamento de Sistemas - Área de Desarrollo, es la encargada de velar por el óptimo funcionamiento de los servicios tecnológicos en cuanto aplicativos.	12	A	M
[HW] EQUIPAMIENTO INFORMÁTICO	34	[HW] - Impresora Marca: HP LASERJET M1212NF (1)	8	[E20] Vulnerabilidades de los programas (software)	Fallos o vulnerabilidades presentes en la seguridad del sistema. Ausencia de plan de seguridad.	5	40	C	2	El Departamento de Sistemas - Área de Desarrollo, es la encargada de velar por el óptimo funcionamiento de los servicios tecnológicos en cuanto aplicativos.	20	I	I
[HW] EQUIPAMIENTO INFORMÁTICO	35	[HW] - Impresora Marca: HP LASERJET ENTERPRISE M608 (1)	8	[E21] Errores de mantenimiento / actualización de	Ausencia en el control de actualizaciones del sistema de seguridad e implantación de parches. No se	5	40	C	2	El Departamento de Sistemas - Área de Desarrollo, es la	20	I	I

Activos de Información	No. De Amenazas y	Nombre del activo de información	VALORACIÓN DEL RIESGO DE LOS	Amenazas Metodología Magerit	Vulnerabilidades	Probabilidad de vulneración (1	Calculo del riesgo neto	Criticidad neta (1 a 4 despreciable	Calificación de Gestión (1 control	Si la opción es 2 - 3 o 4 Indique el Control aplicado actual	Riesgo residual (riesgo neto	Criticidad residual (1 a 4	Niveles de aceptación del riesgo
				programas (software)	realiza un eficiente mantenimiento al sistema.					encargada de velar por el óptimo funcionamiento de los servicios tecnológicos en cuanto aplicativos.			
[HW] EQUIPAMIENTO INFORMÁTICO	36	[HW] - Impresora Marca: HP LASERJET PRO MFP M426FDW (1)	8	[E2] Errores del administrador	Configuraciones erradas que generan deficiencias en el funcionamiento adecuado del software.	3	24	C	3	El Departamento de Sistemas - Área de Desarrollo, es la encargada de velar por el óptimo funcionamiento de los servicios tecnológicos en cuanto aplicativos.	8	B	M
[HW] EQUIPAMIENTO INFORMÁTICO	37	[HW] - Impresora Marca: HP LASERJET P4515x (1)	8	[E20] Vulnerabilidades de los programas (software)	Fallos o vulnerabilidades presentes en la seguridad del sistema. Ausencia de plan de seguridad.	5	40	C	2	El Departamento de Sistemas - Área de Desarrollo, es la encargada de velar por el óptimo funcionamiento de los servicios tecnológico	20	I	I

Activos de Información	No. De Amenazas y	Nombre del activo de información	VALORACIÓN DEL RIESGO DE LOS	Amenazas Metodología Magerit	Vulnerabilidades	Probabilidad de vulneración (1 Calculo del riesgo neto		Criticidad neta (1 a 4 despreciable	Calificación de Gestión (1 control	Si la opción es 2 - 3 o 4 Indique el Control aplicado actual	Riesgo residual (riesgo neto	Criticidad residual (1 a 4	Niveles de aceptación del riesgo
										s en cuanto aplicativos.			
[HW] EQUIPAMIENTO INFORMÁTICO	38	[HW] - Impresora Marca: LASERJET 600 M603 (1)	8	[E21] Errores de mantenimiento / actualización de programas (software)	Ausencia en el control de actualizaciones del sistema de seguridad e implantación de parches. No se realiza un eficiente mantenimiento al sistema.	5	40	C	2	El Departamento de Sistemas - Área de Desarrollo, es la encargada de velar por el óptimo funcionamiento de los servicios tecnológicos en cuanto aplicativos.	20	I	I
[HW] EQUIPAMIENTO INFORMÁTICO	39	[HW] - Impresora Marca: HP OFFICEJET PRO 8600 (1)	8	[E2] Errores del administrador	Configuraciones erradas que generan deficiencias en el funcionamiento adecuado del software.	3	24	C	3	El Departamento de Sistemas - Área de Desarrollo, es la encargada de velar por el óptimo funcionamiento de los servicios tecnológicos en cuanto aplicativos.	8	B	M

Activos de Información	No. De Amenazas y	Nombre del activo de información	VALORACIÓN DEL RIESGO DE LOS	Amenazas Metodología Magerit	Vulnerabilidades	Probabilidad de vulneración (1 Calculo del riesgo neto		Criticidad neta (1 a 4 despreciable	Calificación de Gestión (1 control	Si la opción es 2 - 3 o 4 Indique el Control aplicado actual	Riesgo residual (riesgo neto	Criticidad residual (1 a 4	Niveles de aceptación del riesgo
[HW] EQUIPAMIENTO INFORMÁTICO	40	[HW] - Impresora Marca: HP LASERJET M1522N (1)	8	[E21] Errores de mantenimiento / actualización de programas (software)	Ausencia en el control de actualizaciones del sistema de seguridad e implantación de parches. No se realiza un eficiente mantenimiento al sistema.	5	40	C	2	El Departamento de Sistemas - Área de Desarrollo, es la encargada de velar por el óptimo funcionamiento de los servicios tecnológicos en cuanto aplicativos.	20	I	I
[HW] EQUIPAMIENTO INFORMÁTICO	41	[HW] - Impresora Marca: KYOCERA FS-1035MFP (1)	15	[A12] Análisis de tráfico	Ausencia en la configuración adecuada de permisos para la aceptación o denegación de conexiones.	5	75	C	2	El Departamento de Sistemas - Área de Desarrollo, es la encargada de velar por el óptimo funcionamiento de los servicios tecnológicos en cuanto aplicativos.	38	C	I
[HW] EQUIPAMIENTO INFORMÁTICO	42	[HW] - Puntos de Acceso Alámbricos	17	[E20] Vulnerabilidades de los programas (software)	Fallos o vulnerabilidades presentes en la seguridad del sistema. Ausencia de plan de seguridad.	5	85	C	2	El Departamento de Sistemas - Área de Desarrollo, es la	43	C	I

Activos de Información	No. De Amenazas y	Nombre del activo de información	VALORACIÓN DEL RIESGO DE LOS	Amenazas Metodología Magerit	Vulnerabilidades	Probabilidad de vulneración (1 Calculo del riesgo neto		Criticidad neta (1 a 4 despreciable Calificación de Gestión (1 control		Si la opción es 2 - 3 o 4 Indique el Control aplicado actual	Riesgo residual (riesgo neto Criticidad residual (1 a 4 Niveles de aceptación del riesgo		
										encargada de velar por el óptimo funcionamiento de los servicios tecnológicos en cuanto aplicativos.			
[HW] EQUIPAMIENTO INFORMÁTICO	43	[HW] - Switches: Marca ArubaOS-Switch, ARUBA 2530 24G (6)	16	[E21] Errores de mantenimiento / actualización de programas (software)	Ausencia en el control de actualizaciones del sistema de seguridad e implantación de parches. No se realiza un eficiente mantenimiento al sistema.	5	80	C	2	El Departamento de Sistemas - Área de Desarrollo, es la encargada de velar por el óptimo funcionamiento de los servicios tecnológicos en cuanto aplicativos.	40	C	I
[HW] EQUIPAMIENTO INFORMÁTICO	44	[HW] - Cortafuegos Cisco ASA 5505 (1)	17	[E2] Errores del administrador	Configuraciones erradas que generan deficiencias en el funcionamiento adecuado del software.	3	51	C	3	El Departamento de Sistemas - Área de Desarrollo, es la encargada de velar por el óptimo funcionamiento de los servicios tecnológico	17	I	I

Activos de Información	No. De Amenazas y	Nombre del activo de información	VALORACIÓN DEL RIESGO DE LOS	Amenazas Metodología Magerit	Vulnerabilidades	Probabilidad de vulneración (1 Calculo del riesgo neto	Criticidad neta (1 a 4 despreciable	Calificación de Gestión (1 control	Si la opción es 2 - 3 o 4 Indique el Control aplicado actual	Riesgo residual (riesgo neto	Criticidad residual (1 a 4	Niveles de aceptación del riesgo
									s en cuanto aplicativos.			
[HW] EQUIPAMIENTO INFORMÁTICO	45	[HW] - Puntos de Acceso (2)	17	[E20] Vulnerabilidades de los programas (software)	Fallos o vulnerabilidades presentes en la seguridad del sistema. Ausencia de plan de seguridad.	5	85	C	2	El Departamento de Sistemas - Área de Desarrollo, es la encargada de velar por el óptimo funcionamiento de los servicios tecnológicos en cuanto aplicativos.	43	C	I
[HW] EQUIPAMIENTO INFORMÁTICO	46	[HW] - Teléfono IP (6)	17	[E21] Errores de mantenimiento / actualización de programas (software)	Ausencia en el control de actualizaciones del sistema de seguridad e implantación de parches. No se realiza un eficiente mantenimiento al sistema.	5	85	C	2	El Departamento de Sistemas - Área de Desarrollo, es la encargada de velar por el óptimo funcionamiento de los servicios tecnológicos en cuanto aplicativos.	43	C	I

Activos de Información	No. De Amenazas y	Nombre del activo de información	VALORACIÓN DEL RIESGO DE LOS	Amenazas Metodología Magerit	Vulnerabilidades	Probabilidad de vulneración (1 Calculo del riesgo neto		Criticidad neta (1 a 4 despreciable Calificación de Gestión (1 control		Si la opción es 2 - 3 o 4 Indique el Control aplicado actual	Riesgo residual (riesgo neto Criticidad residual (1 a 4		Niveles de aceptación del riesgo
[COM] REDES DE COMUNICACIONES	47	[COM] - Sistema Comunicación Voz IP	8	[E2] Errores del administrador	Configuraciones erradas que generan deficiencias en el funcionamiento adecuado del software.	3	24	C	3	El Departamento de Sistemas - Área de Desarrollo, es la encargada de velar por el óptimo funcionamiento de los servicios tecnológicos en cuanto aplicativos.	8	B	M
[COM] REDES DE COMUNICACIONES	48	[COM] - Red Inalámbrica - Institucional	17	[A14] Interceptación de información (escucha)	Ausencia de sistema de Seguridad adecuado	3	51	C	3		17	I	I
[COM] REDES DE COMUNICACIONES	49	[COM] - Red Local Institucional	17	[E24] Caída del sistema por agotamiento de recursos	Ausencia de encapsulamiento de protocoles.	4	68	C	4		17	I	I
[COM] REDES DE COMUNICACIONES	50	[COM] - Internet Palacio	15	[I8] Fallo de servicios de comunicaciones	Fallas relacionadas con el internet, intermitencia, por daños en la infraestructura o inutilidad del mismo.	5	75	C	1		75	C	I
[Media] SOPORTE DE INFORMACIÓN	51	[Media] - Cloud Plus	17	[E2] Errores del administrador	Intermitencia del servicio por fallas.	3	51	C	1		51	C	I

Activos de Información	No. De Amenazas y	Nombre del activo de información	VALORACIÓN DEL RIESGO DE LOS	Amenazas Metodología Magerit	Vulnerabilidades	Probabilidad de vulneración (1	Calculo del riesgo neto	Criticidad neta (1 a 4 despreciable	Calificación de Gestión (1 control	Si la opción es 2 - 3 o 4 Indique el Control aplicado actual	Riesgo residual (riesgo neto	Criticidad residual (1 a 4	Niveles de aceptación del riesgo
[AUX] EQUIPAMIENTO AUXILIAR	52	[AUX] - UPS del Palacio	16	[E23] Errores de mantenimiento / actualización de equipos (hardware)	Falta de conocimiento en la manipulación de los dispositivos	3	48	C	7		7	B	M
[AUX] EQUIPAMIENTO AUXILIAR	53	[AUX] - Cableado Eléctrico	17	[E24] Caída del sistema por agotamiento de recursos	Deterioro total o parcial del cableado incluido equipos conectados al mismo.	2	34	C	1		34	C	I
[AUX] EQUIPAMIENTO AUXILIAR	54	[AUX] - Cableado Estructurado	13	[E25] Pérdida de equipos	Daños por uso e instalación inadecuado.	3	39	C	1		39	C	I
[L] INSTALACIONES	55	[L] - Instalaciones Palacio	19	[A11] Acceso no autorizado	Falta de un Sistema Biométrico o de monitoreo para el acceso a las Instalaciones y dependencias de acceso restringido.	3	57	C	1		57	C	I
[L] INSTALACIONES	55	[L] - Instalaciones Palacio	19	[A26] Ataque destructivo	Ejecución de Huelgas y/o Paros Nacionales/Territoriales, presencia de actos terroristas.	1	19	I	1		19	I	I
[L] INSTALACIONES	55	[L] - Instalaciones Palacio	19	[N*] Desastres naturales	Se cuenta con Plan de Prevención y Atención de Desastres, así como un Plan de Resguardo o	1	19	I	1		19	I	I

Activos de Información	No. De Amenazas y	Nombre del activo de información	VALORACIÓN DEL RIESGO DE LOS	Amenazas Metodología Magerit	Vulnerabilidades	Probabilidad de vulneración (1 Calculo del riesgo neto		Criticidad neta (1 a 4 despreciable Calificación de Gestión (1 control		Si la opción es 2 - 3 o 4 Indique el Control aplicado actual	Riesgo residual (riesgo neto Criticidad residual (1 a 4 Niveles de aceptación del riesgo		
					Protección, pero es poco el personal capacitado.								
[P] PERSONAL	56	[P] - Funcionarios de Planta y Contratistas (75)	19	[A29] Extorsión	Susceptibilidad de los servidores públicos a ser obligados para ejecutar actos inicuos en contra la Administración Municipal.	3	57	C	1		57	C	I
[P] PERSONAL	56	[P] - Funcionarios de Planta y Contratistas (75)	19	[E19] Fugas de información	Deficiencia en el monitoreo sobre el uso adecuado de la información publicada en la Plataforma PISAMI y el control de acceso a los datos, carencia de LOGS de auditoria.	3	57	C	1		57	C	I
[P] PERSONAL	56	[P] - Funcionarios de Planta y Contratistas (75)	19	[E28] Indisponibilidad del personal	Ausencia del personal por incapacidades medicas a a causa del COVID 19, y deficiencia en los procesos contractuales para la contratación de nuevo personal.	3	57	C	1		57	C	I
[P] PERSONAL	57	[P] - Técnicos/Auxiliares de Mantenimiento (2)	19	[E28] Indisponibilidad del personal	Ausencia del personal por incapacidades medicas a a causa del COVID 19, y deficiencia	3	57	C	1		57	C	I

Activos de Información	No. De Amenazas y	Nombre del activo de información	VALORACIÓN DEL RIESGO DE LOS	Amenazas Metodología Magerit	Vulnerabilidades	Probabilidad de vulneración (1 Calculo del riesgo neto		Criticidad neta (1 a 4 despreciable Calificación de Gestión (1 control		Si la opción es 2 - 3 o 4 Indique el Control aplicado actual	Riesgo residual (riesgo neto Criticidad residual (1 a 4 Niveles de aceptación del riesgo		
					en los procesos contractuales para la contratación de nuevo personal.								
[P] PERSONAL	57	[P] - Técnicos/Auxiliares de Mantenimiento (2)	19	[A29] Extorsión	Susceptibilidad de los servidores públicos a ser obligados para ejecutar actos inicuos en contra la Administración Municipal.	3	57	C	1		57	C	I
[P] PERSONAL	58	[P] - Profesionales	12	[A29] Extorsión	Susceptibilidad de los servidores públicos a ser obligados para ejecutar actos inicuos en contra la Administración Municipal.	3	36	C	1		36	C	I
[P] PERSONAL	58	[P] - Profesionales	12	[E28] Indisponibilidad del personal	Ausencia del personal por incapacidades medicas a a causa del COVID 19, y deficiencia en los procesos contractuales para la contratación de nuevo personal.	3	36	C	1		36	C	I
[P] PERSONAL	59	[P] - Servicio Web: MEDIA COMMERCE PARTNERS (1)	12	[E30] Ingeniería Social	Suministro de información a terceros mediante amenazas.	3	36	C	4	Establecimiento de Cláusulas de Confidencialidad en el proceso Contractual.	9	B	M

Activos de Información	No. De Amenazas y	Nombre del activo de información	VALORACIÓN DEL RIESGO DE LOS	Amenazas Metodología Magerit	Vulnerabilidades	Probabilidad de vulneración (1	Calculo del riesgo neto	Criticidad neta (1 a 4 despreciable	Calificación de Gestión (1 control	Si la opción es 2 - 3 o 4 Indique el Control aplicado actual	Riesgo residual (riesgo neto	Criticidad residual (1 a 4	Niveles de aceptación del riesgo
[P] PERSONAL	60	[P] - Servicio Correo Institucional: ITO SOFTWARE SAS (1)	12	[A30] Extorsión	Entrega de información confidencial a terceros por presión mediante extorsión	2	24	C	4	Establecimiento de Cláusulas de Confidencialidad en el proceso Contractual.	6	B	M

Fuente. Autor

Así mismo se pudo establecer que la principal vulnerabilidad, radica en el personal en el desarrollo de sus funciones, toda vez que dependiendo del manejo que cada uno brinde a las herramientas utilizadas tanto de software como de hardware, así mismo será la funcionalidad del Sistema de Gestión Documental y el tratamiento de los datos que se le dará al mismo.

9 CONCLUSIONES

El implementar la metodología MARGERIT, basados en la Norma Internacional ISO 27001:2013, permite a la entidad contar con información acertada y precisa de las vulnerabilidades a las que esta propenso el Sistema de Gestión Documental, generando con ello mayor facilidad para la toma de decisiones y soluciones enfocadas en controles y políticas que conlleven a mejorar el nivel de seguridad de la Información.

Teniendo como resultado el análisis realizado con la metodología MARGERIT, se propuso mecanismos de control y gestión, establecidos en la Norma Internacional ISO 27001:2013, los cuales le permitirán a la Alcaldía de Ibagué, reducir las vulnerabilidades identificadas en su Sistema de Gestión Documental, propendiendo por la protección y tratamiento de los datos.

De acuerdo a los resultados obtenidos en la aplicación de la metodología MARGERIT, se puedo determinar que la Alcaldía Municipal de Ibagué, en su Sistema de Gestión Documental, cuenta con una serie de hallazgos los cuales se plasmaron en un informe ejecutivo el cual le permitirá contar con una información concreta del estado actual de sus Sistema de Seguridad.

10 RECOMENDACIONES

Diseñar e implementar en la Administración Municipal políticas de confidencialidad de la Información, tanto del Personal de Planta como de contrato y proveedores, quienes en el ejercicio de sus funciones tienen acceso a la información desde la plataforma PISAMI y demás sistemas de información.

Capacitar constante a los funcionarios de planta y Contrato sobre el uso del Sistema de Gestión Documental, herramientas tecnológicas y Sistema de Seguridad de la Información, ello con el fin de pormenorizar los riesgos a los que se ve expuesta la información por falta de conocimiento y/o desentendimiento del buen uso de los mismos; esto teniendo en cuenta que la perdida de información sensible de toda entidad, se efectúa inicialmente mediante el sistema de ataque al personal.

Instaurar política de contraseña segura, toda vez que actualmente el Sistema de Gestión Documental – Plataforma PISAMI, permite ingresar contraseñas sin previa validación de longitud, ingreso de caracteres alfanuméricos y repetición de contraseña, una vez caducada la anterior, generando con ello un nivel de seguridad bajo, sin controles adecuados que prevean o eviten algún riesgo en el Sistema de Información de la entidad.

Implementar la metodología MARGERIT en la entidad, para identificación, clasificación y valoración de los Activos, toda vez que dicha metodología cuenta con reglas específicas orientadas establecer los activos de mayor importancia, así mismo permite determinar las amenazas y vulnerabilidades del Sistema de Información, facilitando con ello un diseño de mecanismos de control y políticas de seguridad, asentados en la norma ISO 27001, con el propósito de mejorar y preservar el Sistema de Gestión de Seguridad de la Información de la entidad.

Realizar seguimiento y validación a los controles implementados por la Administración Municipal, con el fin de establecer la efectividad de los mismos y determinar si ha sido efectiva la disminución de los riesgos identificados. De esta manera es necesario aplicar el análisis correspondiente, mediante la aplicación de la metodología MARGERIT.

Aplicar los controles sugeridos en el presente documento, según lo establecido en la norma ISO 27001:2013, en su anexo de controles de seguridad del estándar ISO 27002, considerando los dominios establecidos para reducir la ocurrencia de los riesgos identificados, de esta manera es necesario a su vez actualizar las políticas de seguridad en las cuales se enmarque los nuevos controles que se determinen implementar.

BIBLIOGRAFÍA

ADMINISTRACIÓN ELECTRÓNICA [Sitio Web] MARGERIT v.3 Metodología de Análisis y Gestión de los Riesgos de los Sistemas de Información. [Consultado: 01 de mayo de 2021]. Disponible en:]https://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_Magerit.html

ALCALDÍA MUNICIPAL DE IBAGUÉ [Sitio Web]. Plataforma Integrada de Sistemas Alcaldía Municipal de Ibagué – PISAMI. [Consulta 01 de mayo de 2021]. Disponible en: https://pisami.ibague.gov.co/app/PISAMI/index.php?id_error=3

ALCALDÍA MUNICIPAL DE IBAGUÉ. [Sitio Web] Gestión de Infraestructura Tecnológica. Ibagué. [Consulta: 09 de septiembre de 2021]. Disponible en: https://ibague.gov.co/portal/seccion/contenido/index.php?type=3&cnt=7

ALCALDÍA MUNICIPAL DE IBAGUÉ. [Sitio Web]. Ibagué, Gestión de Infraestructura Tecnológica. [Consulta: 29 de septiembre de 2021]. Disponible en: https://ibague.gov.co/portal/admin/archivos/publicaciones/2020/25046-DOC-20200814093308.pdf

ALCALDÍA MUNICIPAL DE IBAGUÉ. [Sitio Web]. Ibagué, Plan de Continuidad. [Consulta: 29 de septiembre de 2021]. Disponible en: https://ibague.gov.co/portal/admin/archivos/publicaciones/2019/29357-DOC-20191223.pdf

ALCALDÍA MUNICIPAL DE IBAGUÉ. [Sitio Web]. Ibagué, Plan de Incidentes. [Consulta: 29 de septiembre de 2021]. Disponible en: https://ibague.gov.co/portal/admin/archivos/publicaciones/2019/29356-DOC-20191222.pdf

ALCALDÍA MUNICIPAL DE IBAGUÉ. [Sitio Web]. Ibagué, Plan de Sensibilización Capacitación y Comunicación. [Consulta: 29 de septiembre de 2021]. Disponible en: https://ibague.gov.co/portal/admin/archivos/publicaciones/2019/29355-DOC-20191221.pdf

ALCALDÍA MUNICIPAL DE IBAGUÉ. [Sitio Web]. Ibagué. Conservación Documental. [Consulta: 29 de septiembre de 2021]. Disponible en: https://ibague.gov.co/portal/admin/archivos/publicaciones/2017/18768-DOC-20171101.pdf

ALCALDÍA MUNICIPAL DE IBAGUÉ. [Sitio Web]. Ibagué. Creación y Custodia de Copias de Seguridad de la Información. [Consulta: 29 de septiembre de 2021]. Disponible en:

https://ibague.gov.co/portal/admin/archivos/publicaciones/2019/25050-DOC-20191127142431.pdf

ALCALDÍA MUNICIPAL DE IBAGUÉ. [Sitio Web]. Ibagué. Desarrollo y Mantenimiento de Software. .[Consulta: 29 de septiembre de 2021]. Disponible en: https://ibague.gov.co/portal/admin/archivos/publicaciones/2019/25054-DOC-20191127144526.pdf

ALCALDÍA MUNICIPAL DE IBAGUÉ. [Sitio Web]. Ibagué. Gestión de Servicios. [Consulta: 29 de septiembre de 2021]. Disponible en: https://ibague.gov.co/portal/admin/archivos/publicaciones/2019/26883-DOC-20191127143617.pdf

ALCALDÍA MUNICIPAL DE IBAGUÉ. [Sitio Web]. Ibagué. Gestión de Servicios. [Consulta: 29 de septiembre de 2021]. Disponible en: https://ibague.gov.co/portal/admin/archivos/publicaciones/2019/27438-DOC-20191127144210.pdf

ALCALDÍA MUNICIPAL DE IBAGUÉ. [Sitio Web]. Ibagué. Plan Estratégico de TIC. [Consulta: 29 de septiembre de 2021]. Disponible en: https://ibague.gov.co/portal/admin/archivos/publicaciones/2019/29358-DOC-20191224.pdf

ALCALDÍA MUNICIPAL DE IBAGUÉ. [Sitio Web]. Ibagué. Planeación de Gestión Documental. [Consulta: 29 de septiembre de 2021]. Disponible en: https://ibague.gov.co/portal/admin/archivos/publicaciones/2019/18777-DOC-20191107091316.pdf

ALCALDÍA MUNICIPAL DE IBAGUÉ. [Sitio Web]. Ibagué. Política de Seguridad de la Información. [Consulta: 29 de septiembre de 2021]. Disponible en: https://ibague.gov.co/portal/admin/archivos/publicaciones/2021/25290-DOC-20210511151206.pdf

ALCALDÍA MUNICIPAL DE IBAGUÉ. [Sitio Web]. Ibagué. Política General de SGSI. [Consulta: 29 de septiembre de 2021]. Disponible en: https://ibague.gov.co/portal/admin/archivos/publicaciones/2021/25289-DOC-20210511151205.pdf

ALCALDÍA MUNICIPAL DE IBAGUÉ. [Sitio Web]. Ibagué. Programa de Gestión Documental. [Consulta: 29 de septiembre de 2021]. Disponible en: https://ibague.gov.co/portal/admin/archivos/publicaciones/2018/18801-DOC-20181022.pdf

ALCALDÍA MUNICIPAL DE IBAGUÉ. [Sitio Web]. Ibagué. Programa y Manejo de Residuos Tecnológicos. [Consulta: 29 de septiembre de 2021]. Disponible en:

https://ibague.gov.co/portal/admin/archivos/publicaciones/2019/25049-DOC-20191127143142.pdf

ALCALDÍA MUNICIPAL DE IBAGUÉ. [Sitio Web]. Sistema Integrado de Gestión. Ibagué. [Consulta: 01 de mayo de 2021]. Disponible en: https://ibague.gov.co/portal/seccion/contenido/contenido.php?type=3&cnt=129&subtype=1&subcnt=228

APC-COLOMBIA. Bo [Sitio Web]. Programa de Gestión Documental. [Consulta: 01 de mayo de 2021]. Disponible en: https://www.apccolombia.gov.co/sites/default/files/archivos_usuario/2017/a-ot-009programagestiondocumentalv5.pdf

ARCHIVO GENERAL DE LA NACIÓN – AGN. [Sitio Web]. Glosario [Consulta: 17 de mayo de 2021]. Disponible en: https://www.archivogeneral.gov.co/Transparencia/informacion-interes/Glosario

ARCHIVO GENERAL DE LA NACIÓN. [Sitio Web]. Bogotá: AGN, Acuerdo 003 de 2015 [Consulta: 01 de mayo de 2021]. Disponible en: https://normativa.archivogeneral.gov.co/acuerdo-003-de-2015/

ARCHIVO GENERAL DE LA NACIÓN. [Sitio Web]. Bogotá: AGN, Ley 527 de 1999 [Consulta: 01 de mayo de 2021]. Disponible en: https://normativa.archivogeneral.gov.co/ley-527-de-1999/

ARCHIVO GENERAL DE LA NACIÓN. [Sitio Web]. Bogotá: AGN, Ley 594 de 2000 [Consulta: 01 de mayo de 2021]. Disponible en: https://normativa.archivogeneral.gov.co/ley-594-de-2000/.

ARCHIVO GENERAL DE LA NACIÓN. [Sitio Web]. Ley 1712 de 2014. Bogotá: AGN. [Consulta: 01 de mayo de 2021]. Disponible: https://normativa.archivogeneral.gov.co/ley-1712-de-2014/

CENTRO DE INNOVACIÓN PÚBLICA DIGITAL. [Sitio Web]. Iniciativa Cero Papel MINTIC [Consulta: 17 de mato de 2021]. Disponible: https://centrodeinnovacion.mintic.gov.co/es/experiencias/iniciativa-cero-papel-mintic

Cesar T. LA importancia de realizar un análisis de riesgo en las empresas. [Sitio Web] Universidad Piloto de Colombia. [Consulta: 09 de septiembre de 2021] Disponible en: http://polux.unipiloto.edu.co:8080/00003266.pdf

EALDE BUSINESS SCHOOL. [Sitio Web]. Madrid: EALDE. Gestión del Riesgo. Que es la norma ISO 31000 y para qué sirve [Consulta: 01 de mayo de 2021]. Disponible en: https://www.ealde.es/iso-31000-para-que-sirve/.

FIRMA-e. [Sitio Web]. ¿Qué es un SGSI - Sistema de Gestión de la Información? [Consulta: 01 de mayo de 2021] Disponible en: https://www.firma-e.com/blog/que-es-un-sgsi-sistema-de-gestion-de-seguridad-de-la-informacion/

FUNCIÓN PUBLICA. [Sitio Web]. Ley 527 de 1999. [Consulta: 01 de mayo de 2021]. Disponible en: https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=4276

GOBIERNO DE ESPAÑA. [Sitio Web]. MAGERIT v.3 : Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. España. Administración Electrónica. [Consultado: 17 de mayo 2021]. Disponible en: https://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_Magerit.html.

GOBIERNO EN LÍNEA. [Sitio Web]. Buenas Prácticas para reducir el consumo de papel. Bogotá: [Consulta: 01 de mayo de 2021]. Disponible: https://estrategia.gobiernoenlinea.gov.co/623/articles-8257_papel_buenaspracticas.pdf.

INCIBE-CERT. [Sitio Web]. Inventario de Activos y Gestión de Seguridad en SCI. España. [Consulta 18 de mayo de 2021] Disponible en: https://www.incibe-cert.es/blog/inventario-activos-y-gestion-seguridad-sci

Isabel C. [Sitio Web]. La importancia de la gestión de riesgos en las empresas. [Consulta: 01 de mayo de 2021]. Disponible: http://blogs.portafolio.co/buenas-practicas-de-auditoria-y-control-interno-en-las-organizaciones/la-importancia-la-gestion-riesgos-las-empresas/

ISO.es. Controles ISO 27002-2013. [Sitio Web] https://www.iso27000.es [Consulta: 29 de septiembre de 2021]. Disponible en: https://www.iso27000.es/assets/files/ControlesISO27002-2013.pdf

ISO. [Sitio Web]. ISO 31000:2018 Gestión del Riesgo - Directrices. [Consulta 01 de mayo de 2021]. Disponible en:]https://www.iso.org/obp/ui/es/#iso:std:iso:31000:ed-2:v1:es

ISOTools. [Sitio Web]. ¿Cuál es la terminología que utiliza la nueva ISO 31000?. [Consulta 01 de mayo de 2021]. Disponible en: https://www.isotools.org/2018/02/28/la-terminologia-utiliza-la-nueva-iso-31000/

Metodología Margerit para el análisis e identificación de riesgos en SGSI https://www.pmg-ssi.com/2021/07/metodologia-margerit-para-el-analisis-e-identificacion-de-riesgos-en-sgsi/

MININTERIOR. [Sitio Web]. Bogotá: Mapa de Riesgos [Consulta: 01 de mayo de 2021]. Disponible en: https://www.mininterior.gov.co/content/mapa-de-riesgos

MINTIC. [Sitio Web]. Guía para la Gestión y Clasificación de Activos de la Información. Bogotá: EALDE. [Consulta 17 de mayo de 2021]. Disponible en: https://www.mintic.gov.co/gestionti/615/articles-5482_G5_Gestion_Clasificacion.pdf

MINTIC. [Sitio Web]. Modelo de Seguridad y Privacidad de la Información. Bogotá. [Consulta: 01 de mayo de 2021]. Disponible: https://www.mintic.gov.co/gestionti/615/articles-5482_Modelo_de_Seguridad_Privacidad.pdf

MINTIC. Guía para la Gestión y Clasificación. [Sitio Web]. Bogotá. [Consultado: 17 de mayo 2021]. Disponible en: https://www.mintic.gov.co/gestionti/615/articles-5482_G5_Gestion_Clasificacion.pdf#page=16&zoom=100,148,133. P16.

MINTIC. Guía para la Gestión y Clasificación. [Sitio Web]. Bogotá. [Consultado: 17 de mayo 2021]. Disponible en: https://www.mintic.gov.co/gestionti/615/articles-5482_G5_Gestion_Clasificacion.pdf#page=16&zoom=100,148,133. P13.

NORMA ISO 27001. [Sitio Web]. Madrid: ISO 27001 Seguridad de la Información [Consulta: 01 de mayo de 2021]. Disponible en: https://normaiso27001.es/referencias-normativas-iso-27000/#def328

NORMA ISO 27001. [Sitio Web]. Madrid: Referencias Normativas Iso 27000 [Consulta: 01 de mayo de 2021]. Disponible en: https://normaiso27001.es/referencias-normativas-iso-27000/#def328

NORMA ISO 27001. [Sitio Web]. Madrid: Referencias Normativas Iso 27000 [Consulta: 01 de mayo de 2021]. Disponible en: https://normaiso27001.es/referencias-normativas-iso-27000/#def36

NORMA ISO 27001. [Sitio Web]. Madrid: Referencias Normativas Iso 27000 [Consulta: 01 de mayo de 2021]. Disponible en: https://normaiso27001.es/referencias-normativas-iso-27000/#def310.

NORMA ISO 27001. [Sitio Web]. Madrid: Referencias Normativas Iso 27000 [Consulta: 01 de mayo de 2021]. Disponible en: https://normaiso27001.es/referencias-normativas-iso-27000/#def37.

NORMA ISO 27001. [Sitio Web]. Madrid: Referencias Normativas Iso 27000 [Consulta: 01 de mayo de 2021]. Disponible en: https://normaiso27001.es/referencias-normativas-iso-27000/#terminos

NORMAS ISO. [Sitio Web]. ISO 27001 Seguridad de la Información. [Consulta: 01 de mayo de 2021]. Disponible en: https://www.normas-iso.com/iso-27001/

Sierra, M y Hurtado J, [En línea]. Modelo de Seguridad y Privacidad de la Información para la Alcaldía de Puerto Asís en su Fase de Diagnóstico y Planificación. Trabajo de Grado. Bogotá. Institución Universitaria Politécnico Gran Colombiano. (2016). [Consulta: 01 de mayo de 2021] Disponible en: https://alejandria.poligran.edu.co/bitstream/handle/10823/1241/Proyecto%20de%20grado.pdf?sequence=1&isAllowed=y

ANEXOS

A continuación, se relaciona los anexos que soportan el desarrollo del proyecto aplicado.

Anexo A: Autorización Empresa V1

Anexo B: Acuerdo de confidencialidad - Empresa Estudiante V1

Anexo C: Acta de Reunión No. 001

Anexo D: Acta de Reunión No. 002

Anexo E: Organigrama Institucional

Anexo F: Matriz Inventario y Clasificación.

Anexo G: Identificación de Activos - MARGERIT

Anexo H: Matriz Metodología – MARGERIT

Anexo I: Matriz Resumen Amenazas.

Anexo J: Estructura del documento para la estructura del Resumen Analítica Especializado - RAE

Link Archivos: https://unadvirtualedu-my.sharepoint.com/:f:/g/personal/advalenciab_unadvirtual_edu_co/EuZuGT4YvztLuVia9ZV5a7kBYScaG4x2L3PDJ571G_LtyA?e=L0yn15

Anexo A

V0.1

Ibagué, 28 de marzo de 2021

Doctora:
JULIANA CUARTAS CANDAMIL
Secretaria Administrativa
ALCALDÍA MUNICIPAL DE IBAGUÉ

Asunto: Autorización para la ejecución del proyecto titulado: *Análisis de los riesgos de seguridad de la información del Sistema de Gestión Documental de la Alcaldía Municipal de Ibagué*.

Cordial saludo estimada Secretaria:

Como es de su conocimiento, actualmente me encuentro adelantando estudios de posgrado en la Especialización en Seguridad Informática ofertado por la Universidad Nacional Abierta y a Distancia "UNAD". Para finalizar mi proceso académico es mi objetivo desarrollar un trabajo de grado aplicado a la Alcaldía Municipal de Ibagué, de manera que pueda aportar mis conocimientos adquiridos y generar un impacto positivo en la empresa, relacionado con los temas de Seguridad Informática, motivo por el cual, muy comedidamente solicito su autorización y aprobación para la ejecución del proyecto titulado: "*Análisis de los riesgos de seguridad de la información del Sistema de Gestión Documental de la Alcaldía Municipal de Ibagué"* el cual se encuentra avalado por parte la Institución de educación superior "UNAD".

El proyecto en su objetivo general describe lo siguiente: "Analizar los riesgos de seguridad de la información del Sistema de Gestión Documental de la Alcaldía Municipal de Ibagué, aplicando la metodología MAGERIT la cual está asociada con las normas ISO 31000 y la ISO 27001:2013."; al mismo tiempo será apoyado por los objetivos específicos: "Identificación y categorización de activos de información existentes en la Alcaldía Municipal de Ibagué; Aplicar la metodología MARGERIT para la evaluación de riesgos que permita identificar vulnerabilidades y amenazas de seguridad, así como evaluar los riesgos conforme lo establece la metodología; Proponer mecanismos de control y gestión que reduzcan las vulnerabilidades identificadas en el análisis realizado; Elaborar informe de hallazgos y recomendaciones que permita precisar un Sistema de Seguridad de la información concreta a la realidad de la Alcaldía Municipal de Ibagué." para obtener como resultado un alto impacto en la seguridad de la empresa Alcaldía de Ibagué.

Continuación anexo A

V0.1

De obtener esta autorización, se elaborará un acuerdo de confidencialidad para proteger la identidad la empresa y sus activos de información; a su vez se destacan los siguientes procesos para ser garantes en la transaparencia de la ejecución del proyecto:

- Se prohíbe la ejecución de cualquier tipo de pruebas de seguridad que no estén autorizadas expresamente por *Alcaldía Municipal de Ibagué.*
- La empresa *Alcaldía Municipal de Ibagué* deberá establecer qué tipo de información es privada y cuál es pública para delimintar el acceso de pruebas en la ejecución del proyecto.
- La solicitud de información al igual que ejecución de prubas deben quedar por escrito y se genera un informe de resultados semanalmente el cual será compartido con el gerente de la organización o empresa.
- La persona autorizada siempre debe operar dentro de la ley 1273 de 2009 y de las demás regulaciones establecidas en la empresa.
- Respetar la privacidad de todos los individuos y mantener su privacidad en los reportes. Se encuentra prohibida la divulgación de información personal en tales reportes.

El resultado del proyecto se verá reflejado en un documento el cual será cargado al repositorio institucional de la Universidad Nacional Abierta y a Distancia "UNAD". El dcumento ampara la confidencialidad y anonimato de la empresa, estos aspectos se encuentran estipulados en el acuerdo de confidencialidad; agradezco el apoyo prestado en esta etapa de mi carrerar profesional.

Firman en Ibagué, a los (28) días del mes de marzo de 2021

Cordialmente,

ALBA DENYS VALENCIA BAUTISTA
Estudiante UNAD.

JULIANA CUARTAS CANDAMIL
Secretaría Administrativa

Anexo B

Alcaldía Municipal
Ibagué
NIT.800113389-7

V 0.1

ACUERDO DE CONFIDENCIALIDAD ENTRE ALBA DENYS VALENCIA BAUTISTA Y ALCALDÍA MUNICIPAL DE IBAGUÉ

Por la **parte reveladora**

Nombre: Alcaldía Municipal de Ibagué – Secretaría Administrativa
Dirección: Calle 9 No 2-59 Palacio Municipal
Teléfono: 261 18 55
E-mail: administrativa@ibagué.gov.co

Por la parte **receptora de la información**

Nombre: Alba Denys Valencia Bautista
Dirección: Carrera 59 No 1B – 65 Barrio La Floresta
Teléfono: 312 556 80 10
E-mail: advalenciab@unadvirtual.edu.co

Identificación del proyecto

Entre los firmantes, identificados anteriormente, hemos convenido en celebrar el presente acuerdo de confidencialidad previa las siguientes **CONSIDERACIONES**

1. Que la información compartida en virtud del presente acuerdo pertenece a la *Alcaldía Municipal de Ibagué*, y la misma es considerada sensible y de carácter restringido en su divulgación, manejo y utilización. Dicha información es compartida en virtud del desarrollo del proyecto *aplicado con el título: Análisis de los riesgos de seguridad de la información del Sistema de Gestión Documental de la Alcaldía Municipal de Ibagué*

2. Que la información de propiedad de *Alcaldía Municipal de Ibagué* ha sido desarrollada u obtenido legalmente, como resultado de

Continuación anexo B

sus procesos, programas o proyectos y, en consecuencias abarca documentos, datos, tecnología y/o material que considera

único y confidencial, o que es objeto de protección a título de secreto industrial.

3. Que el presente acuerdo se realiza por un lado entre la parte receptora de la información como integrante del proyecto de aplicado "*Análisis de los riesgos de seguridad de la información del Sistema de Gestión Documental de la Alcaldía Municipal de Ibagué", Alba Denys Valencia Bautista* que, para el presente caso actual como **revelador, guarda y administrados** de la información de propiedad de *Alcaldía Municipal de Ibagué*.

En consecuencia, **las partes** se suscriben a las siguientes cláusulas:

Primera. Objeto: en virtud del presente **acuerdo de confidencialidad,** la **parte receptora**, se obliga a no divulgar directa, indirecta, próxima a remotamente, ni a través de ninguna otra persona o de sus subalternos o funcionarios, asesores o cualquier persona relacionada con ella, la **información confidencial** perteneciente al ***Alcaldía Municipal de Ibagué,*** así como también a no utilizar dicha

información en beneficio propio ni de terceros, sólo con fines estadísticos y de mejoramiento de la ***Alcaldía Municipal de Ibagué.***

Segunda. Definición de información confidencial: se entiende como **Información Confidencial**, para los efectos del presente acuerdo:

1. La información que no sea pública y sea conocida por la **parte receptora** con ocasión de del proyecto de investigación y/ extensión.

2. Cualquier información societaria, técnica, jurídica, financiera, comercial, de mercado, estratégica, de productos, nuevas tecnologías, patentes, modelos de utilidad, diseños industriales,

Continuación anexo B

modelos de negocios, información del personal de la organización y/o cualquier otra relacionada con el proyecto "*Análisis de los riesgos de seguridad de la información del Sistema de Gestión Documental de la Alcaldía Municipal de Ibagué*" lograr tales fines, y/o cualquier otro ente relacionado con la estructura organizacional, bien sea que la misma sea escrita, oral o visual, o en cualquier forma tangible o no, incluidos los mensajes de datos (en la forma definida en la ley), de la cual, la **parte receptora** tenga conocimiento o a la que tenga acceso por cualquier medio o circunstancia en virtud de las reuniones sostenidas y/o documentos suministrados.

3. La que corresponda o deba considerarse como tal para garantizar el derecho constitucional a la intimidad, la honra y el buen nombre de las personas y deba guardarse la debida diligencia en su discreción y manejo en el desempeño de sus funciones.

Tercera. Origen de la información confidencial: provendrá de documentos suministrados en el desarrollo del proyecto y que tiene que ver con las creaciones del intelecto, a la naturaleza, medios, formas de distribución, comercialización de productos o de prestación de servicios, transmitida verbal, visual o materialmente, por escrito en los documentos, medios electrónicos, discos ópticos, microfilmes, películas, e-mail u otros elementos similares suministrados de manera tangible o intangible, independiente de su fuente o soporte y sin que requiera advertir su carácter confidencial.

Cuarta. Obligaciones de la parte receptora: Se considerará como **parte receptora** de la **información confidencial** a la persona que recibe la información, o que tenga acceso a ella. La parte receptora se obliga a:

De ser necesario o conveniente según la necesidad del titular de la información, se adicionarán las obligaciones que se consideren pertinentes:

Continuación anexo B

1. Mantener la **información confidencial** segura, usarla solamente para los propósitos relacionados con él, en caso de ser solicitada, devolverla toda (incluyendo copias de esta) en el momento en que ya no requiera hacer uso de la misma o cuando termine la relación, caso en el cual, deberá entregar dicha información antes de la terminación de la vinculación.

2. Proteger la **información confidencial**, sea verbal, escrita, visual, tangible, intangible o que por cualquier otro medio reciba, siendo legitima poseedora de la misma *Alcaldía Municipal de Ibagué*, restringiendo su uso exclusivamente a las personas que tengan absoluta necesidad de conocerla.

3. Abstenerse de publicar la **información confidencial** que conozca, reciba o intercambie con ocasión de las reuniones sostenidas.

4. Usar la **información confidencial** que se le entregue, únicamente para los efectos señalados al momento de la entrega de dicha información.

5. Mantener la **información confidencial** en reserva hasta tanto adquiera el carácter de pública.

6. Responder por el mal uso que le den sus representantes a la **información confidencial.**

7. Guardar la reserva de la **información confidencial** como mínimo, con el mismo cuidado con la que protege la **información confidencial.**

8. La **parte receptora** se obliga a no transmitir, comunicar revelar o de cualquier otra forma divulgar total o parcialmente, pública o privadamente, la **información confidencial** sin el previo consentimiento por escrito por parte de ***Alcaldía Municipal de Ibagué.***

9. La **parte receptora** se compromete a establecer que los datos a utilizar son: Almacenamiento físico (ficheros, copias de respaldo, credenciales, etc) servicios, software (plataforma PISMAMI, antivirus, sistema operativo, entre otros), equipamiento informático, redes de comunicación, equipamiento auxiliar, instalaciones, personal (no se solicita datos personales del personal).

10. La información capturada por la **parte receptora** se observará como, *información cualitativa,* no existirá ningún tipo de ganancia económica, es netamente educativo.

11. La identidad de todo el personal ***Alcaldía Municipal de Ibagué*** no será revelada, dado que no se capturará sus nombres completos ni algún otro tipo de información que revele su identidad física o digital.

12. Las pruebas realizadas por la **parte receptora** nunca pondrán en peligro los activos tecnológicos de ***Alcaldía Municipal de Ibagué,*** ni violentará la ley de delitos informáticos Colombiana 1273 de 2009 estando en el margen de las buenas prácticas y los procesos legales pertinentes.

13. El estudiante *Alba Denys Valencia Bautista* se compromete a difuminar, bloquear y ocultar toda información que revele la identidad de la empresa *Alcaldía Municipal de Ibagué* para salvaguardar la confidencialidad e identidad de la empresa en el documento final del proyecto el cual será publicado en el repositorio institucional y de acceso público.

14. El título del proyecto no podrá contener el nombre de la empresa u organización con la que se firma el presente acuerdo de confidencialidad, este nombre deberá ser reemplazado.

Parágrafo: Cualquier divulgación autorizada de la **información confidencial** a terceras personas estará sujeta a las mismas obligaciones de confidencialidad derivadas del presente **Acuerdo** y la

Continuación anexo B

parte receptora deberá informar estas restricciones incluyendo la identificación de la información cono confidencial.

Quinta. Obligaciones de la parte reveladora: Son obligaciones de la parte reveladora:

1. Mantener la reserva de la **información confidencial** hasta tanto adquiera el carácter de pública.

2. Documentar toda la **información confidencial** que transmita de manera escrita, oral o visual, mediante documentos, medios electrónicos, discos ópticos, microfilmes, películas, e-mails u otros elementos similares o en cualquier forma tangible o no, incluidos los mensajes de datos, como registro de la misma para la determinación de su alcance, e indicar específicamente y de manera clara e inequívoca el carácter confidencia de la información suministrada de la **parte receptora**.

Sexta. Exclusiones a la confidencialidad: La **parte receptora** queda relevada o eximida de la obligación de confidencialidad, únicamente en los siguientes casos:

1. Cuando la **información confidencial** haya sido o sea de dominio público. Si la información se hace de dominio público durante el plazo del presente acuerdo, por un hecho ajeno a la **parte receptora,** esta conservará su deber de reserva sobre la información que no haya sido afectada.

2. Cuando la **información confidencial** deba ser revelada por sentencia en firme de un tribunal o autoridades competentes en desarrollo de sus funciones que ordenen el levantamiento de la reserva y soliciten el suministro de esta información. No obstante, en este caso la parte reveladora será la encargada de dar cumplimiento a la orden, restringiendo la divulgación a la información estrictamente necesaria, y en el evento de que la

Continuación anexo B

confidencialidad se mantenga, no eximirá a la parte receptora del deber de reserva.

3. Cuando la **parte receptora pruebe** que la **información confidencial** ha sido obtenida por otras fuentes.

4. Cuando la **información confidencial** ya la tenía en su poder la parte receptora antes de la entrega de la información reservada.

Séptima. Responsabilidad: la parte que contravenga el acuerdo será responsable ante la otra parte o ante los terceros de buena fe sobre los cuales se demuestre que se han visto afectados por la inobservancia del presente **acuerdo**, por los perjuicios morales y económicos que estos puedan sufrir como resultado del incumplimiento de las obligaciones aquí contenidas.

Octava. Solución de controversias: Las partes *(Alba Denys Valencia Bautista – Alcaldía Municipal de Ibagué)* se comprometen a esforzarse en resolver mediante los mecanismos alternativos de solución de conflictos cualquier diferencia que surja con motivo de la ejecución del presente **acuerdo.** En caso de no llegar a una solución directa para la controversia planteada, someterán la cuestión controvertida a las leyes colombianas y a la jurisdicción competente en el momento de presentarse la diferencia. La Universidad Nacional Abierta y a Distancia como institución educativa no se hace responsable del no cumplimiento de las cláusulas del presente acuerdo de confidencialidad por parte de *Alba Denys Valencia Bautista.*

Novena. Legislación aplicable: Este **acuerdo** se regirá por las leyes de la República de Colombia y se interpretará de acuerdo con las mismas.

Continuación anexo B

Alcaldia Municipal
Ibagué
NIT.800113389-7

V 0.1

Décima. Aceptación del Acuerdo: Las partes han leído y estudiado de manera detenida los términos y el contenido del presente **Acuerdo** y por tanto manifiestan estar conformes y aceptan todas las condiciones.

Firman en Ibagué, a los (28) días del mes de (marzo) de 2021.

Como Parte Receptora:

Alba Denys Valencia Bautista
Estudiante UNAD.
C.C. No. 38.364.056 de Ibagué

Por la parte reveladora:

Juliana Cuartas Candamil
Secretaría Administrativa
C.C. No. 38.246.184 de Ibagué

Anexo C

Universidad Nacional Abierta y a Distancia

ACTA DE REUNIÓN

ACTA No. 01		
FECHA: 12 de mayo de 2021	***HORA:*** 10:00 a 10:30 a.m	***LUGAR:*** Despacho Secretaría de las TIC

OBJETIVO
Recopilación de información, para el desarrollo del proyecto Aplicado "*Análisis de los riesgos de seguridad de la información del sistema de gestión documental de la alcaldía municipal de Ibagué*"

ORDEN DEL DÍA	
1. Socialización Proyecto Aplicado.	2. Entrega Información
3. Compromisos	4. Cierre Reunión

DESARROLLO REUNIÓN
1 **Socialización Proyecto aplicado:**

De acuerdo a la aprobación emitida por parte de la Secretaria Administrativa Juliana Cuartas Candamil, para la entre de información confidencial y publica de los activos de la Administración Municipal a la estudiante y funcionaria Alba Denys Valencia Bautista, la misma, procede a socializar el objetivo del proyecto aplicado como modalidad de grado del programa de Especialización de Seguridad Informática.

La presente informa que el proyecto se denomina "*Análisis de los riesgos de seguridad de la información del sistema de gestión documental de la alcaldía municipal de Ibagué*", cuyos objetivos radican en:

OBJETIVOS GENERAL:

ANALIZAR LOS RIESGOS DE SEGURIDAD DE LA INFORMACIÓN DEL SISTEMA DE GESTIÓN DOCUMENTAL DE LA ALCALDÍA MUNICIPAL DE IBAGUÉ, APLICANDO LA METODOLOGÍA MAGERIT LA CUAL ESTÁ ASOCIADA CON LAS NORMAS ISO 31000 Y LA ISO 27001:2013.

OBJETIVOS ESPECÍFICOS

- Aplicar la metodología MARGERIT para la evaluación de riesgos que permita identificar vulnerabilidades y amenazas de seguridad, así como evaluar los riesgos conforme lo establece la metodología.
- Proponer mecanismos de control y gestión que reduzcan las vulnerabilidades identificadas en el análisis realizado.
- Elaborar informe de hallazgos y recomendaciones que permita precisar un Sistema

Continuación Anexo C:

Universidad Nacional Abierta y a Distancia

ACTA DE REUNIÓN

de Seguridad de la información concreta a la realidad de la Alcaldía Municipal de Ibagué.

Teniendo en cuenta lo expuesto la funcionaria afirma que para el desarrollo del mismo es necesario contar con información de los activos relacionados a continuación:

- Aplicaciones
- Hardware
- Red
- Tecnología
- Equipamiento.

2 Entrega de Información:

Conforme lo socializado por la ingeniera Alba Denys, el profesional universitario Jaime Orlando Jaramillo, adscrito a la Secretaría de las TIC, grupo Ciencia Tecnología e Innovación, se compromete a efectuar entrega de la información correspondiente a los activos: Aplicaciones.

Así mismo el funcionario John Freddy, efectúa, adscrito a la Secretaría de las TIC del Grupo de Infraestructura Tecnológica, queda pendiente de entrega de la información correspondiente a Hardware, Red, Tecnología y Equipamiento Auxiliar.

3 Compromisos

No. Comp	Acción	Responsable	Cargo	Fecha Entrega
1	Entrega información Activos: Aplicaciones	Jaime Orlando Jaramillo	Profesional Universitario	15/05/2021
2	Hardware, Red, Tecnología y Equipamiento Auxiliar	Jhon Fredy Lugo Luna	Profesional Universitario	15/05/2021

4 Cierre Reunión

Una vez desarrollado el orden del día de la reunión, se procede a efectuar el cierre de la misma, siendo las 10:30 a.m.

Continuación Anexo C

Universidad Nacional Abierta y a Distancia

ACTA DE REUNIÓN

FUNCIONARIOS ADMINISTRACIÓN MUNICIPAL	
FIRMA:	FIRMA:
NOMBRE: JOHN FREDDY LUGO LUNA	**NOMBRE:** JAIME ORLANDO JARAMILLO
CARGO: Profesional Universitario	**CARGO:** Profesional Universitario

ESTUDIANTE UNIVERSIDAD UNAD
FIRMA:
NOMBRE: ALBA DENYS VALENCIA BAUTISTA
CARGO: Estudiante

Anexo D

Universidad Nacional Abierta y a Distancia

ACTA DE REUNIÓN

ACTA No. 02		
FECHA: 12 de mayo de 2021	***HORA:*** 10:30 a 11:00 a.m	***LUGAR:*** Despacho Secretaría Administrativa

OBJETIVO
Recopilación de información, para el desarrollo del proyecto Aplicado "*Análisis de los riesgos de seguridad de la información del sistema de gestión documental de la alcaldía municipal de Ibagué*"

ORDEN DEL DÍA	
1. Socialización Proyecto Aplicado.	2. Entrega Información
3. Compromisos	4. Cierre Reunión

DESARROLLO REUNIÓN	
1	**Socialización Proyecto aplicado:**

De acuerdo a la aprobación emitida por parte de la Secretaria Administrativa Juliana Cuartas Candamil, para la entre de información confidencial y publica de los activos de la Administración Municipal a la estudiante y funcionaria Alba Denys Valencia Bautista, la misma, procede a socializar el objetivo del proyecto aplicado como modalidad de grado del programa de Especialización de Seguridad Informática.

La presente informa que el proyecto se denomina "*Análisis de los riesgos de seguridad de la información del sistema de gestión documental de la alcaldía municipal de Ibagué*", cuyos objetivos radican en:

OBJETIVOS GENERAL:

ANALIZAR LOS RIESGOS DE SEGURIDAD DE LA INFORMACIÓN DEL SISTEMA DE GESTIÓN DOCUMENTAL DE LA ALCALDÍA MUNICIPAL DE IBAGUÉ, APLICANDO LA METODOLOGÍA MAGERIT LA CUAL ESTÁ ASOCIADA CON LAS NORMAS ISO 31000 Y LA ISO 27001:2013.

OBJETIVOS ESPECÍFICOS

- Aplicar la metodología MARGERIT para la evaluación de riesgos que permita identificar vulnerabilidades y amenazas de seguridad, así como evaluar los riesgos conforme lo establece la metodología.
- Proponer mecanismos de control y gestión que reduzcan las vulnerabilidades identificadas en el análisis realizado.
- Elaborar informe de hallazgos y recomendaciones que permita precisar un Sistema de Seguridad de la información concreta a la realidad de la Alcaldía Municipal de Ibagué.

Continuación Anexo D

ACTA DE REUNIÓN

Teniendo en cuenta lo expuesto la funcionaria afirma que para el desarrollo del mismo es necesario contar con información de los activos relacionados a continuación:

- Personal
- Instalaciones.

2 Entrega de Información:

Conforme lo socializado por la ingeniera Alba Denys, la funcionaria Magda Mayerly, se compromete entregar la información correspondiente al personal e instalaciones de la Alcaldía Municipal de Ibagué.

3 Compromisos

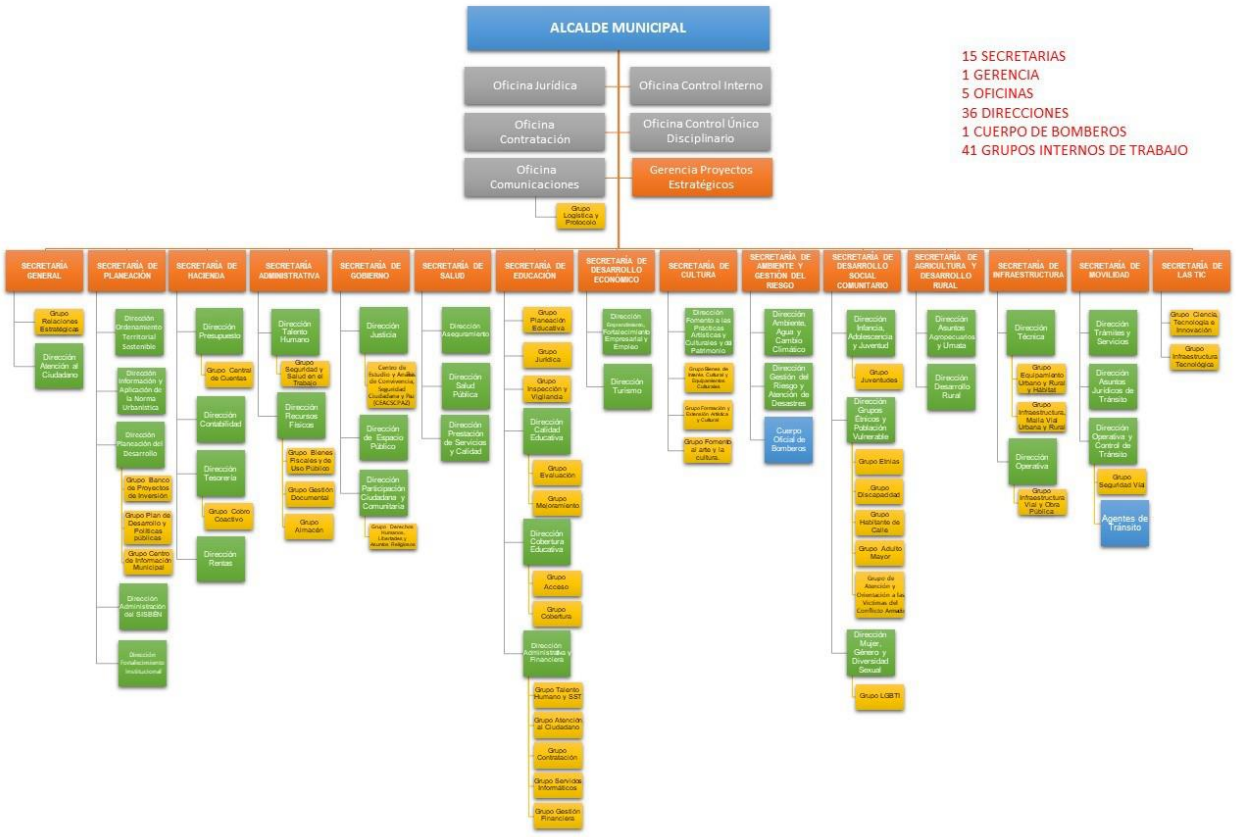
No. Comp	Acción	Responsable	Cargo	Fecha Entrega
1	Entrega información Activos: Personal e Instalaciones	Magda Mayerly Ospitia	Profesional Especializado	14/05/2021

4 Cierre Reunión

Una vez desarrollado el orden del día de la reunión, se procede a efectuar el cierre de la misma, siendo las 11:00 a.m.

FUNCIONARIO ADMINISTRACIÓN MUNICIPAL	ESTUDIANTE UNIVERSIDAD UNAD
FIRMA:	FIRMA:
NOMBRE: MAGDA MAYERLY OSPITIA	**NOMBRE:** ALBA DENYS VALENCIA BAUTISTA
CARGO: Profesional Especializado	**CARGO:** Estudiante

Anexo E


ALCALDE MUNICIPAL
Oficina Jurídica
Oficina Control Interno
Oficina Contratación
Oficina Control Único Disciplinario
Oficina Comunicaciones
Gerencia Proyectos Estratégicos
Grupo Logística y Protocolo
15 SECRETARIAS
1 GERENCIA
5 OFICINAS
36 DIRECCIONES
1 CUERPO DE BOMBEROS
41 GRUPOS INTERNOS DE TRABAJO
SECRETARÍA GENERAL
SECRETARÍA DE PLANEACIÓN
SECRETARÍA DE HACIENDA
SECRETARÍA ADMINISTRATIVA
SECRETARÍA DE GOBIERNO
SECRETARÍA DE SALUD
SECRETARÍA DE EDUCACIÓN
SECRETARÍA DE DESARROLLO ECONÓMICO
SECRETARÍA DE CULTURA
SECRETARÍA DE AMBIENTE Y GESTION DEL RIESGO
SECRETARÍA DE DESARROLLO SOCIAL COMUNITARIO
SECRETARÍA DE AGRICULTURA Y DESARROLLO RURAL
SECRETARÍA DE INFRAESTRUCTURA
SECRETARÍA DE MOVILIDAD
SECRETARÍA DE LAS TIC

ANEXO F

Item	DATOS DEL ACTIVO DE INFORMACIÓN						1. CLASIFICACIÓN DE ACTIVOS DE LA INFORMACIÓN											
							Confidencialidad				Integridad				Disponibilidad			
	Categoría de Activos	Proceso	Nombre del Activo	Propietario del Activo	Responsable	Descripción	Reservada	Clasificada	Pública	No Clasificada	A - Alta	M- Mediano	B - Bajo	No Clasificada	1 - Alta	2 Mediano	3 - Bajo	4 - No Clasificada
1	Datos	Gestión Documental	CAR-GD-01 Gestión Documental.	Dirección de Recursos Físicos - Grupo Gestión Documental	Profesional Universitario	Caracterización del proceso en el cual se especifica las entradas salidas y beneficiarios,			×				×			×		
2	Datos	Gestión Documental	PGR-GD-01 Programa de Gestión Documental.	Dirección de Recursos Físicos - Grupo Gestión Documental	Profesional Universitario	Detalle de las funciones, procesos y procedimientos de programa			×				×			×		
3	Datos	Gestión Documental	PRO-PGD-10 Planeación de la Gestión Documental.	Dirección de Recursos Físicos - Grupo Gestión Documental	Profesional Universitario	Planeación de cada uno de los procesos ejecutados por el programa			×				×			×		
4	Datos	Gestión Documental	PLA-GD-02 Plan de Conservación Documental.	Dirección de Recursos Físicos - Grupo Gestión Documental	Profesional Universitario	Se detalla los pasos y procedimientos para la conservación del acervo documental			×				×			×		
5	Datos	Gestión de Infraestructura Tecnológica	PLA-GIT-02 Plan de incidentes .	Secretaría de las TIC	Secretaria de Despacho	Establece acciones y lineamientos para estar en la capacidad de responder a incidentes.			×				×			×		
6	Datos	Gestión de Infraestructura Tecnológica	POL-GIT-01 Política general SGSI	Secretaría de las TIC	Secretaria de Despacho	Se establece los lineamientos para el control de la información			×				×			×		
7	Datos	Gestión de Infraestructura Tecnológica	POL-GIT-02 Política de Seguridad de la Información.	Secretaría de las TIC	Secretaria de Despacho	Conjunto de reglas alineadas a las actividades de los Sistemas de Información			×				×			×		
8	Datos	Gestión de Infraestructura Tecnológica	PRO-GIT-03 Desarrollo y Mantenimiento de Software .	Secretaría de las TIC	Secretaria de Despacho	Procedimiento para efectuar mantenimiento y soporte - Software			×				×			×		
9	Datos	Gestión de Infraestructura Tecnológica	PRO-GIT-5 Mantenimiento y Soporte de Hardware	Secretaría de las TIC	Secretaria de Despacho	Procedimiento para efectuar mantenimiento y soporte - Hardware			×				×			×		
10	Datos	Gestión de Infraestructura Tecnológica	PRO-GIT-01 Creación y Custodia de Copias de Seguridad	Secretaría de las TIC	Secretaria de Despacho	Procedimiento para la creación custodia y copias de seguridad			×				×			×		
11	Datos	Gestión de Infraestructura Tecnológica	PGR-GIT-01 Programa y Manejo de Residuos Tecnológicos.	Secretaría de las TIC	Secretaria de Despacho	Detalla el proceso para la disposición final de residuos solidos y tecnológicos			×				×			×		
12	Datos	Gestión de Infraestructura Tecnológica	Datos de Control de Acceso a la Plataforma	Secretaría de las TIC - Grupo Ciencia, Tecnología e Innovación	Profesional Universitario	Relación												
13	Datos	Gestión de Infraestructura Tecnológica	Copias de Seguridad	Secretaría de las TIC - Grupo Infraestructura Tecnológica	Profesional Universitario	Copias de seguridad de los equipos de computo de la Administración Municipal y Sendtor	×				×				×			
14	Aplicaciones	Gestión de Infraestructura Tecnológica	PISAMI (Plataforma Integrada de Sistema Alcaldía Municipal Ibagué)	Secretaría de las TIC - Grupo Ciencia, Tecnología e Innovación	Profesional Universitario	Sistema Integrado, Tipo Web, desarrollado lenguaje PHP. SISTEMA OPERATIVO: Windows Server 2016 Motor BD: ORACLE 10G	×				×				×			
15	Aplicaciones	Gestión de Infraestructura Tecnológica	Lenguaje de Programación	Secretaría de las TIC - Grupo Ciencia, Tecnología e Innovación	Profesional Universitario	PHP y Laravel	×				×				×			
16	Aplicaciones	Gestión de Infraestructura Tecnológica	Sistemas Operativos	Secretaría de las TIC - Grupo Ciencia, Tecnología e Innovación	Profesional Universitario	Windows 10, Windows Server 2016, Win7 Pro, Win Vista, Win9P	×				×				×			
17	Aplicaciones	Gestión de Infraestructura Tecnológica	Motor Base de Datos	Secretaría de las TIC - Grupo Ciencia, Tecnología e Innovación	Profesional Universitario	Oracle 10G	×				×				×			
18	Aplicaciones	Gestión de Infraestructura Tecnológica	Antivirus	Secretaría de las TIC - Grupo Ciencia, Tecnología e Innovación	Profesional Universitario	Avira Antivirus	×				×				×			
19	Hardware	Gestión de Infraestructura Tecnológica	Equipo de Computo	Secretaría de las TIC - Grupo Ciencia, Tecnología e Innovación	Auxiliar Administrativo	HP PRODESK 400, WINPRO		×				×				×		
20	Hardware	Gestión de Infraestructura Tecnológica	Equipo de Computo	Secretaría de las TIC - Grupo Ciencia, Tecnología e Innovación	Auxiliar Administrativo	HP PRODESK, , WINPRO		×				×				×		
21	Hardware	Gestión de Infraestructura Tecnológica	Equipo de Computo	Secretaría de las TIC - Grupo Ciencia, Tecnología e Innovación	Profesional Especializado	HP COMPAQ PRO 6300, WINPRO		×				×				×		
22	Hardware	Gestión de Infraestructura Tecnológica	Equipo de Computo	Secretaría de las TIC - Grupo Ciencia, Tecnología e Innovación	Profesional Universitario	HP PRODESK, , WINPRO		×				×				×		
23	Hardware	Gestión de Infraestructura Tecnológica	Equipo de Computo - Portátil	Secretaría de las TIC - Grupo Ciencia, Tecnología e Innovación	Secretaria de Despacho	HP PROBOOK 250 G6, , WINPRO		×				×				×		
24	Hardware	Gestión de Infraestructura Tecnológica	Equipo de Computo	Secretaría de las TIC - Grupo Ciencia, Tecnología e Innovación	Técnico Operativo	HP PRODESK, , WINPRO		×				×				×		
25	Hardware	Gestión de Infraestructura Tecnológica	Equipo de Computo - Portátil	Secretaría de las TIC - Grupo Infraestructura Tecnológica	Técnico Operativo	HP PROBOOK 250 G6, , WINPRO		×				×				×		
26	Hardware	Gestión de Infraestructura Tecnológica	Equipo de Computo - Portátil	Secretaría de las TIC - Grupo Infraestructura Tecnológica	Técnico Operativo	HP PROBOOK 4540s, WINPRO		×				×				×		
27	Hardware	Gestión Humana	Equipo de Computo	Secretaria Administrativa - Despacho	Auxiliar Administrativo	HP PRODESK, WIN 10 PRO		×				×				×		
28	Hardware	Gestión Humana	Equipo de Computo	Secretaria Administrativa - Despacho - Dirección de Recursos Físicos	Auxiliar Administrativo	HP COMPAQ 6000 PRO, WIN 7 PRO		×				×				×		
29	Hardware	Gestión Humana	Equipo de Computo	Secretaria Administrativa - Despacho - Dirección de Recursos Físicos	Director	HP PRODESK 400, WIN 10 PRO		×				×				×		
30	Hardware	Gestión Humana	Equipo de Computo	Secretaria Administrativa - Despacho - Dirección de Recursos Físicos	Profesional Especializado	HP PRODESK400, WIN 10 PRO		×				×				×		
31	Hardware	Gestión Humana	Equipo de Computo	Secretaria Administrativa - Despacho - Dirección de Recursos Físicos	Profesional Universitario	DELL VOSTRO 2205, WIN VISTA BUSINESS		×				×				×		
32	Hardware	Gestión Humana	Equipo de Computo	Secretaria Administrativa - Despacho - Dirección de Recursos Físicos	Técnico Operativo	COMPAQ PAVILION 100, WIN 7 PRO		×				×				×		
33	Hardware	Gestión Humana	Equipo de Computo - Portátil	Secretaria Administrativa - Despacho - Dirección de Recursos Físicos	Técnico Operativo	HP 250 G6, WIN 10 PRO		×				×				×		
34	Hardware	Gestión Humana	Equipo de Computo	Secretaria Administrativa - Despacho - Dirección de Recursos Físicos	Técnico Operativo	DELL OPTIPLEX 745, WIN PRO		×				×				×		
35	Hardware	Gestión Humana	Equipo de Computo	Secretaria Administrativa - Despacho - Dirección de Recursos Físicos	Técnico Operativo	DELL VOSTRO 2205, WIN VISTA		×				×				×		
36	Hardware	Gestión Humana	Equipo de Computo	Secretaria Administrativa - Dirección de Talento Humano	Auxiliar Administrativo	HP PRODESK 400, WIN 7 PRO		×				×				×		
37	Hardware	Gestión Humana	Equipo de Computo	Secretaria Administrativa - Dirección de Talento Humano	Director	HP COMPAQ 6000 PRO, WIN10 PRO		×				×				×		
38	Hardware	Gestión Humana	Equipo de Computo	Secretaria Administrativa - Dirección de Talento Humano	Profesional Universitario	DELL OPTIPLEX 3020, WIND7 PRO		×				×				×		
39	Hardware	Gestión Humana	Equipo de Computo	Secretaria Administrativa - Dirección de Talento Humano	Asesor	DELL VOSTRO 2205, WIN7 VISTA		×				×				×		
40	Hardware	Gestión Humana	Equipo de Computo	Secretaria Administrativa - Dirección de Talento Humano	Técnico Operativo	HP COMPAQ ELITE 8300, WIN 7 PRO		×				×				×		
41	Hardware	Gestión Humana	Equipo de Computo	Secretaria Administrativa - Dirección de Talento Humano	Técnico Operativo	DELL OPTIPLEX 3020, WIND7 PRO		×				×				×		
42	Hardware	Gestión Humana	Equipo de Computo	Secretaria Administrativa - Dirección de Talento Humano	Técnico Operativo	HP COMPAQ PRO 6300, WIN 10 PRO		×				×				×		
43	Hardware	Gestión de Infraestructura Tecnológica	Servidor - Plataforma PISAMI	Secretaría de las TIC - Grupo Infraestructura Tecnológica	Profesional Universitario	DELL PowerEdge R510, Linux CentOS 7	×				×				×			
44	Hardware	Gestión de Infraestructura Tecnológica	Servidor - Plataforma PISAMIV2 (Soporte	Secretaría de las TIC - Grupo Infraestructura Tecnológica	Profesional Universitario	HP Proliant DL180 GEN9, Windows 2016 Server	×				×				×			
45	Hardware	Gestión de Infraestructura Tecnológica	Router	Secretaría de las TIC - Grupo Infraestructura Tecnológica	Técnico Operativo		×				×				×			
46	Hardware	Gestión de Infraestructura Tecnológica	Switches - Clientes	Secretaría de las TIC - Grupo Infraestructura Tecnológica	Técnico Operativo	ArubaOS-Switch, ARUBA 2530 24G	×				×				×			
47	Hardware	Gestión de Infraestructura Tecnológica	Switches - Enlaces Trunk entre SW.	Secretaría de las TIC - Grupo Infraestructura Tecnológica	Técnico Operativo	ArubaOS-Switch, ARUBA 2530 24G	×				×				×			
48	Hardware	Gestión de Infraestructura Tecnológica	Switches - CORE	Secretaría de las TIC - Grupo Infraestructura Tecnológica	Técnico Operativo	HUAWEI S5720, vr200910c00spc600b221	×				×				×			
49	Hardware	Gestión de Infraestructura Tecnológica	Impresora	Secretaría de las TIC - Grupo Ciencia, Tecnología e Innovación	Profesional Universitario	HP LASERJET M1212NF		×				×				×		
50	Hardware	Gestión de Infraestructura Tecnológica	Impresora	Secretaría de las TIC - Grupo Infraestructura Tecnológica	Profesional Universitario	HP LASERJET ENTERPRISE M608		×				×				×		
51	Hardware	Gestión Humana	Impresora	Secretaria Administrativa - Despacho	Secretaria de Despacho	HP LASERJET PRO MFP M426FDW		×				×				×		
52	Hardware	Gestión de Infraestructura Tecnológica	Impresora	Secretaría de las TIC	Secretaria de Despacho	HP LASERJET P4515x		×				×				×		
53	Hardware	Gestión Documental	Impresora	Secretaria Administrativa - Despacho - Dirección de Recursos Físicos	Director	LASERJET 600 M603		×				×				×		
54	Hardware	Gestión Documental	Impresora	Secretaria Administrativa - Despacho - Dirección de Recursos Físicos	Técnico Operativo	HP OFFICEJET PRO 8600		×				×				×		
55	Hardware	Gestión Humana	Impresora	Secretaria Administrativa - Dirección de Talento Humano	Director	HP LASERJET M1522N		×				×				×		
56	Hardware	Gestión Humana	Impresora	Secretaria Administrativa - Dirección de Talento Humano	Técnico Operativo	KYOCERA FS-1035MFP		×				×				×		
57	Red	Gestión de Infraestructura Tecnológica	Red Local	Secretaría de las TIC - Grupo Infraestructura Tecnológica	Técnico Operativo	Topología de Red Estrella	×				×				×			
58	Red	Gestión de Infraestructura Tecnológica	Firewalls	Secretaría de las TIC - Grupo Infraestructura Tecnológica	Técnico Operativo	Rendimiento superior de firewall para IPv4 / IPv6, SCTP y multicifusión	×				×				×			
59	Red	Gestión de Infraestructura Tecnológica	Wi-fi	Secretaría de las TIC - Grupo Infraestructura Tecnológica	Técnico Operativo	Aruba AP-303	×				×				×			
60	Red	Gestión de Infraestructura Tecnológica	Wi-fi	Secretaría de las TIC - Grupo Infraestructura Tecnológica	Técnico Operativo	Aruba AP-303	×				×				×			
61	Red	Gestión de Infraestructura Tecnológica	Telefonía IP	Secretaría de las TIC - Grupo Infraestructura Tecnológica	Técnico Operativo	Unify OpenScape Business X8		×	×			×				×		
62	Personal	Alcaldía de Ibagué	Funcionarios de Planta	Secretarios, Directores, Profesionales Universitarios, Técnicos Operativos, Asesores,	NA	(Provisionalidad, Carrera Administrativa, Libre nombramiento y Remisión			×				×				×	
63	Personal	Alcaldía de Ibagué	Clientes Externo	NA	NA	Comunidad que efectúa radicación de P.Q.R			×				×				×	
64	Personal	Alcaldía de Ibagué	Contratistas	NA	NA	Contrato OPS diferentes dependencias de la Administración Municipal			×				×				×	
65	Personal	Alcaldía de Ibagué	Proveedores	NA	NA	Prestación de Servicio de Aseo, Vigilancia, Correo Certificado, Contratos Suministros			×				×				×	
66	Instalaciones	Alcaldía de Ibagué	Palacio Municipal	Secretaría de las TIC		Oficinas de Mantenimiento, Desarrollo, Innovación y Despacho			×				×				×	
67	Instalaciones	Alcaldía de Ibagué	Palacio Municipal	Secretaría Administrativa		Oficinas Dirección de Recursos Físicos, Dirección de Talento Humano, Despacho			×				×				×	
68	Instalaciones	Alcaldía de Ibagué	Palacio Municipal	Secretaría de las TIC		Ubicación Datacenter y UPS				×				×			×	
69	Equipamiento Auxiliar	Gestión de Infraestructura Tecnológica	UPS	Secretaría de las TIC		Marca PEI, 15KVA		×				×				×		

ANEXO G

MATRIZ IDENTIFICACIÓN Y CLASIFICACIÓN DE ACTIVOS
ALCALDÍA MUNICIPAL DE IBAGUÉ

SIGLA	TIPO DE ACTIVO	ACTIVO	CANT	UBICACIÓN	OBSERVACION
[D] DATOS INFORMACIÓN					
[fikes]	Ficheros	Datos Correspondencia Interna y Externa		Secretaría de la TIC, Grupo Ciencia, Tecnología e Innovación	
[backu]	Copias de Respaldo	Copias de Seguridad		Secretaría de la TIC, Ciencia, Tecnología e Innovación	Copias: Sistemas de Información - Servidores Virtuales
[conf]	Datos de Configuración	Configuración de Equipos Propios del Centro		Secretaría de la TIC, Ciencia, Tecnología e Innovación	Servidores, Equipos y otros
[int]	Datos de Gestión Interna	Bases de Datos		Secretaría de la TIC, Ciencia, Tecnología e Innovación	Sistema de Registro y Control
[password]	Credenciales	Contraseñas		Secretaría de la TIC, Ciencia, Tecnología e Innovación	Acceso a la Plataforma PISAMI.
[acl]	Datos de Control de acceso	Datos de Control de Acceso del Cento		Secretaría de la TIC, Ciencia, Tecnología e Innovación	Asignación de Permisos.
[K] CLAVES CRIPTOGRÁFICAS					
[inf]	Protección de la Información	Protección de la Información Correos Institucionales		Secretaría de la TIC, Grupo de Infraestructura Tecnologica	
[com]	Protección de las Comunicaciones	Protección de las Comunicaciones - Voz IP		Secretaría de la TIC, Grupo de Infraestructura Tecnologica	
		Protección de las Comunicaciones - Wifi		Secretaría de la TIC, Grupo de Infraestructura Tecnologica	
[S] SERVICIOS					
[int]	Interno	Servicios de Impresión		Secretaría de la TIC, Grupo de Infraestructura Tecnologica	
[int]	Interno	Servicio Soporte Técnico		Secretaría de la TIC, Grupo de Infraestructura Tecnologica	
[www]	World Wide Web	Servicios Pagina Web Institucional	1	Secretaría de la TIC, Grupo de Infraestructura Tecnologica	dominio1.edu.co
[email]	Correo Electronico	Servicio Correo Electronico - Google Sites	1	Secretaría de la TIC, Grupo de Infraestructura Tecnologica	correodominio1@.edu.co
[ftp]	Trasnferencia de Ficheros	Transferencia de Archivos		Secretaría de la TIC, Grupo de Infraestructura Tecnologica	
[idm]	Gestión de identidades	Gestión de usuarios y Contraseñas		Secretaría de la TIC, Grupo de Infraestructura Tecnologica	
[SW] APLICACIONES (SOFTWARE)					
[prp]	Desarrollo Propio	Plataforma PISAMI	1	Secretaría de la TIC, Ciencia, Tecnología e Innovación	http://pisami.ibague.gov.co
[std]	Estandar	PHP y Larabel	1	Secretaría de la TIC, Ciencia, Tecnología e Innovación	
[browser]	Navegador Web	Apache	1	Secretaría de la TIC, Ciencia, Tecnología e Innovación	
[app]	Servidor de Aplicaciones	Windows 2016 Server Linux Centos 7		Secretaría de la TIC, Ciencia, Tecnología e Innovación	
[file]	Servidor de ficheros	Joomla V.2.5		Secretaría de la TIC, Ciencia, Tecnología e Innovación	
[dbms]	Sistema de Gestión de Bases de Datos	Bases de Datos MySQL	1	Secretaría de la TIC, Ciencia, Tecnología e Innovación	
		Oracle 10G	1	Secretaría de la TIC, Ciencia, Tecnología e Innovación	
[av]	Anti virus	Avira		Secretaría de la TIC, Ciencia, Tecnología e Innovación	
[os]	Sistema Operativo	Windows 10 Pro		Secretaría de la TIC, Ciencia, Tecnología e Innovación	
[HW] EQUIPOS INFORMÁTICOS (HARDWARE)					
[host]	Grandes Equipos	Servidor de Archivos FTP - Marca: DELL en Torre PowerEdge T130	1	Antigua Oficina de Sistemas	Administración de almacenamiento y administracion de archivos. Solo puede acceder al Servidor personas autorizadas.
		Servidor DHCP - Marca: Dell en Torre PowerEdge T440	1	Antigua Oficina de Sistemas	
		Servidor DHCP - Marca: Dell en Torre PowerEdge T440	1	Antigua Oficina de Sistemas	
[mid]	Equipos Medios	Equipos de Computo	1	Secretaría de las TIC - Despacho	
		Equipos de Computo	6	Grupo de Ciencia, Tecnologia e Innovación	
		Equipos de Computo	2	Grupo de Infraestructura Tecnológica	
		Equipos de Computo	1	Secretaría Adminitrativa	
		Equipos de Computo	8	Grupo de Recursos Fisicos	
		Grupo de Talento Humano	7	Grupo de Talento Humano	
[peripheral]	**Periféricos**				
[print]	Medios de Impresión	Impresora Marca: HP LASERJET M1212NF	1	Secretaría de las TIC - Grupo Ciencia, Tecnología e Innovación	Se establece conexión entre más PC
		Impresora Marca: HP LASERJET ENTERPRISE M608	1	Secretaría de las TIC - Grupo Infraestructura Tecnológica	
		Impresora Marca: HP LASERJET PRO MFP M426FDW	1	Secretaría Administrativa - Despacho	
		Impresora Marca: HP LASERJET P4515x	1	Secretaría de las TIC	
		Impresora Marca: LASERJET 600 M603	1	Secretaría Administrativa - Despacho - Dirección de Recursos Físicos	
		Impresora Marca: HP OFFICEJET PRO 8600	1	Secretaría Administrativa - Despacho - Dirección de Recursos Físicos	
		Impresora Marca: HP LASERJET M1522N	1	Secretaría Administrativa - Dirección de Talento Humano	
		Impresora Marca: KYOCERA FS-1035MFP	1	Secretaría Administrativa - Dirección de Talento Humano	
[network]	**Soporte de la Red**				
[hub]	Concentradores	Puntos de Acceso Alámbricos		Red de Datos - Centro	Interconexión de la red de datos.
[switch]	Conmutadores	Swtches: Marca ArubaOS-Switch, ARUBA 2530 24G	6	Red de Datos - Secretaría Administrativa	Interconexión de la red de datos.
[firewall]	Cortafuegos	Cortafuegos Cisco ASA 5505	1	Secretaría de las TIC	Proteccion a la Red de Datos.
[wab]	Punto de acceso Inalámbrico	Puntos de Acceso	2	Secretaría de las TIC	Puntos de acceso servicio internet Alcaldía de Ibagué
[ipphone]	Teléfono IP	Teléfono IP	6	Dependencias	Voz IP - Comuncación Despacho Secretarias y Direcciones.
[COM] REDES DE COMUNICACIONES					
[ISDN]	Red Digital	Sistema Comunicación Voz IP		Palacio Municipal de Ibagué	
[wifi]	Red Inalámbrica	Red Inalámbrica - Institucional		Palacio Municipal de Ibagué	
[LAN]	Red Local	Red Local Institucional		Palacio Municipal de Ibagué	
[Internet]	Internet	Internet Centro		Palacio Municipal de Ibagué	
[Media] SOPORTES DE INFORMACIÓN					
[vdisk]	Discos Virtuales	Cloud Plus		Departamento de Sistemas	
[AUX] EQUIPAMIENTO AUXILIAR					
[ups]	Sistemas e Alimentación Ininterrumpida	UPS del Centro		Datacenter	
[cabling]	Cableado	Cableado Electrico		Palacio Municipal de Ibagué	
[cabling]	Cableado	Cableado Estructurado		Palacio Municipal de Ibagué	
[L] INSTALACIONES					
[building]	Edificio	Instalaciones Palacio		Palacio Municipal de Ibagué	Oficina Secretaría de las TIC (Despacho y Grupos), Secretaria Administrativa (Despacho y Direcciones)
[P] PERSONAL					
[ue]	Usuarios Externos	Comunidad Ibaguereña		Palacio Municipal de Ibagué	
[ui]	Usuarios Internos	Funcionarios de Planta y Contratistas	75	Palacio Municipal de Ibagué	Secretaría de las TIC (Despacho y Grupos), Secretaria Administrativa (Despacho y Direcciones)
[adm]	Administradores de Sistemas	Técnicos/Auxiliares de Mantenimiento	2	Secretaría de las TIC, Grupo Infraestructura Tecnológica	
[des]	Desarrolladores / Programadores	Profesionales		Secretaría de las TIC, Grupo de Ciencia, Tecnología e Innovació	Desarrollo de Plataforma PISAMI
[prov]	Proveedores	Servicio Web: MEDIA COMMERCE PARTNERS	1	Secretaría de las TIC	Plan Máximo
		Servicio Correo Institucional: ITO SOFTWARE SAS	1	Secretaría de las TIC	dominio @ibague.gov.co

ANEXO H

ACTIVO	VULNERABILIDAD	AMENAZAS [N] Desastres Naturales	[I] De Origen Industrial	Errores y fallos no intencionad	[A] Ataques Intencionados.
[D] DATOS INFORMACIÓN					
[D] - Datos Correspondencia Interna y Externa	Posible falta de conocimiento en el ingreso de la información en las bases de datos por parte de los funcionarios responsables.	NA	NA	[E.1] Errores de los Usuarios [I] [C] [D] [E.2] Errores del Administrador [I] [C] [D] [E.4] Errores de Configuración [I] [E.15] Alteración accidental de la información. [I] [E.18] Destrucción de información [D] [E.19] Fugas de información. [C]	[A.3] Manipulacion de los registros de actividad (Log) [I] [A.4] Manipulación de la Configuración. [I] [C] [D] [A.11] Acceso no Autorizado. [I] [C] [A.13] Repudio [I] [A.15] Modificación deliberada de la información. [I] [A.18] Destrucción de información. [D] [A.19] Divulgación de información [C]
[D] - Copias de Seguridad	Omisión de copias de seguridad en los PC de las diferentes dependencias.				
[D] - Configuración de Equipos Propios de la Administración.	No se implementaron o no se da uso adecuado de los controles de acceso a los Servidores de Bases de Datos.				
[D] - Bases de Datos	Ausencia de actualización de los sistemas de base de datos y de parches de seguridad en los diferentes equipos de computo de las dependencias.				
[D] - Contraseñas	Se evidencia falta de validación de las contraseñas, no solicita la combinación de caracteres alfanuméricos en la contraseña				
[D] - Datos de Control de Acceso.	No se cuenta con auditorias periódicas y monitoreo adecuado del estado de la información				
[K] CLAVES CRIPTOGRÁFICAS					
[K] - Protección de la Información Correos Institucionales	No se cuenta con los niveles de seguridad adecuados para la protección de la información financiera.	NA	NA	[E.1] Erroresde los Usuarios [C] [D] [I] [E.2] Errores del Administrador. [C] [I] [D] [E.15] Alteración accidental de la información. [I]. [E.18] Destrucción de información [D] [E.19] Fugas de información. [C]	[A.5] Suplantación de la identidad del Usuario. A. I.C [A.6] Abuso de Privilegios de acceso. [C][I][D] [A.11] Acceso no autorizado. [C][I] [A.15] Modificación deliberada de la información. [I] [A.18] Destrucción de información. [D]
[K] - Protección de las Comunicaciones - Voz IP	La eventual inexperiencia del personal de practica de otras dependencias, encargado de la alimentación de la información en el sistema, puede provocar en el ingreso erróneo de la información				
[K] - Protección de las Comunicaciones - Wifi	Presencia de exceso de privilegios y mala disposición de niveles de acceso para la información.				
[S] SERVICIOS					
[S] - Servicios de Impresión	Ausencia de Politicas de Control de Acceso correspondiente a los Servidores de Bases de Datos.	NA	NA	[E.1] Errores de los Usuarios [I] [C] [D] [E.2] Errores del Administrador [I] [C] [D] [E.9] Errores de [re-]encaminamiento. [C] [E.10] Errores de Secuencia. [I] [E.15] Alteración accidental de la información. [I] [E.18] Destrucción de información [D] [E.19] Fugas de información. [C] [E.24] Caída del Sistema por Agotamiento de Recursos. [D] [E.25] Pérdida de Equipos. [D][C]	[A.5] Suplantación de la Identidad del Usuario. [A.6] Abuso de Privilegios de acceso. [C][I][D] [A.7] Uso no previsto. [C][I][D] [A.9] [Re-]encaminamiento de mensajes.[C] [A.10] Alteración de Secuencia. [I] [A.11] Acceso no autorizado. [C][I] [A.13] Repudio [I] [A.15] Modificación deliberada de la información. [I] [A.18] Destrucción de información. [D] [A.24] Denegación del Servicio. [D]
[S] - Servicio Soporte Técnico	No se cuenta con auditorias periódicas y monitoreo adecuado del estado de las Bases de Datos.				
[S] - Servicios Pagina Web Institucional (1)	Configuración insuficiente de servidor. Configuración errónea de los parámetros de autenticación.				
[S] - Servicio Correo Electronico - Google Sites (1)	Ineficiente sistema de autenticación y gestor de permisos y permisos.				
[S] - Transferencia de Archivos	Vulnerabilidad presentada en los servidores de Godaddy, frente a un control inadecuado de un alto tráfico.				
[S] - Gestión de usuarios y Contraseñas	Gestión y disposición errónea de las cuentas para los usuarios.				
[SW] APLICACIONES (SOFTWARE)					
[SW] - Plataforma PISAMI (1)	Ausencia de capacitación (Ingeniería Social), concientización y plan de seguridad para los usuarios; que permita un uso adecuado y seguro del servicio.	NA	[I.5] Avería de Origen físico o Lógico [D]	[E.1] Errores de los Usuarios. [D][I][C] [E.2] Errores del Administrador [D][I][C] [E.8] Difusión de Software dañino [D][I][C] [E.9] Errores de [re-]encaminamiento. [C] [E.10] Errores de Secuencia. [I] [E.15] Alteración accidental de la información. [I] [E.18] Destrucción de información. [D] [E.19] Fugas de información. [C] [E.20] Vulnerabilidades de los Programas. [I][D][C] [E.21] Errores de Mantenimiento / Actialización (Software). [I][D]	[A.5] Suplantación de la Identidad del Usuario. [C][A][I]. [A.6] Abuso de Privilegios de acceso. [C][I][D] [A.7] Uso no previsto. [C][I][D] [A.8] Difusión de Software Dañino. [C][I][C]. [A.9] [Re-]encaminamiento de mensajes.[C] [A.10] Alteración de Secuencia. [I] [A.11] Acceso no autorizado. [C][I] [A.15] Modificación deliberada de la información. [I] [A.18] Destrucción de información. [D] [A.19] Divulgación de información. [C] [A.22] Manipulación de Programas. [C][I][D]
[SW] - PHP y Larabel (1)	Daños generados por uso inadecuado del servicio por falta de capacitación del uso adecuado de los herramientas tecnológicas.				
[SW] - Apache (1)	Gestión de la configuración, disposición de accesos al servicio y gestión de capacitaciones para el uso adecuado del servicio				
[SW] - Windows 2016 Server Linux Centos 7	No se realizan las actualizaciones correspondientes y actuales al sistema. No se realiza un eficiente mantenimiento al sistema.				
[SW] - Joomla V.2.5	Instalación ineficiente, deficiente mantenimiento de los equipos.				
[SW] - Bases de Datos MySQL (1)	Configuración inadecuada o errada del protocolo.				
[SW] - Oracle 10G (1)	No se cuentan con los recursos suficientes para cubrir con lo requerido por la organización				
[SW] - Avira	Ineficientes medidas de seguridad implementadas; ausencia en la configuración UTM para la detección de intrusiones, zona desmilitarizada para la protección de los servidores.				
[SW] - Windows 10 Pro	Incorrecta configuración de usuarios y contraseñas. Uso de contraseñas genéricas.				
[HW] EQUIPOS INFORMÁTICOS (HARDWARE)					
[HW] - Servidor de Archivos FTP - Marca: DELL en Torre PowerEdge T130 (1)	No se cuentan disponibilidad suficiente, recursos físico, humano necesario para cubrir con los casos de soporte requeridos por los usuarios organización	[N.1] Fuego [D] [N.2] Daños por Agua [D] [N.10]]Inundación [D]	[I.1] Fuego [D] [I.2] Daños por agua [D] [I.5] Avería de Origen físico o Lógico [D] [I.6] Corte del Suministro eléctrico [D] [I.7] Condiciones inadecuadas de temperatura o humedad [D] [I.11] Emanaciones Electromágneticas.[C]	[E.2] Errores de Administrador [D] [I] [C] [E.23] Errores de Mantenimiento/Actualizacion de equipos [D] [E.24] Caída del Sistema por agotamiento de Recursos.[D] [E.25] Perdida de Equipos. [D]	[A.6] Abuso de Privilegios de Acceso [D] [I] [C] [A.7] Uso no previsto [D] [I] [C] [A.11] Acceso no autorizado [C] [I] [A.23] Manupulacion de Equipos [C] [D] [A.24] Denegacion de Servicio. [D] [A.25] Robo [C] [D] [A.26] Ataque Destructivo [D]
[HW] - Servidor DHCP - Marca: Dell en Torre PowerEdge T440 (1)	Ausencia de configuración de privilegios de aceptación o denegación de conectividad firwall, ineficiente medidas de seguridad.				
[HW] - Servidor DHCP - Marca: Dell en Torre PowerEdge T440 (1)	Uso inadecuado. Ausencia de conocimiento sobre la operabilidad y uso del sistema operativo.				
[HW] - Equipos de Computo (1)	Fallos o vulnerabilidades presentes en la seguridad del sistema. Ausencia de plan de seguridad.				
[HW] - Equipos de Computo (6)	No se realizan las actualizaciones correspondientes y actuales al sistema. No se realiza un eficiente mantenimiento al sistema.				
[HW] - Equipos de Computo (2)	Fallos en la configuración de seguridad del sistema operativo, ausencia de antivirus actualizado				
[HW] - Equipos de Computo (1)	Fallos o vulnerabilidades presentes en la seguridad del sistema. Ausencia de plan de seguridad.				
[HW] - Equipos de Computo (8)	Ausencia en el control de actualizaciones del sistema de seguridad e implantación de parches. No se realiza un eficiente mantenimiento al sistema.				
[HW] - Grupo de Talento Humano (7)	Configuraciones erradas que generan deficiencias en el funcionamiento adecuado del software.				
[HW] - Impresora Marca: HP LASERJET M1212NF (1)	Fallos o vulnerabilidades presentes en la seguridad del sistema. Ausencia de plan de seguridad.				
[HW] - Impresora Marca: HP LASERJET ENTERPRISE M608 (1)	Ausencia en el control de actualizaciones del sistema de seguridad e implantación de parches. No se realiza un eficiente mantenimiento al sistema.				
[HW] - Impresora Marca: HP LASERJET PRO MFP M426FDW (1)	Configuraciones erradas que generan deficiencias en el funcionamiento adecuado del software.				
[HW] - Impresora Marca: HP LASERJET P4515x (1)	Fallos o vulnerabilidades presentes en la seguridad del sistema. Ausencia de plan de seguridad.				
[HW] - Impresora Marca: LASERJET 600 M603 (1)	Ausencia en el control de actualizaciones del sistema de seguridad e implantación de parches. No se realiza un eficiente mantenimiento al sistema.				
[HW] - Impresora Marca: HP OFFICEJET PRO 8600 (1)	Configuraciones erradas que generan deficiencias en el funcionamiento adecuado del software.				
[HW] - Impresora Marca: HP LASERJET M1522N (1)	Ausencia en el control de actualizaciones del sistema de seguridad e implantación de parches. No se realiza un eficiente mantenimiento al sistema.				
[HW] - Impresora Marca: KYOCERA FS-1035MFP (1)	Ausencia en la configuración adecuada de permisos para la aceptación o denegación de conexiones.				
[HW] - Puntos de Acceso Alámbricos	Fallos o vulnerabilidades presentes en la seguridad del sistema. Ausencia de plan de seguridad.				
[HW] - Swtches: Marca ArubaOS-Switch, ARUBA 2530 24G (6)	Ausencia en el control de actualizaciones del sistema de seguridad e implantación de parches. No se realiza un eficiente mantenimiento al sistema.				
[HW] - Cortafuegos Cisco ASA 5505 (1)	Configuraciones erradas que generan deficiencias en el funcionamiento adecuado del software.				
[HW] - Puntos de Acceso (2)	Fallos o vulnerabilidades presentes en la seguridad del sistema. Ausencia de plan de seguridad.				
[HW] - Teléfono IP (6)	Ausencia en el control de actualizaciones del sistema de seguridad e implantación de parches. No se realiza un eficiente mantenimiento al sistema.				
[COM] REDES DE COMUNICACIONES					
[ISDN] Sistema Comunicación Voz IP	Configuraciones erradas que generan deficiencias en el funcionamiento adecuado del software.		[I.8] Fallo de Servicios de Comunicaciones. D	[E.2] Errores del Administrador [D][I][C] [E.9] Errores de [re-]encaminamiento. [C] [E.10] Errores de Secuencia. [I] [E.15] Alteración accidental de la información. [I]	[A.5] suplantación de la Identidad del Usuario. [C][A][I] [A.6] Abuso de Privilegios de Acceso [D] [I] [C] [A.7] Uso no previsto [D] [I] [C] [A.9] [Re-]encaminamiento de mensajes.[C]
[wifi] Red Inalámbrica - Institucional	Ausencia de sistema de Seguridad adecuado				
[LAN] Red Local Institucional	Ausencia de encapsulamiento de protocoles.				
[Internet] Internet Palacio	Fallas relacionadas con el internet, intermitencia, por daños en la infraestructura o inutilidad del mismo				
[Media] SOPORTES DE INFORMACIÓN					
[vdisk] Cloud Plus	Intermitencia del servicio por fallas.	[N.1] Fuego [D] [N.2] Daños por Agua [D] [N.10]]Inundación [D]	[I.1] Fuego [D] [I.2] Daños por agua [D] [I.5] Avería de Origen físico o Lógico [D] [I.6] Corte del Suministro eléctrico [D] [I.7] Condiciones inadecuadas de temperatura o humedad [D] [I.10] Degradación de los soportes de almacenamiento de la información [D] [I.11] Emanaciones Electromágneticas.[C]	[E.1] Errores de los Usuarios. [D][I][C] [E.2] Errores del Administrador [D][I][C] [E.15] Alteración accidental de la información. [I] [E.18] Destrucción de información. [D] [E.19] Fugas de información. [C] [E.23] Errores de Mantenimiento/Actualizacion de equipos [D] [E.25] Pérdida de Equipos. [D][C]	[A.7] Uso no previsto [D] [I] [C] [A.11] Acceso no autorizado. [C][I] [A.15] Modificación deliberada de la información. [I] [A.18] Destrucción de información. [D] [A.23] Manupulacion de Equipos [C] [D]. [A.25] Robo [C] [D] [A.26] Ataque Destructivo [D]
[AUX] EQUIPAMIENTO AUXILIAR					
[AUX] - UPS del Alcaldía	Falta de conocimiento en la manipulación de los dispositivos	[N.1] Fuego [D] [N.2] Daños por Agua [D] [N.10]]Inundación [D]	[I.1] Fuego [D] [I.2] Daños por agua [D] [I.5] Avería de Origen físico o Lógico [D] [I.6] Corte del Suministro eléctrico [D] [I.7] Condiciones inadecuadas de temperatura o humedad [D] [I.9] Interrupción de Otros Servicios Suministros [D]. [I.11] Emanaciones Electromágneticas.[C]	[E.23] Errores de Mantenimiento/Actualizacion de equipos [D] [E.24] Caída del Sistema por Agotamiento de Recursos. [D] [E.25] Pérdida de Equipos. [D][C]	[A.7] Uso no previsto [D] [I] [C] [A.11] Acceso no autorizado. [C][I] [A.23] Manupulacion de Equipos [C] [D] [A.25] Robo [C] [D] [A.26] Ataque Destructivo [D]
[AUX] - Cableado Electrico	Deterioro total o parcial del cableado incluido equipos conectados al mismo.				
[AUX] - Cableado Estructurado	Daños por uso e instalación inadecuado.				
[L] INSTALACIONES					
[L] - Instalaciones Palacio	Falta de un Sistema Biometrico o de monitoreo para el acceso a las instalaciones y dependencias de acceso restringido.	[N.1] Fuego [D] [N.2] Daños por Agua [D] [N.10]]Inundación [D]	[I.1] Fuego [D] [I.2] Daños por agua [D] [I.11] Emanaciones Electromágneticas.[C]	[E.15] Alteración accidental de la información. [I] [E.18] Destrucción de información. [D] [E.19] Fugas de información. [C]	[A.7] Uso no previsto [D] [I] [C] [A.11] Acceso no autorizado. [C][I] [A.15] Modificación deliberada de la información. [I] [A.18] Destrucción de información. [D]. [A.19] Divulgación de información. [C]. [A.26] Ataque Destructivo [D]. [A.27] Ocupación Enemiga. [D][C]
[P] PERSONAL					
[P] - Funcionarios de Planta y Contratistas (75)	Susceptibilidad de los servidores públicos a ser obligados para ejecutar actos inicuos en contra la Administración Municipal.			[E.7] Deficiencias en la Organización. [D] [E.15] Alteración accidental de la información. [I] [E.19] Fugas de información. [C] [E.28] Indisponibilidad del Personal. [D]	[A.28] Indisponibilidad del Personal [D] [A.29] Extorsión. [C][I][D] [A.30] Ingeniería Social. [C][I][D].
[P] - Funcionarios de Planta y Contratistas (75)	Deficiencia en el monitoreo sobre el uso adecuado de la información publicada en la Plataforma PISAMI y el control de acceso a los datos, carencia de LOGS de auditoria.				
[P] - Funcionarios de Planta y Contratistas (75)	Ausencia del personal por incapacidades medicas a a causa del COVID 19, y deficiencia en los procesos contractuales para la contratación de nuevo personal.				
[P] - Técnicos/Ausxiliares de Mantenimiento (2)	Ausencia del personal por incapacidades medicas a a causa del COVID 19, y deficiencia en los procesos contractuales para la contratación de nuevo personal.				
[P] - Técnicos/Ausxiliares de Mantenimiento (2)	Susceptibilidad de los servidores públicos a ser obligados para ejecutar actos inicuos en contra la Administración Municipal.				
[P] - Profesionales	Susceptibilidad de los servidores públicos a ser obligados para ejecutar actos inicuos en contra la Administración Municipal.				
[P] - Profesionales	Ausencia del personal por incapacidades medicas a a causa del COVID 19, y deficiencia en los procesos contractuales para la contratación de nuevo personal.				
[P] - Servicio Web: MEDIA COMMERCE PARTNERS (1)	Suministro de información a terceros mediante amenazas.				
[P] - Servicio Correo Institucional: ITO SOFTWARE SAS (1)	Entrega de información confidencial a terceros por presión mediante extorsión				

ANEXO I

OBJETIVO	Realizar la identificación, análisis y evaluación de los activos y riesgos de seguridad de la información del departamento de sistemas de la compañía.
ALCANCE	Aplica para los activos de la Secretaría y la Secretaría Administrativa
Nombre de la Empresa:	**Alcaldía Municipal de Ibagué**
Sitio web:	www.ibague.gov.co
CONTEXTO LEGAL	ISO 31000 y la ISO 27001:2013
ENFOQUE METODOLOGICO	El enfoque de gestión de riesgos a aplicar está basado en la metodología **MAGERIT**
TRATAMIENTO	Se tratarán los riesgos cuyos niveles sean:
	[MODERADO]
	16 a 26 INACEPTABLE(I)
	Se aceptarán los riesgos cuyo resultado después de la valoración de riesgos sean:
	[INDIQUE EL NIVEL A ACEPTAR] Eje. **ACEPTABLE** **MODERADO**
	Niveles de aceptación del riesgo (1 a 5 aceptable (A), 6 a 15 moderado (M), 16 a 26 inaceptable(I))
	Una vez aplicados los controles se acepta un riesgo de residual en niveles **APRECIABLE** o **IMPORTANTE**
	Criticidad residual (1 a 4 despreciable (d), 5 a 9 baja (B), 10 a 15 apreciable (a), 16 a 20 importante (i), 21 a 25 crítico(C))

Continuación Anexo I

MATRIZ DE LEVANTAMIENTO DE INFORMACIÓN DE ACTIVOS
SEGÚN METODOLOGÍA MAGERIT Y NORMA ISO 27001:2013

Empresa: Alcaldía Municipal de Ibagué

LEVANTAMIENTO DE INFORMACIÓN, INVENTARIO Y Clasificación DE ACTIVOS - SEGURIDAD DE LA INFORMACIÓN

1	Nombre Entrevistado 1:	Claudia Patricia Guillen	Cargo	Técnico Operativo	Proceso	Proceso Gestión de Documental
2	Nombre Entrevistado 2:	Jaime Orlando Jaramillo	Cargo	Profesional Universitario	Proceso	Ciencia, Tecnología e Innovación
3	Nombre Entrevistado 3:	Jhon Fredy Lugo Luna	Cargo	Profesional Universitario	Proceso	Infraestructura Tecnologica
4	Nombre Entrevistado 4:	Edwin Ferney Castro	Cargo	Técnico Operativo	Proceso	Ciencia, Tecnología e Innovación
5	Nombre Entrevistado 5:	Richard Rodriguez Romero	Cargo	Técnico Operativo	Proceso	Infraestructura Tecnologica

INFORMACIÓN DE LOS ACTIVOS

No.	DATOS DEL ACTIVO DE INFORMACIÓN			DIMENSIÓN					ATRIBUTOS									UBICACIÓN	
	Nombre del activo de información	Proceso propietario del activo	Responsable	Dimensión Autenticidad (A) ¿ Alto (A) Medio (M) Bajo (B) ?	Dimensión Trazabilidad (T) ¿ Alto (A) Medio (M) Bajo (B) ?	Dimensión Confidencialidad (C ¿ Alto (A) Medio (M) Bajo (B) ?	Dimensión Integridad (I ¿ Alto (A) Medio (M) Bajo (B) ?	Dimensión Disponibilidad (D ¿ Alto (A) Medio (M) Bajo (B) ?	¿Existe otra información de terceros cuyo cliente que debe ¿ protegerse?	¿Activo de información que debe ser restringido a un número bajo ¿ de empleados?	Activo de información que debe ser restringido a personas ¿ específicas?	Activo de información que puede ser afectado o comprometido para fraudes o ¿ corrupción	Activo de información cuyo mayor crítico para las ¿ actividades internas	Activo de información cuyo mayor crítico para el envío ¿ a clientes?	Activo de información que en caso de ser conocido, utilizado o modificado por alguna persona o sistema sin la debida autorización, impactaría negativamente a los sistemas y/o procesos de la empresa, de manera:			Físico	Electrónico
															Leve	Importante	Grave		
1	[D] - Datos Correspondencia Interna y Externa	Secretaría de la TIC, Grupo Ciencia, Tecnología e Innovación	Profesional Universitario	B	B	B	B	B	SI	SI	SI	SI	SI	SI		X			X
2	[D] - Copias de Seguridad	Secretaría de la TIC, Ciencia, Tecnología e Innovación	Profesional Universitario	B	B	MA	MA	MA	NO	SI	SI	SI	SI	SI		X			X
3	[D] - Configuración de Equipos Propios del Palacio	Secretaría de la TIC, Ciencia, Tecnología e Innovación	Técnico Operativo	B	B	B	B	B	NO	SI	SI	SI	SI	SI			X		X
4	[D] - Bases de Datos	Secretaría de la TIC, Ciencia, Tecnología e Innovación	Profesional Universitario	B	B	MA	MA	MA	NO	SI	SI	SI	SI	SI			X		X
5	[D] - Contraseñas	Secretaría de la TIC, Ciencia, Tecnología e Innovación	Profesional Universitario	B	B	B	B	B	NO	SI	SI	SI	SI	SI			X		X
6	[D] - Datos de Control de Acceso.	Secretaría de la TIC, Ciencia, Tecnología e Innovación	Profesional Universitario	B	B	B	B	B	NO	SI	SI	SI	SI	SI			X		X
7	[K] - Protección de la Información Correos Institucionales	Secretaría de la TIC, Grupo de Infraestructura Tecnológica	Profesional Universitario	B	B	B	B	B	NO	SI	SI	SI	SI	SI			X		X
8	[K] - Protección de las Comunicaciones - Voz IP	Secretaría de la TIC, Grupo de Infraestructura Tecnológica	Profesional Universitario	B	B	B	B	B	NO	NO	NO	NO	NO	NO	X			X	X
9	[K] - Protección de las Comunicaciones - Wifi	Secretaría de la TIC, Grupo de Infraestructura Tecnológica	Profesional Universitario	B	B	B	B	B	NO	NO	NO	NO	NO	NO	X			X	X
10	[S] - Servicios de Impresión	Secretaría de la TIC, Grupo de Infraestructura Tecnológica	Técnico Operativo	B	B	B	B	B	NO	NO	NO	NO	NO	NO	X			X	X
11	[S] - Servicio Soporte Técnico	Secretaría de la TIC, Grupo de Infraestructura Tecnológica	Técnico Operativo	B	B	B	B	B	NO	NO	NO	NO	NO	NO	X			X	X
12	[S] - Servicios Pagina Web Institucional (1)	Secretaría de la TIC, Grupo de Infraestructura Tecnológica	Profesional Universitario	A	B	MA	MA	MA	NO	SI	SI	SI	SI	SI			X		X
13	[S] - Servicio Correo Electrónico - Google Sites (1)	Secretaría de la TIC, Grupo de Infraestructura Tecnológica	Profesional Universitario	M	MB	A	A	M	SI	SI	SI	SI	SI	NO			X		X
14	[S] - Transferencia de Archivos	Secretaría de la TIC, Grupo de Infraestructura Tecnológica	Técnico Operativo	MB	MB	MA	MA	MA	NO	SI	SI	SI	NO	NO		X			
15	[S] - Gestión de usuarios y Contraseñas	Secretaría de la TIC, Grupo de Infraestructura Tecnológica	Técnico Operativo	B	B	A	MA	MA	NO	SI	SI	SI	SI	SI			X		X
16	[SW] - Plataforma PISAMI (1)	Secretaría de la TIC, Ciencia, Tecnología e Innovación	Profesional Universitario	B	B	A	MA	MA	NO	SI	SI	SI	SI	SI			X		X
17	[SW] - PHP y Larabel (1)	Secretaría de la TIC, Ciencia, Tecnología e Innovación	Profesional Universitario	B	B	A	MA	MA	NO	SI	SI	SI	SI	SI			X		X
18	[SW] - Apache (1)	Secretaría de la TIC, Ciencia, Tecnología e Innovación	Profesional Universitario	B	B	MA	MA	MA	NO	SI	SI	SI	SI	SI			X		X
19	[SW] - Windows 2016 Server Linux Centos 7	Secretaría de la TIC, Ciencia, Tecnología e Innovación	Técnico Operativo	MB	MB	MA	MA	MA	NO	SI	NO	SI	SI	SI			X		X
20	[SW] - Joomla V.2.5	Secretaría de la TIC, Ciencia, Tecnología e Innovación	Profesional Universitario	MB	MB	MA	MA	MA	NO	SI	SI	SI	NO	NO		X			X
21	[SW] - Bases de Datos MySQL (1)	Secretaría de la TIC, Ciencia, Tecnología e Innovación	Profesional Universitario	B	B	A	MA	MA	NO	SI	SI	SI	SI	SI			X		X
22	[SW] - Oracle 10G (1)	Secretaría de la TIC, Ciencia, Tecnología e Innovación	Profesional Universitario	B	B	A	MA	MA	NO	SI	SI	SI	SI	SI			X		X
23	[SW] - Avira	Secretaría de la TIC, Ciencia, Tecnología e Innovación	Técnico Operativo	B	B	MA	MA	MA	NO	SI	SI	NO	SI	NO			X		X
24	[SW] - Windows 10 Pro	Secretaría de la TIC, Ciencia, Tecnología e Innovación	Técnico Operativo	MB	MB	MA	MA	MA	NO	SI	NO	SI	SI	SI			X		X
25	[HW] - Servidor de Archivos FTP - Marca: DELL en Torre PowerEdge T130 (1)	Antigua Oficina de Sistemas	Profesional Universitario	B	B	A	A	MA	NO	SI	SI	NO	NO	SI	X			X	
26	[HW] - Servidor DHCP - Marca: Dell en Torre PowerEdge T440 (1)	Antigua Oficina de Sistemas	Profesional Universitario	B	B	A	A	MA	NO	SI	SI	NO	NO	SI	X			X	
27	[HW] - Servidor DHCP - Marca: Dell en Torre PowerEdge T440 (1)	Antigua Oficina de Sistemas	Profesional Universitario	B	B	A	A	MA	NO	SI	SI	NO	NO	SI	X			X	
28	[HW] - Equipos de Computo (1)	Secretaría de las TIC - Despacho	Secretaria de Despacho	MB	MB	A	A	MA	NO	SI	SI	SI	SI	SI			X	X	
29	[HW] - Equipos de Computo (6)	Grupo de Ciencia, Tecnología e Innovación	Funcionarios Dependencia	B	B	B	B	MA	NO	SI	NO	NO	NO	NO	X			X	
30	[HW] - Equipos de Computo (2)	Grupo de Infraestructura Tecnología	Funcionarios Dependencia	B	B	B	B	MA	NO	SI	NO	NO	NO	NO	X			X	
31	[HW] - Equipos de Computo (1)	Secretaría Administrativa	Secretaria de Despacho	B	B	B	B	MA	NO	SI	NO	NO	NO	NO	X			X	
32	[HW] - Equipos de Computo (8)	Grupo de Recursos Físicos	Funcionarios Dependencia	B	B	B	B	MA	NO	SI	NO	NO	NO	NO	X			X	
33	[HW] - Grupo de Talento Humano (7)	Grupo de Talento Humano	Funcionarios Dependencia	B	B	B	B	MA	NO	SI	NO	NO	NO	NO	X			X	
34	[HW] - Impresora Marca: HP LASERJET M1212NF (1)	Secretaría de las TIC - Grupo Ciencia, Tecnología e Innovación	Funcionarios Dependencia	MB	MB	MB	MB	MA	NO	SI	SI	NO	NO	NO	X			X	
35	[HW] - Impresora Marca: HP LASERJET ENTERPRISE M608 (1)	Secretaría de las TIC - Grupo Infraestructura Tecnológica	Funcionarios Dependencia	MB	MB	MB	MB	MA	NO	SI	SI	NO	NO	NO	X			X	
36	[HW] - Impresora Marca: HP LASERJET PRO MFP M426FDW (1)	Secretaría Administrativa - Despacho	Secretaria de Despacho	MB	MB	MB	MB	MA	NO	SI	SI	NO	NO	NO	X			X	
37	[HW] - Impresora Marca: HP LASERJET P4515x (1)	Secretaría de las TIC	Funcionarios Dependencia	MB	MB	MB	MB	MA	NO	SI	SI	NO	NO	NO	X			X	
38	[HW] - Impresora Marca: LASERJET 600 M603 (1)	Secretaría Administrativa - Despacho - Dirección de Recursos Físicos	Funcionarios Dependencia	MB	MB	MB	MB	MA	NO	SI	SI	NO	NO	NO	X			X	
39	[HW] - Impresora Marca: HP OFFICEJET PRO 8600 (1)	Secretaría Administrativa - Despacho - Dirección de Recursos Físicos	Funcionarios Dependencia	MB	MB	MB	MB	MA	NO	SI	SI	NO	NO	NO	X			X	
40	[HW] - Impresora Marca: HP LASERJET M1522N (1)	Secretaría Administrativa - Dirección de Talento Humano	Funcionarios Dependencia	MB	MB	MB	MB	MA	NO	SI	SI	NO	NO	NO	X			X	
41	[HW] - Impresora Marca: KYOCERA FS-1035MFP (1)	Secretaría Administrativa - Dirección de Talento Humano	Funcionarios Dependencia	MB	MB	MB	MB	MA	NO	SI	SI	NO	NO	NO	X			X	
42	[HW] - Puntos de Acceso Alámbricos	Red de Datos - Palacio	Técnico Operativo	B	B	A	A	MA	NO	SI	SI	SI	SI	SI		X		X	
43	[HW] - Switches: Marca ArubaOS-Switch, ARUBA 2530 24G (6)	Red de Datos - Secretaría Administrativa	Técnico Operativo	B	B	A	A	MA	NO	SI	SI	SI	SI	SI		X		X	
44	[HW] - Cortafuegos Cisco ASA 5505 (1)	Secretaría de las TIC	Técnico Operativo	MB	MB	A	A	MA	NO	SI	SI	SI	SI	SI			X	X	
45	[HW] - Puntos de Acceso (2)	Secretaría de las TIC	Técnico Operativo	B	B	A	A	MA	NO	SI	SI	SI	SI	SI		X		X	
46	[HW] - Teléfono IP (6)	Dependencias	Técnico Operativo	B	B	A	A	A	NO	NO	SI	NO	NO	SI	X				X
47	[COM] - Sistema Comunicación Voz IP	Palacio Municipal de Ibagué	Técnico Operativo	B	B	A	A	MA	NO	SI	NO	NO	SI	SI		X			X
48	[COM] - Red Inalámbrica - Institucional	Palacio Municipal de Ibagué	Técnico Operativo	B	B	A	B	A	NO	SI	NO	NO	NO	NO	X			X	
49	[COM] - Red Local Institucional	Palacio Municipal de Ibagué	Técnico Operativo	B	B	MA	MA	MA	NO	SI	SI	NO	SI	SI			X	X	
50	[COM] - Internet Palacio	Palacio Municipal de Ibagué	Técnico Operativo	B	B	MA	MA	MA	NO	SI	SI	NO	SI	SI			X	X	
51	[Media] - Cloud Plus	Departamento de Sistemas	Técnico Operativo	B	B	MA	MA	MA	NO	NO	NO	SI	SI	SI			X	X	
52	[AUX] - UPS del Palacio	Datacenter	Técnico Operativo	B	B	B	B	MA	NO	SI	SI	NO	SI	SI			X	X	
53	[AUX] - Cableado Eléctrico	Palacio Municipal de Ibagué	Técnico Operativo	B	B	B	B	MA	NO	SI	SI	NO	SI	SI			X	X	
54	[AUX] - Cableado Estructurado	Palacio Municipal de Ibagué	Técnico Operativo	B	B	B	B	MA	NO	SI	SI	NO	SI	SI			X	X	
55	[L] - Instalaciones Palacio	Palacio Municipal de Ibagué	Funcionarios Dependencia	B	B	A	A	A	NO	SI	NO	SI	SI	SI		X		X	
57	[P] - Funcionarios de Planta y Contratistas (75)	Palacio Municipal de Ibagué	NA	B	B	A	A	MA	NO	NO	SI	SI	SI	NO		X		X	
58	[P] - Técnicos/Auxiliares de Mantenimiento (2)	Secretaría de las TIC, Grupo Infraestructura Tecnología	NA	B	B	A	A	MA	NO	NO	SI	SI	SI	NO		X		X	
59	[P] - Profesionales	Secretaría de las TIC, Grupo de Ciencia, Tecnología e Innovación	NA	B	B	A	A	MA	NO	NO	SI	SI	SI	NO		X		X	
60	[P] - Servicio Web: MEDIA COMMERCE PARTNERS (1)	Secretaría de las TIC	NA	B	B	MA	MA	MA	NO	NO	NO	SI	SI	SI			X	X	
61	[P] - Servicio Correo Institucional: ITO SOFTWARE SAS (1)	Secretaría de las TIC	NA	B	B	MA	MA	MA	NO	NO	NO	SI	SI	SI			X	X	

ANEXO J

Estructura del documento para la estructura del Resumen Analítica Especializado - RAE

Fecha de Realización:	20/10/2021
Programa:	Especialización en Seguridad Informática
Línea de Investigación:	Gestión de Sistemas.
Título:	Análisis de los riesgos de seguridad de la información del sistema de gestión documental de la alcaldía municipal de Ibagué
Autor(es):	Alba Denys Valencia Bautista
Palabras Claves:	Amenazas, Riesgos, Seguridad, Vulnerabilidades, MARGERIT
Descripción:	La presente opción de grado "*Proyecto Aplicado",* se planteó con el fin de mostrar los conocimientos adquiridos en cuanto Seguridad Informática; para este caso se determinó dar uso de la metodología MARGERIT y bajo la norma ISO 27001, para con ello, identificar los activos (hardware y software) que evidencien vulnerabilidades y sobre las mismas proponer control y gestión que las minimice. Dicho proceso servirá de apoyo para demostrar la importancia de contar con un sistema que cumpla a cabalidad con los pilares de la seguridad, asentados en la Norma Internacional ISO 27001:2016 y la ISO 31000 que tiene como fin de garantizar, la integridad, disponibilidad y confidencialidad de la información, evitando así la materialización de ataques, perdida de información, fallas en la ejecución de los procesos, entre otros. De esta manera, el proyecto aplicado planteado, propenderá por el desarrollo de los siguientes objetivos: - Aplicar la metodología MARGERIT para la evaluación de riesgos que permita identificar vulnerabilidades y amenazas de seguridad, así como evaluar los riesgos conforme lo establece la metodología. - Proponer mecanismos de control y gestión que reduzcan las vulnerabilidades identificadas en el análisis realizado. - Elaborar informe de hallazgos y recomendaciones que permita precisar un Sistema de Seguridad de la información

Continuación Anexo J

	concreta a la realidad de la Alcaldía Municipal de Ibagué. Buscando cumplir con el objetivo principal el cual es: Analizar los riesgos de seguridad de la información del Sistema de Gestión Documental de la Alcaldía Municipal de Ibagué, aplicando la metodología MAGERIT la cual está asociada con las normas ISO 31000 y la ISO 27001:2013.

Fuentes bibliográficas destacadas:

ARCHIVO GENERAL DE LA NACIÓN – AGN. Glosario [Consulta: 17 de mato de 2021]. Disponible en: https://www.archivogeneral.gov.co/Transparencia/informacion-interes/Glosario

ARCHIVO GENERAL DE LA NACIÓN. [Sitio Web]. Bogotá: AGN, Acuerdo 003 de 2015 [Consulta: 01 de mayo de 2021]. Disponible en: https://normativa.archivogeneral.gov.co/acuerdo-003-de-2015/

ARCHIVO GENERAL DE LA NACIÓN. [Sitio Web]. Bogotá: AGN, Ley 527 de 1999 [Consulta: 01 de mayo de 2021]. Disponible en: https://normativa.archivogeneral.gov.co/ley-527-de-1999/

ARCHIVO GENERAL DE LA NACIÓN. [Sitio Web]. Bogotá: AGN, Ley 594 de 2000 [Consulta: 01 de mayo de 2021]. Disponible en: https://normativa.archivogeneral.gov.co/ley-594-de-2000/.

ARCHIVO GENERAL DE LA NACIÓN. Ley 1712 de 2014. [Sitio Web]. Bogotá: AGN. [Consulta: 01 de mayo de 2021]. Disponible: https://normativa.archivogeneral.gov.co/ley-1712-de-2014/

CENTRO DE INNOVACIÓN PÚBLICA DIGITAL. Iniciativa Cero Papel MINTIC [Consulta: 17 de mato de 2021]. Disponible: https://centrodeinnovacion.mintic.gov.co/es/experiencias/iniciativa-cero-papel-mintic

EALDE BUSINESS SCHOOL. Gestión del Riesgo. Que es la norma ISO 3100 y para qué sirve. [Sitio Web] Madrid: EALDE. [Consulta 01 de mayo de 2021]. Disponible en: https://www.ealde.es/iso-31000-para-que-sirve/.

Continuación Anexo J

GOBIERNO EN LÍNEA. Buenas Prácticas para reducir el consumo de papel. [Sitio Web] Bogotá: [Consulta: 01 de mayo de 2021]. Disponible: https://estrategia.gobiernoenlinea.gov.co/623/articles-8257_papel_buenaspracticas.pdf.

INCIVBE-CERT. Inventario de Activos y Gestión de Seguridad en SCI. [Sitio Web] España. [Consulta 18 de mayo de 2021] Disponible en: https://www.incibe-cert.es/blog/inventario-activos-y-gestion-seguridad-sci

INSTITUTO COLOMBIANO DE NORMAS TÉCNICAS Y CERTIFICACIÓN. ICONTEC. Norma Técnica Colombiana NTC-ISO/IEC 27002, Bogotá: 2007.p.3.

INSTITUTO COLOMBIANO DE NORMAS TÉCNICAS Y CERTIFICACIÓN. ICONTEC. Norma Técnica Colombiana NTC-ISO/IEC 27002, Bogotá: 2007.p.2

ISO.es. Controles ISO 27002-2013. [Sitio Web] https://www.iso27000.es [Consultado 29 de septiembre de 2021]. Disponible en: https://www.iso27000.es/assets/files/ControlesISO27002-2013.pdf

MININTERIOR. [Sitio Web]. Bogotá: Mapa de Riesgos [Consulta: 01 de mayo de 2021]. Disponible en: https://www.mininterior.gov.co/content/mapa-de-riesgos

MINTIC. Guía para la Gestión y Clasificación de Activos de la Información. [Sitio Web] Bogotá: EALDE. [Consulta 17 de mayo de 2021]. Disponible en: https://www.mintic.gov.co/gestionti/615/articles-5482_G5_Gestion_Clasificacion.pdf

NORMA ISO 27001. [Sitio Web]. Madrid: Referencias Normativas Iso 27000 [Consulta: 01 de mayo de 2021]. Disponible en: https://normaiso27001.es/referencias-normativas-iso-27000/#def36

NORMA ISO 27001. [Sitio Web]. Madrid: Referencias Normativas Iso 27000 [Consulta: 01 de mayo de 2021]. Disponible en: https://normaiso27001.es/referencias-normativas-iso-27000/#def310.

NORMA ISO 27001. [Sitio Web]. Madrid: Referencias Normativas Iso 27000 [Consulta: 01 de mayo de 2021]. Disponible en: https://normaiso27001.es/referencias-normativas-iso-27000/#def336.

NORMA ISO 27001. [Sitio Web]. Madrid: Referencias Normativas Iso 27000 [Consulta: 01 de mayo de 2021]. Disponible en: https://normaiso27001.es/referencias-normativas-iso-27000/#terminos

Continuación Anexo J

NORMA ISO 27001. [Sitio Web]. Madrid: Referencias Normativas Iso 27000 [Consulta: 01 de mayo de 2021]. Disponible en: https://normaiso27001.es/referencias-normativas-iso-27000/#def37.	
Contenido del documento:	En el presente proyecto Aplicado, se encontrará información relacionada a la norma ISO 27001, Aplicación Metodología MARGERIT, así como información general del Sistema de Información del proceso de Gestión Documental, el cual es ejecutado en la Plataforma PISAMI.
Marco Metodológico:	Para el desarrollo del presente proyecto, se plantea el siguiente marco metodológico: Para el desarrollo de los objetivos planteados en el presente proyecto, se realizará la metodología MAGERIT (Gobierno de España) la cual está asociada con las normas ISO 31000 y la ISO 27001:2013, dicha metodología contas de un conjunto de actividades por etapas (Inicio, análisis y diseño) enfocadas fin alcanzar los resultados del proyecto propuesto. • ETAPA INICIO: PLANTEAMIENTO DE LA PROPUESTA. • ETAPA ANÁLISIS: RECOLECCIÓN DE INFORMACIÓN. • ETAPA DISEÑO:
Conceptos adquiridos:	Después del desarrollo del trabajo de grado
Conclusiones:	El implementar la metodología MARGERIT, basados en la Norma Internacional ISO 27001:2016, permite a la entidad contar con información acertada y precisa de las vulnerabilidades a las que esta propenso el Sistema de Gestión Documental, generando con ello mayor facilidad para la toma de decisiones y soluciones enfocadas en controles y políticas que conlleven a mejorar el nivel de seguridad de la Información. Teniendo como resultado el análisis realizado con la metodología MARGERIT, se propuso mecanismos de control y gestión, establecidos en la Norma Internacional ISO 27001:2016, los cuales le permitirán a la Alcaldía de Ibagué, reducir las vulnerabilidades identificadas en su

Continuación Anexo J

	Sistema de Gestión Documental, propendiendo por la protección y tratamiento de los datos. De acuerdo a los resultados obtenidos en la aplicación de la metodología MARGERIT, se puedo determinar que la Alcaldía Municipal de Ibagué, en su Sistema de Gestión Documental, cuenta con una serie de hallazgos los cuales se plasmaron en un informe ejecutivo el cual le permitirá contar con una información concreta del estado actual de sus Sistema de Seguridad, de esta manera se planteó una serie de recomendaciones que le permitirán mejorar de manera significativa dicho resultado.