INSTITUCIÓN UNIVERSITARIA POLITÉCNICO GRANCOLOMBIANO
FACULTAD DE INGENIERÍA Y CIENCIAS BÁSICAS
ESPECIALIZACIÓN EN SEGURIDAD DE LA INFORMACIÓN
GRUPO DE INVESTIGACIÓN FICB-PG

DISEÑO DEL SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN (SGSI) PARA LA ADMINISTRACIÓN MUNICIPAL DEL MUNICIPIO DE LA CEJA ANTIOQUIA, BAJO LOS LINEAMIENTOS EMITIDOS POR EL PROGRAMA G.E.L (GOBIERNO EN LÍNEA).

PRESENTA

ARIEL AUGUSTO TOBÓN MEJÍA
Cod. 1712010419

ASESOR TEMÁTICO
WILMAR JAIMES FERNÁNDEZ
Ingeniero

Mayo de 2018

CONTENIDO

LISTA DE TABLAS

LISTA DE ILUSTRACIONES

RESUMEN

La realización de este proyecto tiene como propósito diseñar el Sistema de Gestión de seguridad de la Información (SGSI) para la administración municipal del municipio de La Ceja-Antioquia bajo los lineamientos de MINTIC y en especial el uso de del estándar ISO 27001:2013 y la aplicación de la metodología para el análisis de riegos Magerit.

El estándar ISO 27001:2013 ha sido elaborado para brindar un modelo para el establecimiento, implementación, operación, seguimiento, revisión, mantenimiento y mejora de un sistema de gestión de la seguridad de la información, además le permitirá a la entidad la evaluación del riesgo y la aplicación de los controles necesarios para mitigarlos o eliminarlos.

El diseño del SGSI para la entidad, se convertirá en el marco de referencia para su implementación siguiendo las mejores prácticas de estándares de seguridad como las norma ISO 27001:2013 y mediante la aplicación de una metodología de análisis de riegos como punto central de una estrategia de seguridad de la información, la cual permitirá identificar cuáles son los activos más importantes de la entidad, amenazas, vulnerabilidades y riegos de la información, con el fin de generar un plan de implementación de los controles que aseguren un ambiente informático seguro, bajo los criterios de disponibilidad, confidencialidad e integridad de la información.

Palabras claves: Sistema de Gestión de seguridad de la Información (SGSI), NTC-ISO/IEC 27001:2013, metodología para el análisis de riegos, plan de continuidad del negocio.

ABSTRAC

The purpose of this project is to design the Information Security Management System (ISMS) for the municipal administration of the municipality of La Ceja-Antioquia under the guidelines of MINTIC and especially the use of the ISO 27001: 2013 standard and the application of the methodology for the risk analysis Magerit.

The ISO 27001: 2013 standard has been developed to provide a model for the establishment, implementation, operation, monitoring, review, maintenance and improvement of an information security management system, in addition to allowing the entity to assess the risk and the application of the necessary controls to mitigate or eliminate them.

The design of the ISMS for the entity will become the reference framework for its implementation following the best practices of security standards such as ISO 27001: 2013 and by applying a risk analysis methodology as the central point of a strategy of information security, which will identify which are the most important assets of the entity, threats, vulnerabilities and risks of information, in order to generate a plan for the implementation of controls that ensure a secure computing environment, under the criteria of availability, confidentiality and integrity of information.

Keywords: Information Security Management System (SGSI), NTC-ISO / IEC 27001: 2013, methodology for irrigation analysis, business continuity plans.

INTRODUCCIÓN

Las Tecnologías de Información y Comunicaciones (TIC) son recursos esenciales para la productividad y competitividad de las organizaciones; sin embargo, como cualquier recurso, está sujeto a múltiples amenazas que se pueden materializar en riesgos, con múltiples consecuencias.

Según la investigación realizada por la firma Infométrika Ltda. Para el Ministerio de Tecnologías de la Información, cuatro de cada diez entidades públicas no han implementado sistemas de gestión de la seguridad de la información. ("W3-Article-5414 @ Www.Mintic.Gov.Co," n.d.)

El Ministerio de Tecnologías de la Información y las Comunicaciones "MINTIC en su página web describe "*Un Sistema de Gestión de la Seguridad de la Información le garantiza a las entidades públicas el uso correcto de la información para prevenir que sea utilizada en escenarios inseguros o dañinos"*.

Las entidades territoriales, no encuentran las oportunidades ni han logrado identificar las necesidades para dedicar recursos al tema de la seguridad, sin dejar de mencionar que la escasez de recursos y capacitación retrasan la adopción de sistemas de seguridad.

Con la transformación de la Estrategia de Gobierno en Línea a política de Gobierno Digital, se genera un nuevo enfoque en donde no sólo el Estado sino también los diferentes actores de la sociedad, son actores fundamentales para un desarrollo integral del Gobierno Digital en Colombia y en donde las necesidades y problemáticas del contexto determinan el uso de la tecnología y la forma como ésta puede aportar en la generación de valor público. En este sentido, el nuevo objetivo de la política de Gobierno Digital es el siguiente:

"Promover el uso y aprovechamiento de las tecnologías de la información y las comunicaciones para consolidar un Estado y ciudadanos competitivos, proactivos, e innovadores, que generen valor público en un entorno de confianza digital" ("W3-Article-5414 @ Www.Mintic.Gov.Co," n.d.)

El decreto 2573 de 2014 de Ministerio de Tecnologías de la Información y Comunicaciones, tiene como **objeto**: "*Definir los lineamientos, instrumentos y plazos de la estrategia de Gobierno en Línea para garantizar el máximo aprovechamiento de las Tecnologías de la Información y las Comunicaciones, con el fin de contribuir con la construcción de un Estado abierto, más eficiente, más transparente y más participativo y que preste mejores servicios con la colaboración de toda la sociedad.*

En su **Ámbito de aplicación**. Serán sujetos obligados de las disposiciones contenidas en el presente Decreto las entidades que conforman la Administración Pública en los términos del artículo 39 de la Ley 489 de 1998 y los particulares que cumplen funciones administrativas. [1]

La alcaldía de El municipio de La Ceja – Antioquia, como sujeto obligado del orden Territorial para el cumplimento del decreto 2573, diseñara e implementará un Sistema de Gestión de Seguridad de la Información (SGSI) de acuerdo a la política de gobierno en línea, buscando preservar la confidencialidad, integridad y disponibilidad de los activos de información de la entidad, garantizando su buen uso y la privacidad de los datos, a través de un sistema de gestión de seguridad de la información, cuyo objetivo primordial será la mejora continua y la toma de acciones tanto preventivas como correctivas dentro de una cultura de la seguridad y de buenas prácticas en cuanto al manejo de la información y de sus activos actuando en concordancia con la legislación de la Ley de Protección de Datos Personales, Transparencia y Acceso a la Información Pública, entre otras, las cuales se deben tener en cuenta para la gestión de la información.

[1] DECRETO 2573 DE 2014: Por el cual se establecen los lineamientos generales de la Estrategia de Gobierno en línea, se reglamenta parcialmente la Ley 1341 de 2009 y se dictan otras disposiciones

1 PLANTEAMIENTO DEL PROBLEMA

1.1 ANTECEDENTES DEL PROBLEMA

En la actualidad la alcaldía del municipio de La Ceja – Antioquia, no cuenta con un Sistema de Gestión de Seguridad e la Información (SGSI), que le permita validar, supervisar, controlar y prevenir de ataques y delitos informáticos a los que puede ser objeto.

La entidad no cuenta con un documento base que le permita garantizar la confidencialidad, integridad y disponibilidad de la información como uno de sus activos más importantes.

los controles, medidas, procedimientos de seguridad necesarios para resguardar sus activos de información, tales como documentos, software, dispositivos físicos, personas, imagen, reputación y servicios, los cuales están expuestos a altos niveles de riesgos, frente a las diversas amenazas físicas y lógicas existentes:

- Desastres naturales (Tormentas, rayos, terremotos, inundaciones, etc)
- Estructurales (Incendios, inundaciones, humedad, cortes de electricidad, agua, refrigeración, comunicaciones, etc).
- Hardware (Fallo total o parcial de Servidores, UPS, Estaciones PC, portátiles, etc).
- Software (Errores en los SO, BD, software base, Web servers, aplicaciones, elementos de seguridad, etc).
- Red LAN
- Copias de seguridad (Fallos en elementos de copias, fallos en soportes, discos, unidades USB, etc)
- Información (Bases de datos, ficheros, manuales, procedimientos, planes de contingencia, etc).
- Personal (Errores y ataques de personal interno, externo, funciones, perfiles, formación, etc).
- Riesgos contra el patrimonio (Robo, pérdida no intencionada de activos, etc).
- Otros riesgos (Terrorismo, confianza de los clientes, imagen de entidad, insolvencia de servicios externos, seguros, etc).

Aun cuando el decreto 2573 de 2014, el Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC) y la Estrategia de Gobierno en línea establecen lineamientos para el Sistema de Gestión de Seguridad de la Información (SGSI) para

las entidades públicas del orden territorial, la alcaldía del Municipio de La Ceja no ha iniciado con la implementación del mismo.

Es importante destacar que las administraciones locales se vinculan permanentemente con los contribuyentes. Este es un tema que va más allá de lo político, debido a que se relaciona con el manejo de información. Esto nos plantea el tema del ciudadano, es decir, un mayor cuidado en relación a información privilegiada y privada.

1.2 FORMULACIÓN DEL PROBLEMA

¿Cuenta la alcaldía del municipio de La Ceja - Antioquia, con un Sistema Gestión de Seguridad de la información (SGSI), de tal forma que pueda determinar las necesidades objetivas, los requisitos de seguridad, procesos, el tamaño y la estructura de la misma, todo con el objetivo de preservar la confidencialidad, integridad, disponibilidad de los activos de información, garantizando su buen uso y la privacidad de los datos?

1.3 DESCRIPCIÓN O RESUMEN DEL PROBLEMA

Las Tecnologías de Información y Comunicaciones (TIC) son recursos esenciales para la productividad y competitividad de las organizaciones; sin embargo, como cualquier recurso, está sujeto a múltiples amenazas que se pueden materializar en riesgos, con múltiples consecuencias.

Hoy en día las amenazas tecnológicas son parte de nuestra cotidianidad y más aún de la vida organizacional, las cuales van desde diversas formas de virus, pasando por los recientes ataques de ransomware hasta amenazas sofisticadas como los ataques día cero (en inglés, zero-day attack) lo cual requiere la implementación de controles que puedan ser gestionados a través de un adecuado enfoque de seguridad de la información. (Valencia Duque & Orozco-alzate, 2017).

La seguridad de la información es una disciplina asociada tradicionalmente a la gestión de TIC, cuyo propósito es mantener niveles aceptables de riesgo de la información organizacional y de los dispositivos tecnológicos que permiten su recolección, procesamiento, acceso, intercambio, almacenamiento, transformación y adecuada presentación, todo ello ha sido definido por la norma ISO/IEC 27000 como la preservación de la confidencialidad, integridad y disponibilidad de la información (ISO/IEC, 2014).

“Lograr una gestión más eficiente y comprometida con los resultados, implica transformaciones importantes en el funcionamiento de las instituciones públicas; requiere entre otras cosas, desarrollar liderazgos que impulsen el cambio, a incorporar nuevas técnicas de gestión, a establecer metas medibles de desempeño, todo ello dentro de un marco de participación y compromiso de los integrantes de la una administración municipal” (“manual-del-sistema-integrado-de-gestin-organizacional-sigo-1-.pdf,” n.d.)

El Sistema Integrado de Gestión Organizacional “SIGO” de la administración municipal de La Ceja, en su presentación invita a desarrollar liderazgos que impulsen el cambio y a incorporar nuevas técnicas de gestión que permitan al ciudadano una relación más integra con las entidad. Este es el fin último del uso de la tecnología en la relación del Estado y el ciudadano. El valor público se relaciona con el desarrollo social, la gobernanza, la garantía de derechos, la satisfacción de necesidades y la prestación de servicios de calidad. No sólo es hacer uso de las tecnologías, sino cómo las tecnologías ayudan a resolver problemas reales.

“*Por otro lado, la confianza digital es la principal característica del entorno en donde se relaciona el Estado con los ciudadanos y los demás actores del ecosistema digital. Este entorno debe ser sencillo, corresponsable, previsible y seguro. Debe permitir un diálogo permanente entre los actores del ecosistema y proporcionar medios digitales ágiles, sencillos y útiles para el ciudadano*”.(Ministerio de Tecnologías de la Información y las Comunicaciones, n.d.)

Debido a los múltiples riesgos y amenazas que se generan por el cambio constante y dinámico que enmarca la evolución de las tecnología de la información, es necesario que las organizaciones cuenten con una estrategia seguridad basado en los riesgos y a su vez alineada con las necesidades del negocio, con el objetivo de contar con un Sistemas de Gestión de la Seguridad de la Información que apoye y apalanque los objetivos estratégicos de la organización.

El propósito de un sistema de gestión de la seguridad de la información es, por tanto, garantizar que los riesgos de la seguridad de la información sean conocidos, asumidos, gestionados y minimizados por la organización de una forma documentada, sistemática, estructurada, repetible, eficiente y adaptada a los cambios que se produzcan en los riesgos, el entorno y las tecnologías.

La seguridad de la información, según ISO 27001, consiste en la preservación de su confidencialidad, integridad y disponibilidad, así como de los sistemas implicados en su tratamiento, dentro de una organización. Así pues, estos tres términos constituyen la base sobre la que se cimienta todo el edificio de la seguridad de la información:

- **Confidencialidad:** la información no se pone a disposición ni se revela a individuos, entidades o procesos no autorizados.
- **Integridad**: mantenimiento de la exactitud y completitud de la información y sus métodos de proceso.
- **Disponibilidad**: acceso y utilización de la información y los sistemas de tratamiento de la misma por parte de los individuos, entidades o procesos autorizados cuando lo requieran.

Para garantizar que la seguridad de la información es gestionada correctamente, se debe hacer uso de un proceso sistemático, documentado y conocido por toda la organización, desde un enfoque de riesgo empresarial. Este proceso es el que constituye un SGSI.

La alcaldía de La Ceja ha sido certificada y recertificada por varios años en las normas

- Norma Técnica ISO 9001:2000;
- NTC GP1000:2004;

La implementación del SGSI por parte de la entidad contribuirá al incremento de la transparencia en la Gestión Pública, promoviendo el uso de las mejores prácticas de Seguridad de la Información como base de la aplicación del concepto de Seguridad Digital y mejorara los procesos que en la actualidad se encuentran certificados por el ICONTEC.

Como consecuencias de no poseer un SGSI:

- ✓ Se tiene un municipio:
  - Menos Eficiente.
  - Menos transparente
  - Menos participativo
- ✓ No hay cumplimento de las ley en cuanto a la protección de los datos de los contribuyentes de acuerdo a la legislación actual.
- ✓ En la actualidad no se gestionan los riesgos, ni las amenazas, ni las vulnerabilidades a los que se enfrenta los activos de información de la entidad.
- ✓ No se han establecidos medidas que permitan mitigar los riesgos relacionados con los activos involucrados en el procesamiento y almacenamiento de la información.

2 OBJETIVOS

2.1 OBJETIVO GENERAL

Diseñar el sistema de gestión de seguridad de la información SGSI, alineado con la norma ISO/IEC 27001:2013 y la política de Gobierno Digital para la alcaldía municipal de La Ceja - Antioquia

2.2 OBJETIVOS ESPECÍFICOS

- Implementar una Política de Seguridad de Información que sea desplegada a todos los funcionarios, contratistas, proveedores y terceros involucrados en los procesos llevados a cabo en la alcaldía municipal de La Ceja - Antioquia.

- Gestionar y monitorear de manera eficiente los incidentes y vulnerabilidades de seguridad de la información, para reducirlos en un 80%.

- Desplegar las medidas de seguridad para gestionar los riesgos y ejecutar controles de tratamiento de riesgos, para reducir el 90% de los riesgos a niveles aceptables.

- Formación y concientización al 100% de los funcionarios involucrados en los procesos de seguridad de la información tanto física como lógica, en temas de seguridad de información.

- Cumplimiento de la legislación vigente sobre información personal, propiedad intelectual y otras.

- Lograr procesos internos seguros y eficientes a través del fortalecimiento de las capacidades de gestión de tecnologías de información.

- Habilitar y mejorar la provisión de Servicios Digitales de confianza y calidad.

- Gestionar y controlar el 100% de los documentos del SGSI.

3 JUSTIFICACIÓN

La información es un activo esencial para las organizaciones y es decisiva para la viabilidad de las mismas. La información adopta diferentes formas, impresa, escrita en papel, digital, trasmitida por correo, mostrada en videos o hablada en conversaciones, debido a que está disponible en ambientes cada vez más interconectados, está expuesta a amenazas y vulnerabilidades, mantener su integridad, confidencialidad y disponibilidad es esencial para alcanzar los objetivos de la organización.

La información de administración municipal de La Ceja-Antioquia sin importar el tipo, es crucial para el desarrollo de su objeto misional, su correcto desempeño dentro de la política pública y su relación con el ciudadano, es por ello que debe ser protegida de cualquier posibilidad de ocurrencia de eventos de riesgo de seguridad de la información y que pudiese significar un impacto indeseado generando una consecuencia negativa para el normal progreso de las actividades de la entidad.

El decreto 2693 de diciembre 2012 definió los lineamientos plazos y términos que las entidades territoriales deberían cumplir para garantizar el máximo aprovechamiento de las tecnologías de la información y las comunicaciones, con el fin de contribuir con la construcción de un Estado más eficiente, más trasparente y participativo y que prestara mejores servicios con la colaboración de toda la sociedad.

El decreto 2693 es su artículo 8. Implementación de la Estrategia de gobierno en línea, definió los tiempos y las acciones de cada uno de los componentes que implica gobierno en línea.

“Para alcaldías de categorías cuarta, quinta y sexta, la Administración Pública y demás sujetos obligados en el mismo orden”

Ver. Tabla Nro. 1

Tabla 1 - Fechas para la implementación de la estrategia GEL

Año	Información en línea	Interacción en línea	Transacción en línea	Transformación	Democracia en línea	Transversales
2013	40%	25%	15%	15%	40%	35%
2014	55%	50%	35%	35%	65%	60%
2016	80%	75%	70%	60%	95%	85%
2017	100%	100%	100%	100%	100%	100%

Fuente: http://programa.gobiernoenlinea.gov.co/apc-aa-files/eb0df10529195223c011ca6762bfe39e/manual-3.1.pdf

De acuerdo a esta tabla, el municipio de La Ceja para el año 2017 implemento en su totalidad la estrategia, pero adicional a esta implementación, el manual para la implementación de la estrategia gobierno en línea en las entidades del orden nacional y territorial de la república de Colombia en su versión 3.1, las entidades deben realizar las siguientes actividades con el fin de alcanzar sus objetivos

- Institucionalizar la estrategia de gobierno en línea
- Centrar la atención en el usuario
- Implementar un sistema de gestión de tecnología de información.
- Implementar un sistema de gestión de seguridad de la Información (SGSI)

Igualmente según el tipo de entidad estatal se establecen plazos entre 2015 y 2017 para cumplimento de las acciones establecidas en cada componente

La administración municipal de La Ceja-Antioquia en la actualidad ha incumplido con la implementación de SGSI, la cual es una herramienta o metodología sencilla y de bajo coste que le permitirá a la entidad establecer políticas, procedimientos y controles con el objeto de disminuir los riesgos en sus activos de información.

Con la implementación de un SGSI la entidad se asegura del cumplimiento de la legislación vigente, además, un SGSI implica crear un plan de diseño, implementación, y mantenimiento de una serie de procesos que permitirán gestionar de manera eficiente la información, para asegurar la integridad, confidencialidad y disponibilidad de la misma. y se evitan riesgos y costes innecesarios.

Definir, implementar, operar y mejorar de forma continua un Sistema de Gestión de Seguridad de la Información, soportado en lineamientos claros alineados a las necesidades de la entidad y a los requerimientos regulatorios, además de la actualización de su actual política de seguridad y privacidad de la información, que fue aprobada en el comité del sistema integrado de gestión organizacional en el año 2015, se constituirán en el derrotero a seguir en el uso, protección y manejo de la

información y los recursos tecnológicos por parte de funcionarios, contratistas y particulares que ejercen funciones públicas y su cumplimiento será de carácter obligatorio.

4 ALCANCE

4.1 DEFINICIÓN DEL ALCANCE DEL PROYECTO

El alcance del proyecto inicia con el análisis de cada uno de los riesgos informáticos que han sido identificados por la alcaldía del municipio de La Ceja - Antioquia, la actualización de su política de seguridad actual, hasta el desarrollo de un documento con los pasos para la implementación del sistema de Sistema de Gestión de Seguridad de la información SGSI y Protocolos de Seguridad Informáticos, que le permitan a la Oficina de sistemas de la alcaldía de La Ceja emprender acciones de control y valoración del riesgo informático identificado, así como el cumplimiento de la normatividad y lineamientos del Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC).

El proyecto solo abarcara los procesos:

- ESTRATÉGICOS
- MISIONALES
- DE APOYO

Se excluyen los procesos de EVALUACIÓN

4.2 MAPA DE PROCESOS MUNICIPIO DE LA CEJA ANTIOQUIA

En la administración municipal de La Ceja – Antioquia se lleva a cabo cuatro (4)

ESTRATÉGICOS	Incluyen procesos relativos al establecimiento de políticas y estrategias, fijación de objetivos, provisión de comunicación, aseguramiento de la disponibilidad de recursos necesarios.
MISIONALES	Incluyen todos los procesos que proporcionan el resultado previsto por la entidad en el cumplimiento de su objeto social o razón de ser.
PROCESOS DE APOYO	Incluyen todos aquellos procesos para la provisión de los recursos que son necesarios en los procesos estratégicos, misionales y de mejora continua.
EVALUACIÓN	Incluyen todos aquellos procesos que permiten la evaluación de cada de las metas del plan de desarrollo y los proceso de mejora continua.

Ilustración 1 - Mapa de procesos

Fuente: Autor

4.3 LIMITACIONES DEL PROYECTO

Para el desarrollo del proyecto se presentaron las siguientes limitaciones:

- Disposición de los funcionarios por su carga laboral.
- Disposiciones presupuestales.
- Tiempo de entrega demasiado corto.
- Aprobaciones por las entidades competentes.

5 MARCO DE REFERENCIA

5.1 ESTADO DEL ARTE

5.1.1 La norma ISO 27001: aspectos clave de su diseño e implementación:

La organización isotools en su página web publica un documento denominado “LA NORMA ISO 27001- Aspectos clave de su diseño e implementación, en este documento de describe los aspectos más relevantes del Sistema de Gestión de Seguridad de la Información (SGSI) basado en la norma ISO 27001 y cuyo propósito es garantizar que los riesgos de la seguridad de la información sean conocidos, asumidos, gestionados y minimizados por la organización de una forma documentada, sistemática y estructurada.

5.1.2 Sistemas de Gestión de la Seguridad de la Información (SGSI):

En la página web: http://www.mintic.gov.co/gestionti/615/w3-article-5482.html
El Ministerio de Tecnologías de la Información y las Comunicaciones - MinTIC a través de la Dirección de Estándares y Arquitectura de TI y la Subdirección de Seguridad y Privacidad de TI, dando cumplimiento a sus funciones; publica El Modelo de Seguridad y Privacidad de la Información (MSPI), el cual se encuentra alineado con el Marco de Referencia de Arquitectura TI y soporta transversalmente los otros componentes de la Estrategia GEL: TIC para Servicios, TIC para Gobierno Abierto y TIC para Gestión.

El Modelo de Seguridad y Privacidad para estar acorde con las buenas prácticas de seguridad será actualizado periódicamente; reuniendo los cambios técnicos de la norma 27001 del 2013, legislación de la Ley de Protección de Datos Personales, Transparencia y Acceso a la Información Pública, entre otras, las cuales se deben tener en cuenta para la gestión de la información.

A nivel metodológico es importante tener presente que el (MSPI) cuenta con una serie de guías anexas que ayudarán a las entidades a cumplir lo solicitado permitiendo abordar de manera detallada cada una de las fases del modelo, buscando a su vez comprender cuáles son los resultados a obtener y como desarrollarlos, incluyendo los nuevos lineamientos que permiten la adopción del protocolo IPv6 en el Estado Colombiano.

Mediante la adopción del Modelo de Seguridad y Privacidad por parte de las Entidades del Estado se busca contribuir al incremento de la transparencia en la Gestión Pública, promoviendo el uso de las mejores prácticas de Seguridad de la Información como base de la aplicación del concepto de Seguridad Digital.

5.1.3 Modelo para la implementación de SGSI:

En el año 2016, las estudiantes Ana Milena Pulido Barreto y Jenith Marsella Mantilla Rodríguez en su trabajo de grado para la Universidad Nacional Abierta y a Distancia UNAD denominado "**Modelo para la implementación del sistema general de seguridad informática y protocolos de seguridad informática en la oficina tic de la alcaldía municipal de Fusagasugá, basados en la gestión del riesgo informático** desarrollan a cabo una propuesta académica que le permite a la entidad implementar un Sistema Gestión de Seguridad de la información y protocolos de Seguridad que contribuyan a la Oficina TIC a realizar una mejor gestión y control de los riesgos informáticos que han sido identificados por la entidad.

Este proyecto contribuye al fortalecimiento de los procesos, actividades y servicios que realiza la Oficina TIC de la Alcaldía de Fusagasugá, así como el cumplimiento de lineamientos del Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC), el Modelo de Seguridad y Privacidad de la Información (MSPI) que busca una vez implementado y con índice de madurez alto que la entidad inicie con el requerimiento del Sistema Administrativo de Seguridad de la Información para Gobierno en línea (SASIGEL).

5.1.4 Aplicación de las `TIC` en la administración pública colombiana en línea

En el documento publicado por el Por: William D Ávila, PhD(c) en la página web: http://www.alfa-redi.org/sites/default/files/articles/files/avila.pdf **"Aplicación de las `TIC` en la administración pública colombiana en línea**", realiza una abstracción sobre el uso de las `TIC` en el marco público colombiano, como puente de conexión entre las entidades del sector con la ciudadanía y viceversa. Con esto, le está permitiendo a la nación, renovarse como Estado, mejorar la capacidad de gobernar, promover mayor participación, economizar los recursos públicos, y unificar criterios.

5.1.5 Seguridad en informática (Auditoria de sistemas)

En el año 2005, Luis Daniel Álvarez Basaldúa en su tesis de grado de maestro en ingeniería de sistemas empresariales, centra su trabajo de grado en revisar y evaluar: los procesos de planificación, inversión en tecnología; organización; los controles generales y de aplicación en proyectos de automatización de procesos críticos; el soporte de las aplicaciones; aprovechamiento de las tecnologías; sus controles específicos; los riesgos inherentes a la tecnología; como la seguridad de sus recursos; redes, aplicaciones, comunicaciones, instalaciones y otras.

5.1.6 Diseño e implementas de SGSI en procesos tecnológicos

En el año 2012 Carlos Eduardo Barrantes Porras y Javier Roberto Hugo Herrera en su tesis de grado para la universidad San Martin de Porres en Lima Perú, realizaron el diseño e implementación de un sistema de gestión de seguridad de información en procesos tecnológicos, este trabajo se centró en la implementación de un SGSI bajo una metodología de análisis y evaluación de riegos usando como referencia las norma ISO 27001:2005 e ISO 17799:2005

5.2 MARCO TEÓRICO

5.2.1 Generalidades

En un mundo altamente cambiante y globalizado, como el que tenemos hoy, la información se ha vuelto un elemento fundamental para cualquier organización. De su disponibilidad y precisión dependen decisiones de nivel operativo, táctico y estratégico, que pueden representar la diferencia entre cumplir o no las metas planteadas. Las Tecnologías de Información (TI) son el medio por el cual la información se recoge, administra, almacena, comunica, transforma, visualiza e interpreta, convirtiéndose así en un elemento que puede dar una ventaja competitiva a las organizaciones. Las TI, además de apoyar los procesos de toma de decisiones, permiten automatizar procesos, monitorear el estado del negocio usando indicadores, aplicar estrategias competitivas, posicionar productos o marcas, identificar nuevas oportunidades de negocio y ganar flexibilidad para operar de manera efectiva. Por esta razón, en los últimos años las inversiones en este tipo de tecnologías se han multiplicado en las empresas, con el fin de aprovechar las grandes oportunidades que estas pueden ofrecer. ("ti-organizaciones @ sistemas.uniandes.edu.co," n.d.).

La dependencia de las organizaciones modernas hacia el área de Tecnología de la Información ha crecido dramáticamente durante el último tiempo y promete seguir incrementándose al ritmo de entornos cada vez más desafiantes y competitivos.

Ese aumento tiene varias explicaciones y distintos abordajes. Una primera mirada muestra que cada vez más empresas quieren operar las 24 horas, los 365 días del año, disparando el volumen de datos almacenados, y con él, los costos de seguridad, además, existe una necesidad cada vez mayor de automatizar procesos manuales, suministrar plataformas de información para la toma de decisiones y ahorrar dinero, horas hombre y recursos tecnológicos.

Las empresas quieren ser más rápidas y eficientes, y para ello analizan las mejores opciones de sistemas que se ajusten a su industria y su negocio en particular.

Las nuevas formas y sistemas de trabajo completamente integrados con el uso de las TIC hacen que cada vez más información y datos de todo tipo de especial relevancia para las empresas circulen por internet y se expongan a su robo, manipulación o pérdida. Si tenemos en cuenta que la información es hoy día uno de los principales activos de una gran variedad de empresas, podemos entender que en este contexto la seguridad TIC haya alcanzado la relevancia que tiene. Un fallo en la SEGURIDAD TIC puede provocar pérdidas en una empresa que lleguen incluso a

suponer un riesgo para su continuidad, además de conllevar otra perjuicios como sanciones administrativas, daños irreversibles a su imagen pública, pérdida de clientes por la desconfianza generada, etc. Además, la seguridad TIC es relevante tanto a nivel organizativo como a nivel particular. Según recientes estudios realizados en Europa, cerca del 76% de los usuarios de internet temen ser víctima del cibercrimen, el 12% ha sufrido en algún momento ataques en sus cuentas sociales o de correo electrónico, y el 7% ha sido víctima de algún tipo de fraude online. Por tanto, el desarrollo e implantación de la SEGURIDAD TIC se hace fundamental para el correcto desarrollo e implantación de una gran variedad de servicios online, como el e-commerce o la banca online, ante la reticencia de parte de la sociedad que aún desconfía de este tipo de servicios prestados a través de las TIC. (“la-importancia-de-la-seguridad-en-las-tic @ www.euroinnova.co,” n.d.)

5.2.2 Amenazas informáticas y seguridad de la información:

En la actualidad todas las organizaciones públicas o privadas, al igual que las personas, dependen de alguna manera de la tecnología de la información como una herramienta esencial para lograr sus objetivos de negocio o para poder desarrollar actividades en su vida cotidiana; al mismo tiempo, todos tienen que enfrentarse con una amplia gama de amenazas y vulnerabilidades asociadas a los entornos informáticos de hoy.

La seguridad de la información es más que un problema de seguridad de datos en los computadores; debe estar básicamente orientada a proteger la propiedad intelectual y la información importante de las organizaciones y de las personas.

Los riesgos de la información están presentes cuando confluyen dos elementos: amenazas y vulnerabilidades. Las amenazas y vulnerabilidades están íntimamente ligadas, y no puede haber ninguna consecuencia sin la presencia conjunta de éstas.

Las amenazas deben tomar ventaja de las vulnerabilidades y pueden venir de cualquier parte, interna o externa, relacionada con el entorno de las organizaciones.

Las vulnerabilidades son una debilidad en la tecnología o en los procesos relacionados con la información, y como tal, se consideran características propias de los sistemas de información o de la infraestructura que la contiene. Una amenaza, en términos simples, es cualquier situación o evento que puede afectar la posibilidad de que las organizaciones o las personas puedan desarrollar sus actividades afectando directamente la información o los sistemas que la procesan. (Generales, n.d.)

- **Tipos de amenazas**

Básicamente, podemos agrupar las amenazas a la información en cuatro grandes categorías:

- Factores Humanos (accidentales, errores);
- Fallas en los sistemas de procesamiento de información;
- Desastres naturales y;
- Actos maliciosos o malintencionados;

Algunas de estas amenazas son:

- Virus informáticos o código malicioso
- Uso no autorizado de Sistemas Informáticos
- Robo de Información
- Fraudes basados en el uso de computadores
- Suplantación de identidad
- Denegación de Servicios (DoS)
- Ataques de Fuerza Bruta
- Alteración de la Información
- Divulgación de Información
- Desastres Naturales
- Sabotaje, vandalismo
- Espionaje

5.2.3 Sistema de Gestión de Seguridad de la información SGSI

El SGSI (Sistema de Gestión de Seguridad de la Información) es el concepto central sobre el que se construye ISO 27001.

"La seguridad de la información, según ISO 27001, consiste en la preservación de su confidencialidad, integridad y disponibilidad, así como de los sistemas implicados en su tratamiento, dentro de una organización.

Así pues, estos tres términos constituyen la base sobre la que se cimienta todo el edificio de la seguridad de la información:

- **Funciones y elementos clave de un SGSI**

Como todo sistema, el SGSI debe implementarse de manera estratégica para que los resultados sean acordes con los objetivos propuestos. Si sólo se aplicara parcialmente, no habría garantías para el resto de información proveniente de aquellas secciones o áreas que han quedado sin cobertura.

El Sistema de Seguridad de la Información está basado en tres principios básicos que explicamos a continuación:

- **Confidencialidad**: Es una característica esencial de la información corporativa. Según este principio, los datos internos o que forman parte del

capital de una empresa no se revelan ni se ponen a disposición de terceros individuos, entidades o procesos no autorizados. Son propiedad exclusiva y como tal deben preservarse.

- **Integridad**: La integridad habla de la exactitud y la inalterabilidad de la información, así como de sus métodos de proceso. Esto quiere decir que no deben alterarse ni modificarse bajo ningún fin, salvo que la propia empresa así lo decida y siempre y cuando haya motivos que justifiquen tal medida.

- **Disponibilidad**: El tercer elemento de un SGSI señala la posibilidad de que individuos, entidades o procesos autorizados tengan pleno acceso al manejo de la información que esté en la base de datos de una compañía, así como los sistemas que la regulan. Este no es un principio que se oponga a la confidencialidad, pues se trata del acceso a todos los agentes, internos o externos, que tengan autorización.

Otros elementos a tener en cuenta: Teniendo claros la función de un Sistema de Seguridad de la Información y sus tres principios básicos, veamos ahora otros elementos que las organizaciones no pueden perder de vista en el proceso de implementación:

- **Compromiso y apoyo de la dirección.** Debe ser el área más comprometida a la hora de la difusión, la gestión y el seguimiento del proceso.

- **Definición del alcance.** Es preciso definir qué objetivos tendrá nuestro SGSI, qué beneficios supondrá y por cuánto tiempo queremos aplicarlo.

- **Formación del personal interno.** Los trabajadores de una empresa deben ser parte activa del proceso y para ello es necesario que reciban la formación necesaria que les permita estar a la altura del mismo.

- **Evaluación de riesgos.** Un SGSI se enfoca sobre todo en la gestión de riesgos asociados al manejo y la gestión de la información, que en cada empresa tiene características distintas y, por tanto, soluciones distintas.

- **Compromiso de mejora continua.** Al igual que otros sistemas de gestión interno, un SGSI supone la adopción de la mejora continua como elemento de identidad corporativa.

Para garantizar que la seguridad de la información es gestionada correctamente, se debe hacer uso de un proceso sistemático, documentado y conocido por toda la

organización, desde un enfoque de riesgo empresarial. Este proceso es el que constituye un SGSI".

La información, junto a los procesos y sistemas que hacen uso de ella, son activos muy importantes de una organización. La confidencialidad, integridad y disponibilidad de información sensible pueden llegar a ser esenciales para mantener los niveles de competitividad, rentabilidad, conformidad legal e imagen empresarial necesarios para lograr los objetivos de la organización y asegurar beneficios económicos.

Las organizaciones y sus sistemas de información están expuestos a un número cada vez más elevado de amenazas que, aprovechando cualquiera de las vulnerabilidades existentes, pueden someter a activos críticos de información a diversas formas de fraude, espionaje, sabotaje o vandalismo. Los virus informáticos, el "hacking" o los ataques de denegación de servicio son algunos ejemplos comunes y conocidos, pero también se deben considerar los riesgos de sufrir incidentes de seguridad causados voluntaria o involuntariamente desde dentro de la propia organización o aquellos provocados accidentalmente por catástrofes naturales y fallos técnicos. El cumplimiento de la legalidad, la adaptación dinámica y puntual a las condiciones variables del entorno, la protección adecuada de los objetivos de negocio para asegurar el máximo beneficio o el aprovechamiento de nuevas oportunidades de negocio, son algunos de los aspectos fundamentales en los que un SGSI es una herramienta de gran utilidad y de importante ayuda para la gestión de las organizaciones. (Neira & Spohr, 2010)

La gestión de la seguridad de la información debe realizarse mediante un proceso sistemático, documentado y conocido por toda la organización.

Ilustración 2 - Sistema de Gestión de Seguridad de la información

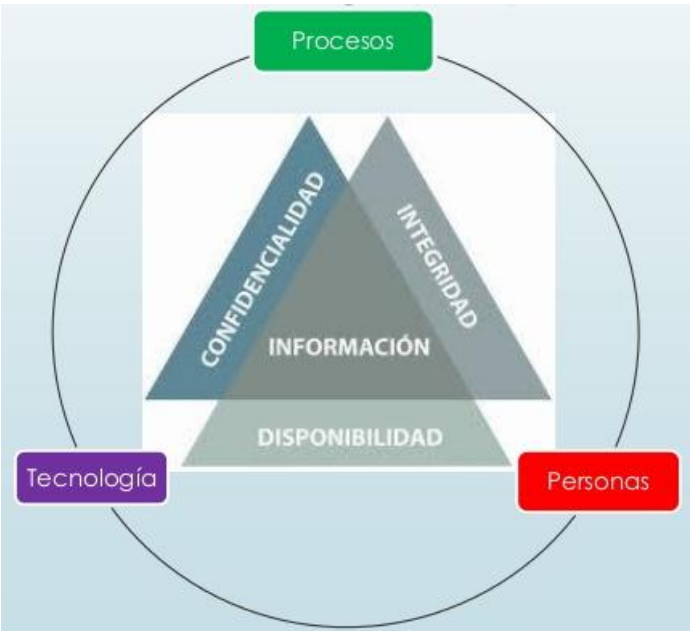
Fuente: Fuente: ISO27000.ES

El propósito de un sistema de gestión de la seguridad de la información es, por tanto, garantizar que los riesgos de la seguridad de la información sean conocidos, asumidos, gestionados y minimizados por la organización de una forma documentada, sistemática, estructurada, repetible, eficiente y adaptada a los cambios que se produzcan en los riesgos, el entorno y las tecnologías. (Neira & Spohr, 2010)

La norma ISO 27001 de Sistemas de Gestión de la Seguridad de la información tiene como finalidad el fomento e impulso de las actividades de protección de la información en las organizaciones como elemento de mejora de su imagen, generador de confianza frente a terceros, como herramienta de cumplimiento de legislación en esta materia e incluso para asegurar la viabilidad y continuidad del negocio. Actualmente la información se trata de uno de los principales activos con los que cuenta una organización, teniendo en muchas ocasiones un valor incalculable para la continuidad de la misma. Es por ello que resulta fundamental contar con un SGSI que asegure y controle el flujo de la misma, evitando pérdidas, filtraciones o deterioros. Además, la entrada en vigor de diferentes normativas hace que la gestión de la seguridad TIC sea fundamental de cara a evitar la imposición de sanciones administrativas por incumplir la legislación aplicable.(“la-importancia-de-la-seguridad-en-las-tic @ www.euroinnova.co,” n.d.)

La Seguridad de la Información se puede definir como conjunto de medidas técnicas, organizativas y legales que permiten a la organización asegurar la confidencialidad, integridad y disponibilidad de su sistema de información.

Ilustración 3 - Dimisiones de la información



Fuente: https://www.slideshare.net/JaimeAndrsBelloVieda/iso-27001-cambios-2005-a-2013

El objetivo de un SGSI es proteger la información y para ello lo primero que debe hacer es identificar los 'activos de información' que deben ser protegidos y en qué grado.

Luego debe aplicarse el plan PDCA ('PLAN – DO – CHECK – ACT'), es decir Planificar, Hacer, Verificar, Actuar y volver a repetir el ciclo.

Se entiende la seguridad como un proceso que nunca termina ya que los riesgos nunca se eliminan, pero se pueden gestionar. De los riesgos se desprende que los problemas de seguridad no son únicamente de naturaleza tecnológica, y por ese motivo nunca se eliminan en su totalidad.

PLANIFICAR (Plan): consiste en establecer el contexto, en él se crean las políticas de seguridad, se hace el análisis de riesgos, se hace la selección de controles y el estado de aplicabilidad.

¿Qué, Quién, Cuándo, Dónde, Con Qué?

HACER (Do): consiste en implementar el sistema de gestión de seguridad de la información, implementar el plan de riesgos e implementar los controles.

Realizar lo planeado

VERIFICAR (Check): consiste en monitorear las actividades y hacer auditorías internas.

¿El producto se hizo según lo planificado?

ACTUAR (Act): consiste en ejecutar tareas de mantenimiento, propuestas de mejora, acciones preventivas y acciones correctivas

¿Cómo hacerlo mejor la próxima vez?

Las normas que están dentro del marco superior del Anexo SL aplican el concepto PDCA – Plan, Do, Check, Act -, en la gestión de riesgos de una organización. ISO 31000 no es la excepción. Por ello, garantizar calidad continua y mejora en procesos, monitoreando objetivos estratégicos y el desempeño en forma periódica, es una parte integral del sistema.

El ciclo PHVA significa actuar sobre el proceso, resolviendo continuamente las desviaciones a los resultados esperados. El Mantenimiento y la mejora continua de la capacidad del proceso pueden lograrse aplicando este ciclo en cualquier nivel de la organización y en cualquier tipo de proceso, ya que se encuentra asociado con la planificación, implementación, control y mejora del desempeño de los procesos.

- **Planear**: establecer los objetivos para obtener resultados.
- **Hacer**: implementar procesos para alcanzar resultados.
- **Verificar**: realizar seguimiento y medir los procesos.
- **Actuar**: realizar acciones para promover la mejora del desempeño.

Tabla 2 - Ciclo PHVA ISO 27001:2013

CONTEXTO DE LA ORGANIZACIÓN	**PLANIFICACION**
LIDERAZGO	
PLANIFICACION	
SOPORTE	
OPERACION	HACER
EVALUACIÓN DE DESEMPEÑO	VERIFICAR
MEJORA	ACTUAR

Fuente: Autor

Según el sector de actividad, cuanto mayor es el valor de la información, mayores son los riesgos que se asocian a los incidentes que puedan afectarle como puede ser su pérdida total o parcial, su manipulación indebida, filtración a terceros, etc. En estos casos, contar con un buen SGSI es la forma más eficaz de minimizar estos riesgos asegurando la identificación y valoración de estos activos y sus riesgos asociados, teniendo presente el impacto para la organización y adoptando los controles y procedimientos adecuados en cada caso. Realizando una gestión eficaz de la seguridad TIC se permite a la organización: garantizar la confidencialidad de la información, limitando el acceso a quienes estén autorizados en cada caso; asegurar su integridad; facilitar su disponibilidad, permitiendo a los usuarios autorizados acceder a la información que necesiten en el momento que sea necesario.

Actualmente las actuaciones y medidas a tomar sobre la seguridad de la información se articulan en torno a 3 elementos básicos, que serían:

- **Los usuarios:** trabajadores de la organización que consultan, modifican y gestionan la información almacenada en los sistemas de la empresa. Son parte fundamental en el desarrollo de la seguridad de la información ya que de sus buenas prácticas dependerá en gran medida su eficiencia.

- **La gestión de la seguridad**: formada por el conjunto de normas y procedimientos que establecen el SGSI y que deben ser de obligado cumplimiento por todos los usuarios.

- **Las herramientas empleadas en la organización:** ya sean hardware o software, son la tercera pieza fundamental para garantizar la seguridad de la información.

La correcta integración e interacción de estos 3 elementos es fundamental para implementar un SGSI en cualquier organización, ya que si no se tienen todos en cuenta se incrementa el riesgo. De nada sirve implementar un sistema de gestión de seguridad si posteriormente no se controla que los usuarios efectivamente cumplan las directrices indicadas, o esperar un uso seguro de los recursos de internet por parte de los usuarios si no se les provee de los programas necesarios, como pueden ser los antivirus entre otros sistemas de protección.

Propósitos del SGSI

- Gestionar los riesgos de seguridad de la información.
- Cumplir con los principios de seguridad de la información.
- Mantener la confianza de los ciudadanos, contribuyentes, entidades gubernamentales y servidores públicos.
- Establecer las políticas, estándares, procedimientos, instructivos y controles en materia de seguridad de la información.
- Fortalecer la cultura de seguridad de la información en servidores públicos, proveedores, entes gubernamentales, ciudadanos y contribuyentes que tienen relación con la Entidad.
- Definir, aplicar y verificar el cumplimiento de los lineamientos para el buen uso de las herramientas informáticas.

5.3 MARCO CONCEPTUAL

5.3.1 Amenazas

Una amenaza es toda acción que aprovecha una vulnerabilidad para atentar contra la seguridad de un sistema de información. Es decir, que podría tener un potencial efecto negativo sobre algún elemento de nuestros sistemas. Las amenazas pueden proceder de ataques

- Fraude, robo, virus
- Sucesos físicos (incendios, inundaciones) o
- Negligencia y decisiones institucionales (mal manejo de contraseñas, no usar cifrado).

Desde el punto de vista de una organización pueden ser tanto internas como externas.

Una Amenaza es la posibilidad de ocurrencia de cualquier tipo de evento o acción que puede producir un daño (material o inmaterial) sobre los elementos de un sistema, en el caso de la Seguridad Informática, los Elementos de Información. Debido a que la Seguridad Informática tiene como propósitos de garantizar la

confidencialidad, integridad, disponibilidad y autenticidad de los datos e informaciones, las amenazas y los consecuentes daños que puede causar un evento exitoso, también hay que ver en relación con la confidencialidad, integridad, disponibilidad y autenticidad de los datos e informaciones.

DE acuerdo a ISO 27010, Las amenazas son las situaciones que desencadenan en un incidente en la empresa, realizando un daño material o pérdidas inmateriales de sus activos de información.

El Sistema de Gestión de Seguridad de la Información basado en la ISO 27001 ayuda a controlar las amenazas que pueden desencadenar los incidentes. La definición de amenaza es la diversidad de consecuencias, lo que hay que tener en cuenta es examinar el impacto.

- **Características de las amenazas:** La definición anterior recoge la esencia de las amenazas, es decir, es un potencial evento. La consecuencia de las amenazas es un incidente que modifica el estado de seguridad de los activos amenazados, por lo que se hace pasar de un estado anterior al evento a otro posterior, de cualquier forma que se trate la amenaza o las agresiones materializadas.

  La distancia que hay entre la amenaza potencial y su materialización como agresión real se mide por la frecuencia o la potencialidad de esta materialización, por lo que se cuenta una agresión materializada, las amenazas se verán si son agresiones potenciales o maternizadas.
- **Tipos de amenazas:** Todas las causas de las amenazas permiten ser clasificadas por su naturaleza. Podemos emplear cuatro causas amenazadoras:

Tabla 3 - Clasificación de las amenazas

TIPO DE AMENAZA	EJEMPLO DE AMENAZA
NO HUMANAS	• Accidente físico de origen industrial, incendios, explosiones, inundaciones, contaminación. • Averías que pueden ser de origen físico o lógico, se debe al el efecto de origen. • Accidente físico de origen natural, inundaciones, fenómeno sísmico o volcánico. • Interrupción de servicios o de suministros esenciales: energía, agua, telecomunicaciones, fluidos y suministros. • Accidentes mecánicos o electromagnéticos.

HUMANAS INVOLUNTARIAS,	• Errores de utilización ocurridos durante la recogida y transmisión de datos. • Errores de diseño existentes desde los procesos de desarrollo del software. • Errores de ruta, secuencia o entrega de la información durante el tránsito. • Errores de monitorización, trazabilidad o registros del tráfico de información.
HUMANAS INTENCIONALES QUE NECESITAN PRESENCIA FÍSICA	• Acceso físico con inutilización. • Acceso lógico con intercepción pasiva simple de la información. • Acceso lógico con alteración o sustentación de la información en tránsito, o reducir la confidencialidad para aprovechar los bienes o servicios. • Acceso lógico con corrupción o destrucción de información de configuración, o con reducción de la integridad y la disponibilidad del sistema sin provecho directo. • No se encuentran disponibles de recursos humanos.
HUMANA INTENCIONAL QUE PROCEDEN DE UN ORIGEN REMOTO	• Acceso lógico con intercepción pasiva. • Acceso lógico con corrupción de información en tránsito o de configuración. • Acceso lógico con modificación de información en tránsito. • Suplantación de origen o de identidad. • Repudio del origen o de la recepción de información en tránsito.

Fuente: https://www.pmg-ssi.com/2015/04/iso-27001-amenazas-y-vulnerabilidades/

5.3.2 Vulnerabilidades

Según [ISO/IEC 13335-1:2004]: una vulnerabilidad es una debilidad de un activo o conjunto de activos que puede ser explotado por una amenaza que y en el caso de la información puede comprometer la integridad, disponibilidad o confidencialidad de la misma, por lo que es necesario encontrarlas y eliminarlas lo antes posible. Ej. Fallos de diseño, errores de configuración o carencias de procedimientos.

5.3.3 Riesgo

El riesgo informático se define como se define como la combinación de la probabilidad de que se produzca un evento y sus consecuencias negativas.

5.3.4 Gestión del riesgo

El objetivo principal de la Gestión del Riesgo consiste en mantener ambientes en las organizaciones seguros, identificando los posibles factores que pueden causar

daños a los recursos tecnológicos de la entidad mediante la implementación de medidas que permitan mitigar el riego, disminuirlo o eliminarlo.

Ilustración 4 - Conformación del riesgo.

Fuente: https://www.incibe.es/protege-tu-empresa/blog/amenaza-vs-vulnerabilidad-sabes-se-diferencian

Antes de abordar la definición de riego definiremos los siguientes conceptos que hacen parte fundamental del análisis de riesgos.

- ✓ **Activo**: cualquier recurso de la empresa necesario para desempeñar las actividades diarias y cuya no disponibilidad o deterioro supone un agravio o coste. La naturaleza de los activos dependerá de la empresa, pero su protección es el fin último de la gestión de riesgos.

La valoración de los activos es importante para la evaluación de la magnitud del riesgo.

Este término en las nuevas normas se generaliza para denominarse ***«fuente de riesgo»*** siendo el elemento que sólo o con otros puede originar un riesgo.

- ✓ **Amenaza**: circunstancia desfavorable que puede ocurrir y que cuando sucede tiene consecuencias negativas sobre los activos provocando su indisponibilidad, funcionamiento incorrecto o pérdida de valor.

En la evolución de las normas este concepto se amplia para denominarse ***«suceso».***

- ✓ **Vulnerabilidad**: debilidad que presentan los activos y que facilita la materialización de las amenazas.

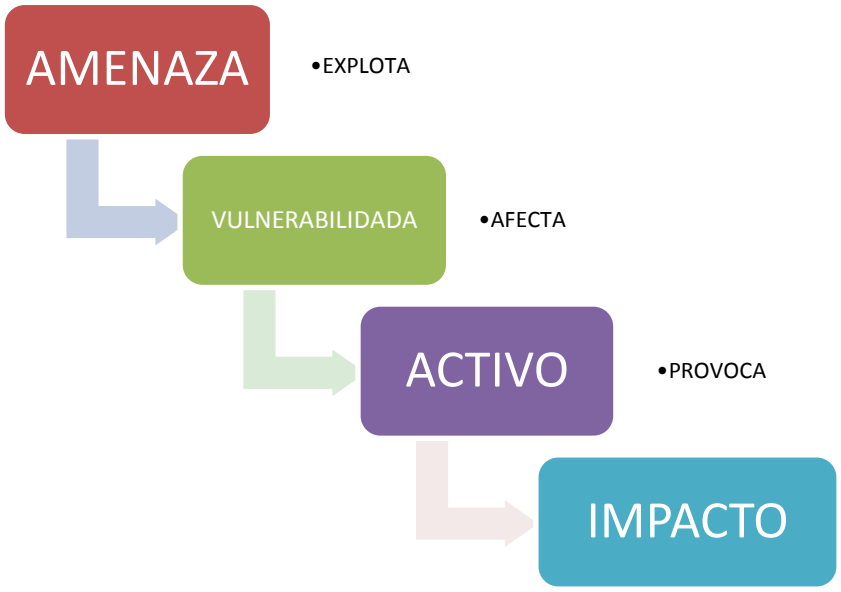
- ✓ **Impacto o consecuencia** de la materialización de una amenaza sobre un activo aprovechando una vulnerabilidad. El impacto se suele estimar en porcentaje de degradación que afecta al valor del activo, el 100% sería la pérdida total del activo. o La consecuencia en las nuevas normas es el resultado de un suceso que afecta a los objetivos.

- ✓ **Probabilidad:** es la posibilidad de ocurrencia de un hecho, suceso o acontecimiento.

  La frecuencia de ocurrencia implícita se corresponde con la amenaza. Para estimar la frecuencia podemos basarnos en datos empíricos (datos objetivos) del histórico de la empresa, o en opiniones de expertos o del empresario (datos subjetivos).

Este término permanece en la evolución de las normas ISO refiriéndose a un suceso en lugar de a una amenaza.

Ilustración 5 - Resumen grafico del riesgo



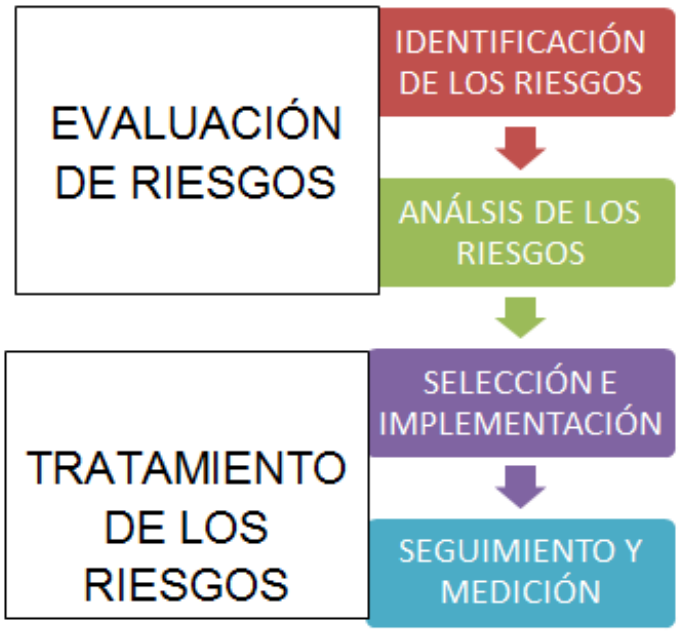
Fuente: Autor

La gestión de riesgos se presenta entonces como una actividad clave para el resguardo de los activos de información de una organización y en consecuencia protege la capacidad de cumplir sus principales objetivos. Es un proceso constante que permite a la administración balancear los costos operacionales y económicos causados por la interrupción de las actividades y la pérdida de activos, con los

costos de las medidas de protección a aplicar sobre los sistemas de información y los datos que dan soporte al funcionamiento de la organización, reduciendo los riegos que presentan los activos de información a niveles aceptables para la misma. (Generales, n.d.)

El proceso de gestión de riesgos involucra cuatro actividades cíclicas:
• La identificación de activos y los riesgos a los que están expuestos
• El análisis de los riesgos identificados para cada activo
• La selección e implantación de controles que reduzcan los riesgos
• El seguimiento, medición y mejora de las medidas implementadas

Ilustración 6 - Proceso de gestión del riesgo



Fuente: Autor

5.3.5 ¿Cómo se mide el nivel de riesgo?

El impacto nos indica las consecuencias de la materialización de una amenaza. El nivel de riesgo es una estimación de lo que puede ocurrir y se valora, de forma cuantitativa, como el producto del impacto, (consecuencia), asociado a una amenaza (suceso), por la probabilidad de la misma.

IMPACTO	X	PROBABILIDAD	=	RIESGO

Cálculo del riesgo

5.3.6 Etapas del proceso de gestión de riesgos

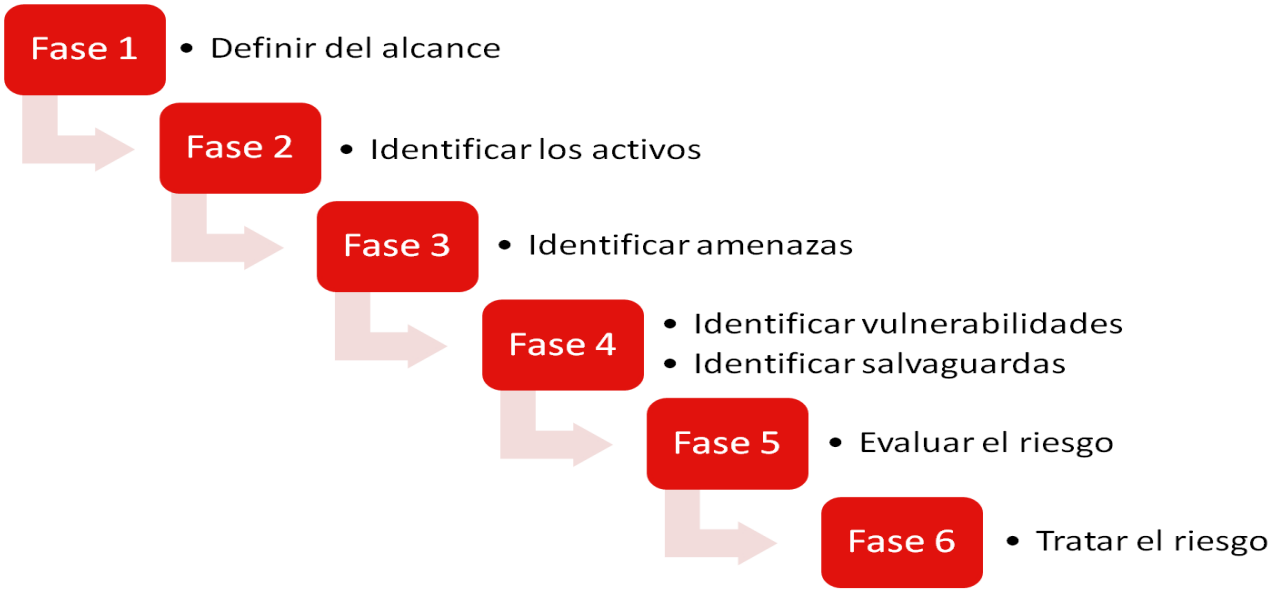
Ilustración 7 - Etapas del proceso de gestión de riesgos bajo los lineamientos generales de ISO 31000

Fuente: https://www.gestiopolis.com/iso-310002009-gestion-riesgos-principios-directrices/

5.3.7 Metodologías para el análisis de riegos

Existen múltiples metodologías para llevar a cabo el proceso de análisis, evaluación y gestión de riesgos informáticos, cada uno con su particularidad y dirigidos a ciertas situaciones. Sin embargo, todos tienen unos componentes y actividades comunes como son las siguientes:

Ilustración 8 - Conjunto de fases que son comunes en la mayor parte de las metodologías para el análisis de riesgos.



Fuente: https://www.incibe.es/protege-tu-empresa/blog/analisis-riesgos-pasos-sencillo

- **Fase 1_Definir el alcance:** El primer paso a la hora de llevar a cabo el análisis de riesgos, es establecer el alcance del estudio, que se va a hacer y en donde se va a hacer.

- **Fase 2_Identificar las Amenazas**: Esta fase consiste en identificar las posibles amenazas a la seguridad de la información y que podrían afectar los activos que procesan y almacenan la información de la entidad

- **Fase 3_Identificar las Vulnerabilidades:** Esta etapa permite identificar las vulnerabilidades a las que están sujetos los activos de información de la entidad, es de anotar que la existencia de vulnerabilidades contribuye a calcular la probabilidad del riesgo.

- **Fase 4_Identificar los Activos:** Esta etapa permite la identificación de los activos de información de la entidad y que tienen un impacto directo en la confidencialidad, integridad y disponibilidad en los datos de la entidad.

- **Fase 5_Determinar el Impacto**: Esta etapa permite determinar el impacto de una amenaza sobre un activo.

- **Fase 6_Determinar la Probabilidad:** Esta etapa permite medir la probabilidad de la ocurrencia de una amenaza a la cual se le asigna un valor de probabilidad.

- **Identificar los Controles:** Durante el desarrollo de esta etapa identificaremos que tipo de controles podremos utilizar para mitigar las amenazas.

- **Evaluar el riesgo:** Durante el desarrollo de esta etapa se evaluara el riesgo esto con la finalidad de minimizarlo, eliminarlo o transferirlo.

- **Tratar el riesgo:** Una vez calculado el riesgo, debemos tratar aquellos riesgos que superen un límite que nosotros mismos hayamos establecido. Por ejemplo, trataremos aquellos riesgos cuyo valor sea superior a “4” o superior a “Medio” en caso de que hayamos hecho el cálculo en términos cualitativos. A la hora de tratar el riesgo, existen cuatro estrategias principales:

    - **Transferir el riesgo a un tercero.**
    - **Eliminar el riesgo.**
    - **Asumir el riesgo.**
    - **Implantar medidas para mitigarlo.**

Características de algunas de las metodologías utilizadas en el análisis de riesgos.

Tabla 4- Metodologías para el análisis de riegos

NOMBRE	CARACTERÍSTICAS
OCTAVE	Es una metodología de análisis de riesgos y los estudia en base a tres principios disponibilidad, confiabilidad e integridad.
ISO 27005	Se ocupa de la gestión de los riesgos en la seguridad de la información.
FAIR	Se utiliza para realizar análisis de riesgos cuantitativos.
TARA	Metodología que realiza un seguimiento y una evaluación continua de los controles de seguridad
CRAMM	• Metodología para el análisis de riesgos, es empleada en la administración pública se basa en tres etapas (objetivos, análisis y selección de medidas)
MAGERIT	Es una metodología para el análisis de riegos en la administración publica Esta metodología describe una serie de etapas que permiten el analsisi de riegos y su debida gestión.
ESTÁNDAR COBIT:	Esta metodología propone un modelo en donde se evalúan algunos criterios que posee la información, y establece una guía de buenas prácticas que permiten auditar los sistemas de información de las organizaciones.

Fuente: Autor

5.3.8 Política de seguridad de la información

Una Política de Seguridad es un conjunto de requisitos definidos por los responsables de un sistema, que indica en términos generales que está y que no está permitido en el área de seguridad durante la operación general del sistema. (“polseginf @ www.segu-info.com.ar,” n.d.)

La RFC 1244[2] define Política de Seguridad como: "una declaración de intenciones de alto nivel que cubre la seguridad de los sistemas informáticos y que proporciona las bases para definir y delimitar responsabilidades para las diversas actuaciones técnicas y organizativas que se requerirán."

La política se refleja en una serie de normas, reglamentos y protocolos a seguir, donde se definen las medidas a tomar para proteger la seguridad del sistema; pero... ante todo, "(...) una política de seguridad es una forma de comunicarse con los usuarios... Siempre hay que tener en cuenta que la seguridad comienza y termina con personas." y debe:

- ✓ **Ser holística** (cubrir todos los aspectos relacionados con la misma). No tiene sentido proteger el acceso con una puerta blindada si a esta no se la ha cerrado con llave.
- ✓ **Adecuarse a las necesidades y recursos.** No tiene sentido adquirir una caja fuerte para proteger un lápiz.
- ✓ **Ser atemporal.** El tiempo en el que se aplica no debe influir en su eficacia y eficiencia.
- ✓ **Definir estrategias y criterios generales** a adoptar en distintas funciones y actividades, donde se conocen las alternativas ante circunstancias repetidas.

Cualquier política de seguridad ha de contemplar los elementos claves de seguridad ya mencionados: la Integridad, Disponibilidad, Privacidad y, adicionalmente, Control, Autenticidad y Utilidad.

No debe tratarse de una descripción técnica de mecanismos de seguridad, ni de una expresión legal que involucre sanciones a conductas de los empleados. Es más bien una descripción de los que deseamos proteger y el porqué de ello.

La política de seguridad es un documento de alto nivel que denota el compromiso de la gerencia con la seguridad de la información, debe ser enriquecida y compatibilizada con otras políticas dependientes de ésta, objetivos de seguridad, procedimientos, debe estar fácilmente accesible de forma que los empleados estén al tanto de su existencia y entiendan su contenido. Puede ser también un documento único o inserto en un manual de seguridad. Además, se debe designar un propietario

[2] *RFC 1244: Site Security Handbook. J. Reynolds - P. Holbrook. Julio 1991*

que será el responsable de su mantenimiento y su actualización a cualquier cambio que se requiera.

Para las entidades es importante contar con políticas de seguridad ya que son ellas quienes guiaran el comportamiento personal y profesional de los funcionarios, contratistas o terceros sobre la información obtenida, generada o procesada por la entidad, así mismo las políticas permitirán que la entidad trabaje bajo las mejores prácticas de seguridad y cumpla con los requisitos legales a los cuales esté obligada a cumplir la entidad. (MINTIC, 2016)

A continuación definiremos algunos conceptos aplicados en la definición de una política de seguridad de la información:

- **Decisión**: elección de un curso de acción determinado entre varios posibles.
- **Plan**: conjunto de decisiones que definen cursos de acción futuros y los medios para conseguirlos. Consiste en diseñar un futuro deseado y la búsqueda del modo de conseguirlo.
- **Estrategia:** conjunto de decisiones que se toman para determinar políticas, metas y programas.
- **Política:** definiciones establecidas por la dirección, que determina criterios generales a adoptar en distintas funciones y actividades donde se conocen las alternativas ante circunstancias repetidas.
- **Meta:** objetivo cuantificado a valores predeterminados.
- **Procedimiento:** Definición detallada de pasos a ejecutar para desarrollar una actividad determinada.
- **Norma:** forma en que realiza un procedimiento o proceso.
- **Programa:** Secuencia de acciones interrelacionadas y ordenadas en el tiempo que se utilizan para coordinar y controlar operaciones.
- **Proyección:** predicción del comportamiento futuro, basándose en el pasado sin el agregado de apreciaciones subjetivas.
- **Pronostico:** predicción del comportamiento futuro, con el agregado de hechos concretos y conocidos que se prevé influirán en los acontecimientos futuros.
- **Control:** capacidad de ejercer o dirigir una influencia sobre una situación dada o hecho. Es una acción tomada para hacer un hecho conforme a un plan.
- **Riesgo**: Proximidad o posibilidad de un daño, peligro. Cada uno de los imprevistos, hechos desafortunados, etc., que puede tener un efecto adverso. Sinónimos: amenaza, contingencia, emergencia, urgencia, apuro.
  (“polseginf @ www.segu-info.com.ar,” n.d.)

5.3.9 Estándar ISO/IEC 27001:2013

A semejanza de otras normas ISO, ISO/IEC 27000 es un conjunto de estándares desarrollados -o en fase de desarrollo- por ISO (International Organization for Standardization) e IEC (International Electrotechnical Commission), que proporcionan un marco de gestión de la seguridad de la información utilizable por cualquier tipo de organización, pública o privada, grande o pequeña y proporciona una metodología para implementar la gestión de la seguridad de la información.

En la siguiente tabla se hace un resumen las distintas normas que componen la serie ISO 27000

Tabla 5 - Normas de la serie ISO 27000

NORMA	DESCRIPCIÓN
ISO/IEC 27000	Esta norma proporciona una visión general de las normas que componen la serie 27000, indicando para cada una de ellas su alcance de actuación y el propósito de su publicación. Recoge todas las definiciones para la serie de normas 27000 y aporta las bases de por qué es importante la implantación de un SGSI, una introducción a los Sistemas de Gestión de Seguridad de la Información, una breve descripción de los pasos para el establecimiento, monitorización, mantenimiento y mejora de un SGSI (la última edición no aborda ya el ciclo Plan-Do-Check-Act para evitar convertirlo en el único marco de referencia para la mejora continua).
ISO/IEC 27001	Es la norma principal de la serie y contiene los requisitos del sistema de gestión de seguridad de la información. Enumera en forma de resumen los objetivos de control y controles que desarrolla la ISO 27002:2005, para que sean seleccionados por las organizaciones en el desarrollo de sus SGSI; a pesar de no ser obligatoria la implementación de todos los controles enumerados en dicho anexo, la organización deberá argumentar sólidamente la no aplicabilidad de los controles no implementados.
ISO/IEC 27002	Es una guía de buenas prácticas que describe los objetivos de control y controles recomendables en cuanto a seguridad de la información. No es certificable. Contiene 39 objetivos de control y 133 controles, agrupados en 11 dominios.
ISO/IEC 27003	Es una guía que se centra en los aspectos críticos necesarios para el diseño e implementación con éxito de un SGSI de acuerdo ISO/IEC 27001. Describe el proceso de especificación y diseño desde la concepción hasta la puesta en marcha de planes de implementación, así como el proceso de obtención de aprobación por la dirección para implementar un SGSI.
ISO/IEC 27004	Es una guía para el desarrollo y utilización de métricas y técnicas de

	medida aplicables para determinar la eficacia de un SGSI y de los controles o grupos de controles implementados según ISO/IEC 27001.
ISO/IEC 27005	Proporciona directrices para la gestión del riesgo en la seguridad de la información. Apoya los conceptos generales especificados en la norma ISO/IEC 27001:2005 y está diseñada para ayudar a la aplicación satisfactoria de la seguridad de la información basada en un enfoque de gestión de riesgos.

Fuente: Autor

- **¿Cómo funciona la ISO 27001?**

El eje central de ISO 27001 es proteger la confidencialidad, integridad y disponibilidad de la información en una empresa. Esto lo hace investigando cuáles son los potenciales problemas que podrían afectar la información (es decir, la evaluación de riesgos) y luego definiendo lo que es necesario hacer para evitar que estos problemas se produzcan (es decir, mitigación o tratamiento del riesgo).

Por lo tanto, la filosofía principal de la norma ISO 27001 se basa en la gestión de riesgos: investigar dónde están los riesgos y luego tratarlos sistemáticamente.

Ilustración 9 - Estructura de ISO 27001

Fuente: https://advisera.com/27001academy/es/que-es-iso-27001/

- **¿Por qué ISO 27001 es importante para las organizaciones?**

  - **Cumplir con los requerimientos legales** – cada vez hay más y más leyes, normativas y requerimientos contractuales relacionados con la seguridad de la información. La buena noticia es que la mayoría de ellos se pueden resolver implementando ISO 27001 ya que esta norma le proporciona una metodología perfecta para cumplir con todos ellos.

  - **Menores costos** – la filosofía principal de ISO 27001 es evitar que se produzcan incidentes de seguridad, y cada incidente, ya sea grande o

pequeño, cuesta dinero; por lo tanto, evitándolos la organización va a ahorrar mucho dinero. Y lo mejor de todo es que la inversión en ISO 27001 es mucho menor que el ahorro que obtendrá.

- **Una mejor organización** – en general, las empresas de rápido crecimiento no tienen tiempo para hacer una pausa y definir sus procesos y procedimientos; como consecuencia, muchas veces los empleados no saben qué hay que hacer, cuándo y quién debe hacerlo. La implementación de ISO 27001 ayuda a resolver este tipo de situaciones ya que alienta a las organizaciones a escribir sus principales procesos (incluso los que no están relacionados con la seguridad), lo que les permite reducir el tiempo perdido de sus empleados.

- **¿Dónde interviene la gestión de seguridad de la información en una organización?**

Básicamente, la seguridad de la información es parte de la gestión global del riesgo en una organización, hay aspectos que se superponen con la ciberseguridad, con la gestión de la continuidad del negocio y con la tecnología de la información:

Ilustración 10 - Gestión del riesgo

Fuente: https://advisera.com/27001academy/es/que-es-iso-27001/

- **Generalidades de la NTC ISO/IEC 27001: 2013.**

Esta Norma ha sido elaborada para suministrar requisitos para el establecimiento, implementación, mantenimiento y mejora continua de un sistema de gestión de la seguridad de la información. La adopción de un sistema de gestión de seguridad de la información es una decisión estratégica para una organización. El establecimiento e implementación del sistema de gestión de la seguridad de la información de una organización están influenciados por las necesidades y objetivos de la organización, los requisitos de seguridad, los procesos organizacionales empleados, y el tamaño y estructura de la organización. Se espera que todos estos factores de influencia cambien con el tiempo.

El sistema de gestión de la seguridad de la información preserva la confidencialidad, la integridad y la disponibilidad de la información, mediante la aplicación de un proceso de gestión del riesgo, y brinda confianza a las partes interesadas acerca de que los riesgos son gestionados adecuadamente. (ICONTEC, 2013)

- **Requisitos de la NTC ISO/IEC 27001: 2013.**

Tabla 6 - Requisitos de la NTC ISO/IEC 27001: 2013.

1. OBJETO Y CAMPO DE APLICACIÓN	Explica el objetivo de ISO 27001 y su compatibilidad con otras normas de gestión.
2. REFERENCIAS NORMATIVAS	Hace referencia a la norma ISO/IEC 27000 como estándar en el que se proporcionan términos y definiciones.
3. TÉRMINOS Y DEFINICIONES	Hace referencia a la norma ISO/IEC 27000.
4. CONTEXTO DE LA ORGANIZACIÓN 4.1. CONOCIMIENTO DE LA ORGANIZACIÓN Y DE SU CONTEXTO. 4.2. COMPRENSIÓN DE LAS NECESIDADES Y EXPECTATIVAS DE LAS PARTES INTERESADAS. 4.3. DETERMINACIÓN DEL ALCANCE DEL SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN. 4.4. SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN.	Esta sección es parte de la fase de Planificación del ciclo PDCA[3] y define los requerimientos para comprender cuestiones externas e internas, también define las partes interesadas, sus requisitos y el alcance del SGSI.
5. LIDERAZGO. 5.1. LIDERAZGO Y COMPROMISO, 5.2. POLÍTICA. 5.3. ROLES, RESPONSABILIDADES Y	Esta sección es parte de la fase de Planificación del ciclo PDCA y define las responsabilidades de la dirección, el establecimiento de roles y responsabilidades y el contenido de la política de alto nivel sobre seguridad de la información

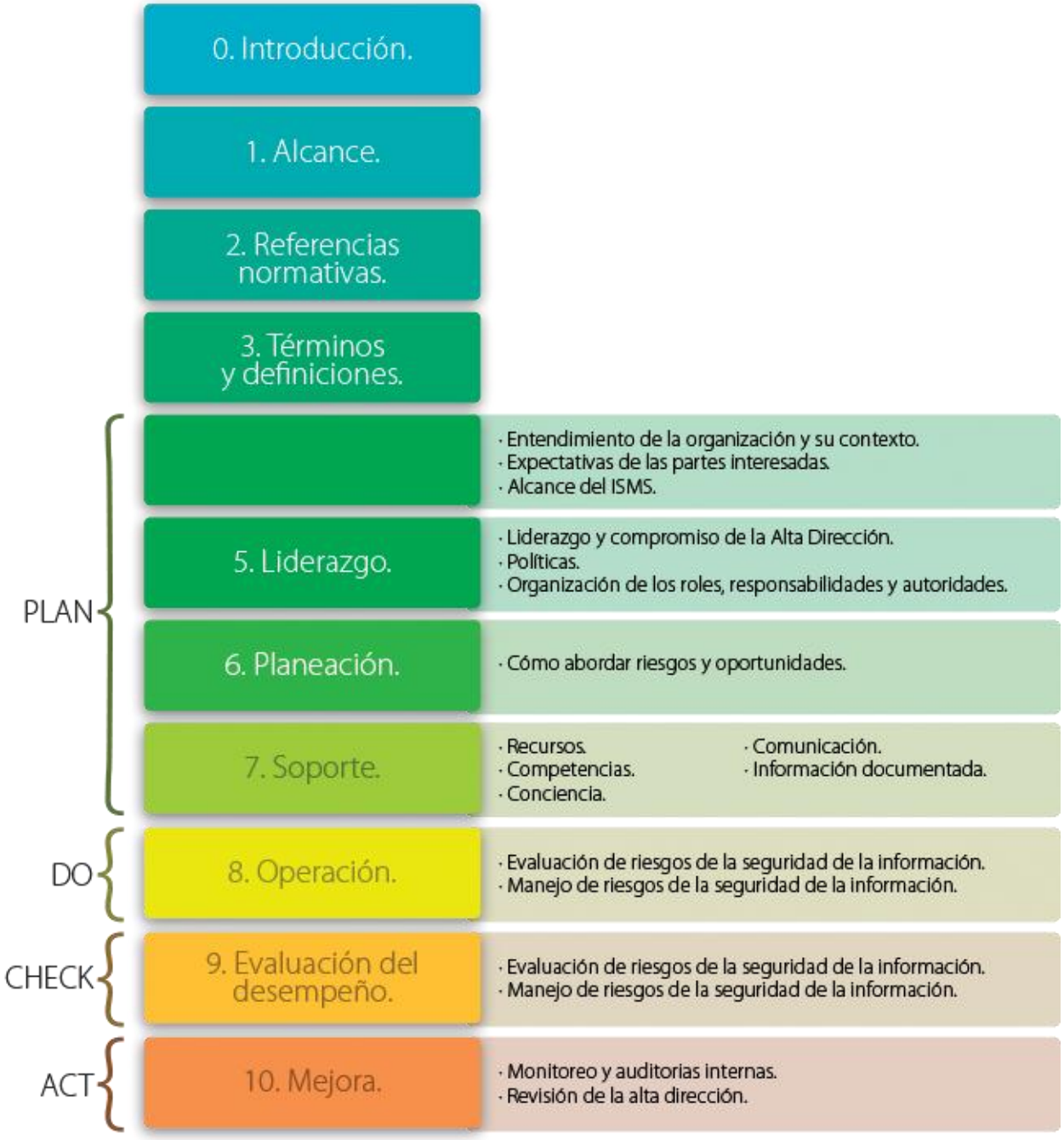
[3] PDCA: Planear – Hacer – Verificar - Actuar

AUTORIDADES EN LA ORGANIZACIÓN.	
6. PLANIFICACIÓN. 6.1. ACCIONES PARA TRATAR RIESGOS Y OPORTUNIDADES. 6.1.1.Generalidades. 6.1.2.Valoración de riesgos de la seguridad de la información. 6.1.3.Tratamiento de riesgos de la seguridad de la información. 6.2. OBJETIVOS DE SEGURIDAD DE LA INFORMACIÓN Y PLANES PARA LOGRARLOS	Esta sección es parte de la fase de Planificación del ciclo PDCA y define los requerimientos para la evaluación de riesgos, el tratamiento de riesgos, la Declaración de aplicabilidad, el plan de tratamiento de riesgos y la determinación de los objetivos de seguridad de la información.
7. SOPORTE 7.1. RECURSOS. 7.2. COMPETENCIA. 7.3. TOMA DE CONCIENCIA. 7.4. COMUNICACIÓN. 7.5. INFORMACIÓN DOCUMENTADA 7.5.1.Generalidades 7.5.2.Creación y actualización	Esta sección es parte de la fase de Planificación del ciclo PDCA y define los requerimientos sobre disponibilidad de recursos, competencias, concienciación, comunicación y control de documentos y registros.
8. OPERACIÓN 8.1. PLANIFICACIÓN Y CONTROL OPERACIONAL. 8.2. VALORACIÓN DE RIESGOS DE LA SEGURIDAD DE LA INFORMACIÓN. 8.3. TRATAMIENTO DE RIESGOS DE LA SEGURIDAD DE LA INFORMACIÓN.	Esta sección es parte de la fase de Planificación del ciclo PDCA y define la implementación de la evaluación y el tratamiento de riesgos, como también los controles y demás procesos necesarios para cumplir los objetivos de seguridad de la información.
9. EVALUACIÓN DEL DESEMPEÑO 9.1. SEGUIMIENTO, MEDICIÓN, ANÁLISIS Y EVALUACIÓN. 9.2. AUDITORÍA INTERNA. 9.3. REVISIÓN POR LA DIRECCIÓN	Esta sección forma parte de la fase de Revisión del ciclo PDCA y define los requerimientos para monitoreo, medición, análisis, evaluación, auditoría interna y revisión por parte de la dirección.
10. MEJORA 10.1. NO CONFORMIDADES Y ACCIONES CORRECTIVAS. 10.2. MEJORA CONTINUA	Esta sección forma parte de la fase de Mejora del ciclo PDCA y define los requerimientos para el tratamiento de no conformidades, correcciones, medidas correctivas y mejora continua.

Fuente: Norma ISO 27001

En la nueva ISO 27001 existen 14 dominios, 35 objetivos de control y 114 controles. Uno de los grandes cambios que se han producido en éste área es la importancia que tiene la evaluación y aprendizaje de los eventos de seguridad de TI que se centra en el programa de respuesta a incidentes.

Ilustración 11 - Dominios ISO 27001:2013



Fuente: http://www.magazcitum.com.mx/?p=2397#.Wt_XMdTwbcc

5.3.10 MAGERIT

Es la metodología de análisis y gestión de riesgos elaborada por el Consejo Superior de Administración Electrónica, como respuesta a la percepción de que la Administración, y, en general, toda la sociedad, dependen de forma creciente de las

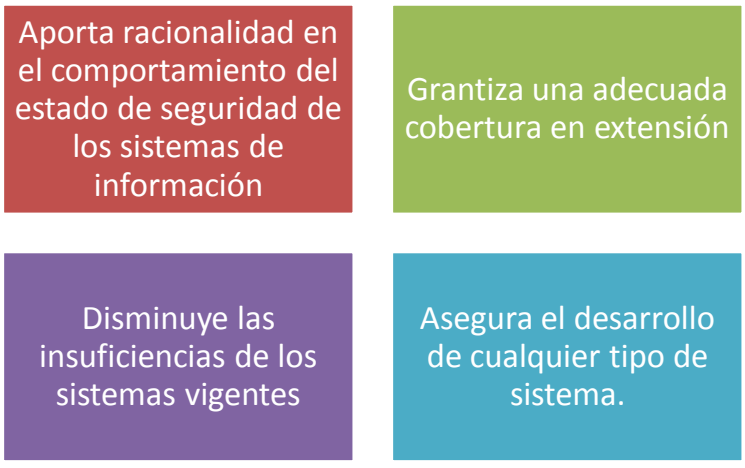
tecnologías de la información para el cumplimiento de su misión.(“pae_Magerit @ administracionelectronica.gob.es,” n.d.)

Magerit es una metodología de análisis y gestión de riesgos originados por el uso de TIC´s y que permite establecer una serie de controles para mitigarlos, disminuirlos o eliminarlos

MAGERIT persigue los siguientes objetivos:

- ✓ Concienciar a los responsables de las organizaciones de información de la existencia de riesgos y de la necesidad de gestionarlos.
- ✓ Ofrecer un método sistemático para analizar los riesgos derivados del uso de tecnologías de la información y comunicaciones (TIC).
- ✓ Ayudar a descubrir y planificar el tratamiento oportuno para mantener los riesgos bajo control Indirectos.
- ✓ Preparar a la Organización para procesos de evaluación, auditoría, certificación o acreditación, según corresponda en cada caso.

Con la aplicación de MAGERIT se permite:



- **Elementos de MAGERIT**

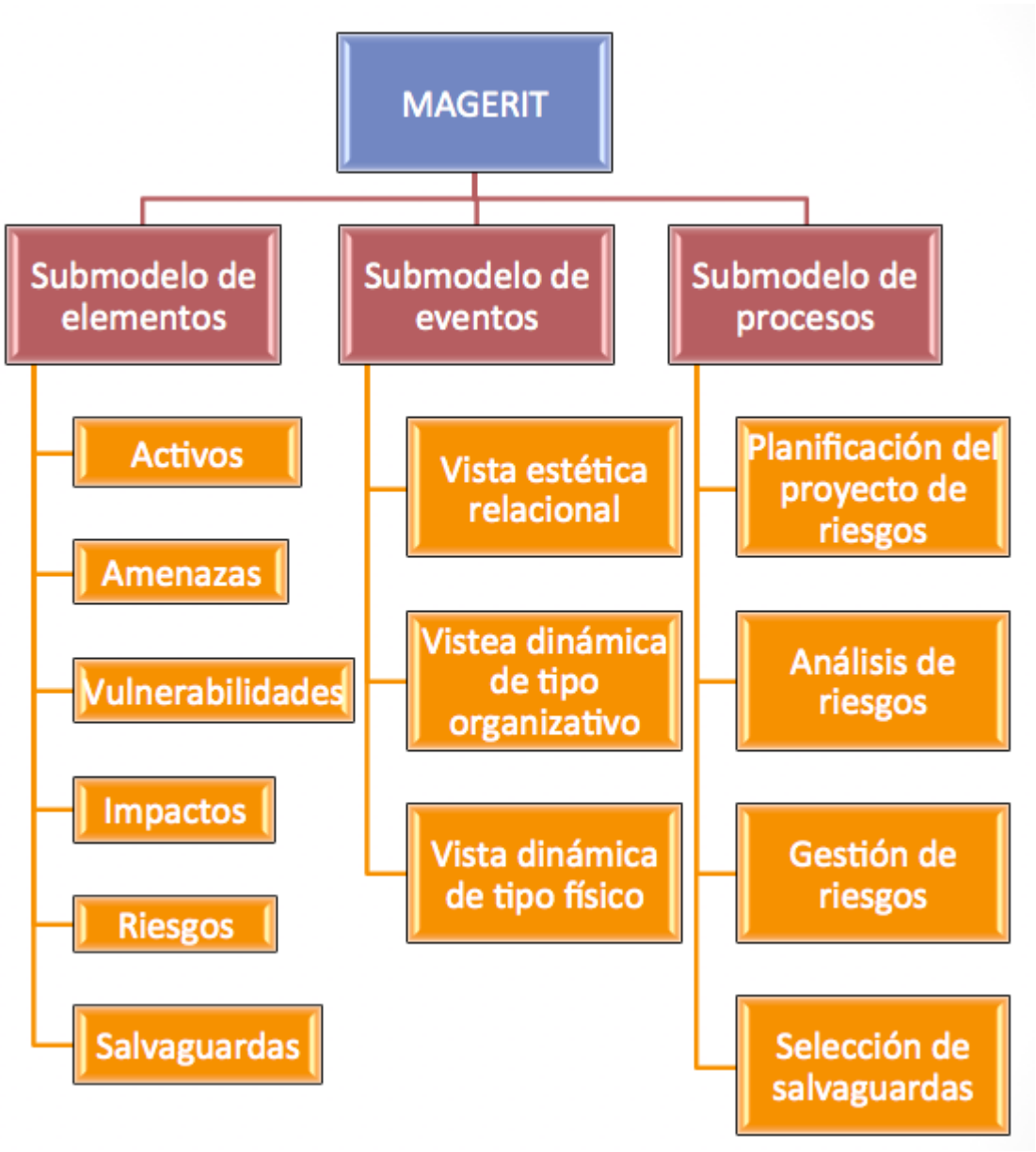
- ✓ **Análisis de Riegos**: Para identificar las amenazas que acechan a los distintos componentes pertenecientes o relacionados al Sistema de

Información (activos); para determinar la vulnerabilidad del sistema ante esas amenazas y para estimar el impacto o grado de perjuicio que una seguridad insuficiente puede tener en la organización, obteniendo cierto conocimiento del riesgo que se corre.

- ✓ **Gestión de Riesgos:** basada en los resultados obtenidos en el análisis anterior, que permite seleccionar e implantar las medidas o "salvaguardas" de seguridad adecuadas para conocer, prevenir, impedir, reducir o controlar los riesgos identificados y así reducir al mínimo su potencialidad o sus posibles perjuicios.

- **Estructura de MAGERIT**

Ilustración 12 - Estructura de MAGERIT



Fuente: https://asijav.weebly.com/auditoria-de-sistemas-de-informacioacuten/magerit-v3-metodologa-de-anlisis-y-gestin-de-riesgos-de-los-sistemas-de-informacin.

A continuación se relacionan cada uno de los pasos que se deben contemplan en un proceso de análisis de riesgos, teniendo en cuenta un orden sistémico que permita concluir el riesgo actual en que se encuentra la empresa

Ilustración 13 - Pasos para la aplicación de la metodología MAGERIT

Fuente: http://seguridadinformaticaunad.blogspot.com.co/2014/03/metodologia-magerit.html

La Evaluación del riesgo es fundamental para llevar cabo planes de seguridad y de contingencia dentro de la organización, para poder gestionarlos y hacerse riguroso frente a posibles ataques a los datos y la información tanto de la organización, como de los servicios que presta.

5.4 MARCO LEGAL

- ✓ **LEY 603 DE 2000:** Esta ley se refiere a la protección de los derechos de autor en Colombia. Recuerde: el software es un activo, además está protegido por el Derecho de Autor y la Ley 603 de 2000 obliga a las empresas a declarar si los problemas de software son o no legales.

- ✓ **LEY ESTATUTARIA 1266 DEL 31 DE DICIEMBRE DE 2008:** Por la cual se dictan las disposiciones generales del Hábeas Data y se regula el manejo de la información contenida en bases de datos personales, en especial la financiera, crediticia, comercial, de servicios y la proveniente de terceros países y se dictan otras disposiciones. Ver esta ley.

- ✓ **LEY 1273 DE 2009**. Denominado “de la protección de la información y de los datos.

- ✓ **LEY 1341 DEL 30 DE JULIO DE 2009:** Por la cual se definen los principios y conceptos sobre la sociedad de la información y la organización de las Tecnologías de la Información y las Comunicaciones -TIC-, se crea la Agencia Nacional del Espectro y se dictan otras disposiciones.

- ✓ **LEY ESTATUTARIA 1581 DE 2012:** Entró en vigencia la Ley 1581 del 17 de octubre 2012 de PROTECCIÓN DE DATOS PERSONALES

- ✓ **DECRETO 1377 DE 2013:** Protección de Datos, decreto por el cual se reglamenta parcialmente la Ley 1581 de 2012.

- ✓ **LEY 1712 DE 2014:** Por medio de la cual se crea la Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional y se dictan otras disposiciones.

- ✓ **DECRETO 2573 DE 2014:** Por el cual se establecen los lineamientos generales de la Estrategia de Gobierno en línea.

- ✓ **DECRETO ÚNICO REGLAMENTARIO 1078 DE 2015**: Estrategia del Gobierno en Línea. Sección 2, Artículo 2.2.9.1.2.1 numeral 4 define el componente de Seguridad y Privacidad de la Información.

- ✓ **DECRETO 415 DE 2016 DE LA PRESIDENCIA DE LA REPÚBLICA:** Establece los lineamientos para el fortalecimiento institucional en materia de Tics.

5.5 MARCO CONTEXTUAL

5.5.1 Nombre de la entidad

Administración municipal de la Ceja – Antioquia

5.5.2 Contexto

La Ceja del Tambo es un municipio de Colombia, localizado en la subregión Oriente del departamento de Antioquia, fundada en El 7 de diciembre de 1789, en la

actualidad cuenta con La Ceja tiene 16 veredas y con una población total de 67.622 habitantes disturbios así:

POBLACIÓN	• **Población Urbana**: 60. 678 HABITANTES
	• **Población Rural**: 6 .944 HABITANTES

Según las cifras de la Gobernación de Antioquia basadas en la encuesta de Calidad de Vida 2004 el estrato socio-económico que predomina en La Ceja es el siguiente y lo conforma la siguiente población:

Ilustración 14 - Estrato Socioeconómico municipio de La Ceja-Antioquia

Estrato 3 (medio-bajo)	65.6%.
Estrato 2 (bajo)	30%.
Estrato 4	2.9%,
Estrato 1 (bajo-bajo)	1.0%
Estrato 5 (medio-alto)	0.5%.

Fuente: Autor

Ilustración 15 - Panorámica municipio de La Ceja-Antioquia

Ilustración 16 - Ubicación de las diferentes dependencias de la administración municipal

Fuente: Autor

5.5.3 Caracterización de servicios

En la Ley 1551 de 2012[4] establece las siguientes funciones a las entidades territoriales, establece las siguientes funciones a los municipios:

Artículo 3. Funciones de los municipios. Corresponde al municipio:

1. Administrar los asuntos municipales y prestar los servicios públicos que determine la ley.

2. Elaborar los planes de desarrollo municipal, en concordancia con el plan de desarrollo departamental, los planes de vida de los territorios y resguardos indígenas, incorporando las visiones de las minorías étnicas, de las organizaciones comunales y de los grupos de población vulnerables presentes en su territorio, teniendo en cuenta los criterios e instrumentos definidos por la Unidad de Planificación de Tierras Rurales y Usos Agropecuarios (UPRA), para el ordenamiento y el uso eficiente del suelo rural, los programas de desarrollo rural con enfoque territorial, y en armonía con el Plan Nacional de Desarrollo, según la ley orgánica de la materia.

[4] Ley 551 de 2012: “Por la cual se dictan normas para modernizar la organización y el funcionamiento de los municipios”

Los planes de desarrollo municipal deberán incluir estrategias y políticas dirigidas al respeto y garantía de los Derechos Humanos y del Derecho Internacional Humanitario;

3. Promover el desarrollo de su territorio y construir las obras que demande el progreso municipal. Para lo anterior deben tenerse en cuenta, entre otros: los planes de vida de los pueblos y comunidades indígenas y los planes de desarrollo comunal que tengan los respectivos organismos de acción comunal.

4. Elaborar e implementar los planes integrales de seguridad ciudadana, en coordinación con las autoridades locales de policía y promover la convivencia entre sus habitantes.

5. Promover la participación comunitaria, la cultura de Derechos Humanos y el mejoramiento social y cultural de sus habitantes. El fomento de la cultura será prioridad de los municipios y los recursos públicos invertidos en actividades culturales tendrán, para todos los efectos legales, el carácter de gasto público social de conformidad con el artículo 1o, numeral 8 de la Ley 397 de 1997.

6. Promover alianzas y sinergias público-privadas que contribuyan al desarrollo económico, social y ambiental del municipio y de la región, mediante el empleo de los mecanismos de integración dispuestos en la ley.

7. Procurar la solución de las necesidades básicas insatisfechas de los habitantes del municipio, en lo que sea de su competencia, con especial énfasis en los niños, las niñas, los adolescentes, las mujeres cabeza de familia, las personas de la tercera edad, las personas en condición de discapacidad y los demás sujetos de especial protección constitucional.

8. En asocio con los departamentos y la Nación, contribuir al goce efectivo de los derechos de la población víctima del desplazamiento forzado, teniendo en cuenta los principios de coordinación, concurrencia, complementariedad, subsidiariedad y las normas jurídicas vigentes.

9. Formular y adoptar los planes de ordenamiento territorial, reglamentando de manera específica los usos del suelo en las áreas urbanas, de expansión y rurales, de acuerdo con las leyes y teniendo en cuenta los instrumentos definidos por la UPRA para el ordenamiento y el uso eficiente del suelo rural. Optimizar los usos de las tierras disponibles y coordinar los planes sectoriales en armonía con las políticas nacionales y los planes departamentales y metropolitanos. Los Planes de Ordenamiento Territorial serán presentados para revisión ante el Concejo Municipal o Distrital cada 12 años.

10. Velar por el adecuado manejo de los recursos naturales y del ambiente, de conformidad con la Constitución y la ley.

11. Promover el mejoramiento económico y social de los habitantes del respectivo municipio, fomentando la industria nacional, el comercio y el consumo interno en sus territorios de conformidad con la legislación vigente para estas materias.

12. Fomentar y promover el turismo, en coordinación con la Política Nacional.

13. Los municipios fronterizos podrán celebrar Convenios con entidades territoriales limítrofes del mismo nivel y de países vecinos para el fomento de la convivencia y seguridad ciudadana, el desarrollo económico y comunitario, la prestación de servicios públicos y la preservación del ambiente.

14. Autorizar y aprobar, de acuerdo con la disponibilidad de servicios públicos, programas de desarrollo de Vivienda ejerciendo las funciones de vigilancia necesarias.

15. Incorporar el uso de nuevas tecnologías, energías renovables, reciclaje y producción limpia en los planes municipales de desarrollo.

16. En concordancia con lo establecido en el artículo 355 de la Constitución Política, los municipios y distritos podrán celebrar convenios solidarios con: los cabildos, las autoridades y organizaciones indígenas, los organismos de acción comunal y demás organizaciones civiles y asociaciones residentes en el territorio, para el desarrollo conjunto de programas y actividades establecidas por la Ley a los municipios y distritos, acorde con sus planes de desarrollo.

17. Elaborar los planes y programas anuales de fortalecimiento, con la correspondiente afectación presupuestal, de los cabildos, autoridades y organizaciones indígenas, organismos de acción comunal, organizaciones civiles y asociaciones residentes en el territorio. Lo anterior deberá construirse de manera concertada con esas organizaciones y teniendo en cuenta sus necesidades y los lineamientos de los respectivos planes de desarrollo.

18. Celebrar convenios de uso de bienes públicos y/o de usufructo comunitario con los cabildos, autoridades y organizaciones indígenas y con los organismos de acción comunal y otros organismos comunitarios.

19. Garantizar la prestación del servicio de agua potable y saneamiento básico a los habitantes de la jurisdicción de acuerdo con la normatividad vigente en materia de servicios públicos domiciliarios.

20. Ejecutar el Programas de Alimentación Escolar con sus propios recursos y los provenientes del Departamento y la Nación, quienes podrán realizar el acompañamiento técnico, acorde con sus competencias.

21. Publicar los informes de rendición de cuentas en la respectiva página web del municipio.

22. Las demás que señalen la Constitución y la ley.

23. En materia de vías, los municipios tendrán a su cargo la construcción y mantenimiento de vías urbanas y rurales del rango municipal. Continuarán a cargo de la Nación, las vías urbanas que formen parte de las carreteras nacionales, y del Departamento las que sean departamentales. (Secretaría General de la Alcaldía Mayor de Bogotá D.C., 2011).

5.5.4 Misión

Desarrollar estrategias programas y proyectos que posibiliten que el municipio de la ceja progrese de manera sostenible y competitiva con un enfoque de inclusión y de participación comunitaria que propicie el empoderamiento de sus pobladores, la articulación con los diferentes sectores sociales y productivos, así como la integración con los entes departamentales y nacionales con quienes, de manera sinérgica. Trabajaremos por fortalecer la institucionalidad y de ese modo, brindar a toda la ciudadanía más y mejores oportunidades de progreso y mejeros en su calidad de vida.

5.5.5 Visión

El municipio de la ceja se proyectara como un municipio planificado, armónico y sostenible, con orden institucional y una arraigada cultura ciudadana, destacado por la inclusión social, la participación comunitaria, la promoción, la protección de los recursos naturales y la vivencia de la paz. Un municipio que brinda posibilidades de desarrollo integral, bienestar social y condiciones de calidad de vida que les permite sus habitantes Vivir mejor

5.5.6 Funciones

Tal como lo establece la Constitución Política de Colombia (Art. 311) y la Ley 136 de 1994 (Art. 1º) el municipio es la entidad fundamental de la división político-administrativa del Estado, impulsadora del desarrollo nacional, con autonomía política, fiscal y administrativa. La base de la reestructuración político-nacional es el gobierno local. Histórica y técnicamente la comunidad municipal es fuente de apoyo, de libertad política, de eficacia del gobierno y de transparencia. El gobierno municipal es autónomo, responsable, está sujeto a la voluntad de sus gobernados y

a su libre examen, apartado de toda función o actividad que no sean inherentes al municipio mismo. Sólo en estas condiciones puede cumplir la administración municipal sus fines propios y realizar a plenitud su sentido histórico.

5.5.7 Objetivos de las entidades territoriales

1. Administrar los asuntos municipales y prestar los servicios públicos que determine la Ley.

2. Ordenar el desarrollo de su territorio y construir las obras que demande el progreso municipal.

3. Promover la participación comunitaria y el mejoramiento social y cultural de sus habitantes.

4. Planificar el desarrollo económico, social y ambiental de su territorio, de conformidad con la Ley y en coordinación con otras entidades.

5. Solucionar las necesidades insatisfechas de salud, educación, saneamiento ambiental, agua potable, servicios públicos domiciliarios, vivienda recreación y deporte, con especial énfasis en la niñez, la mujer, la tercera edad y los sectores discapacitados, directamente y en concurrencia, complementariedad y coordinación con las demás entidades territoriales y la Nación, en los términos que defina la Ley.

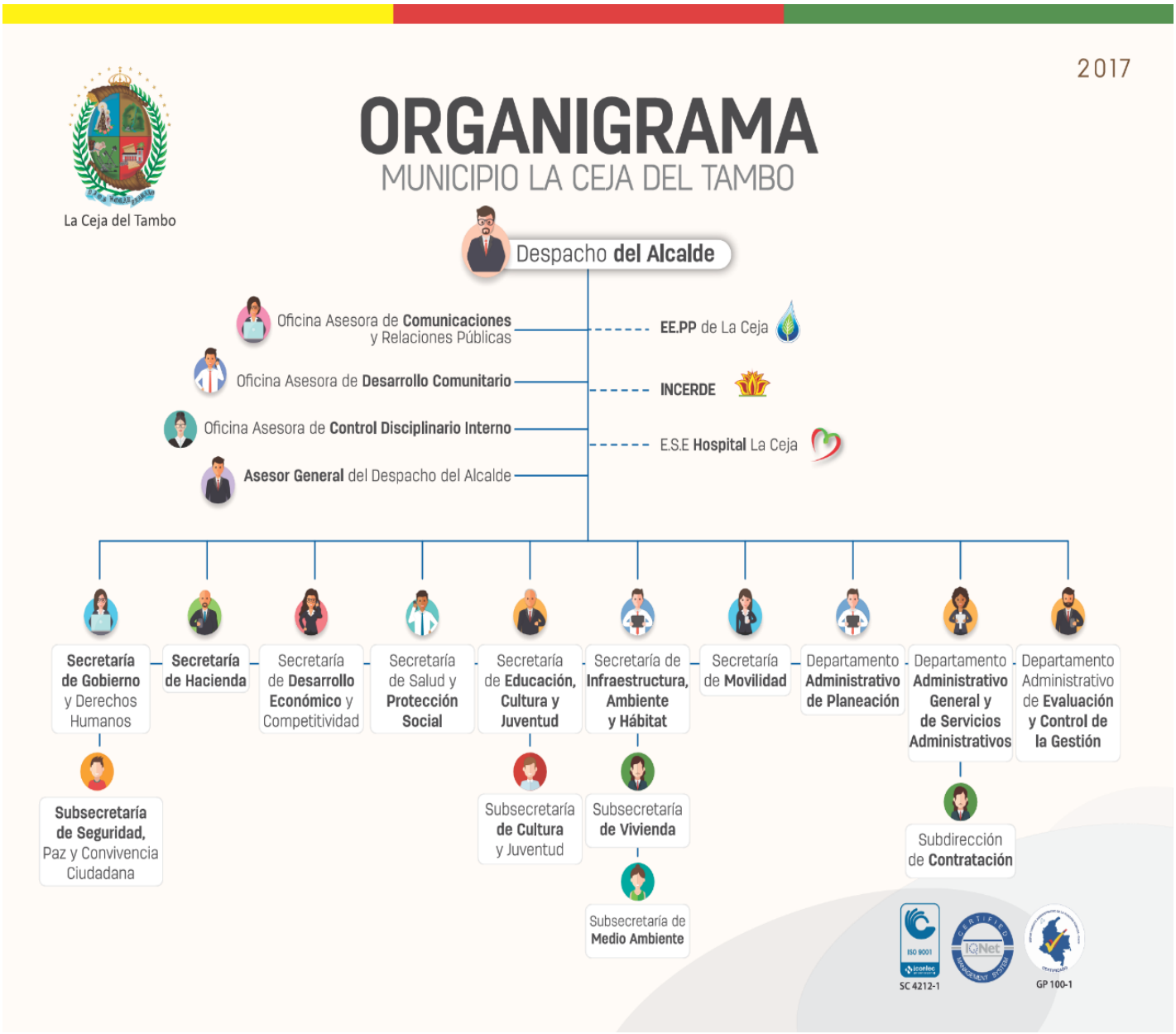
6. Velar por el adecuado manejo de los recursos naturales y del medio ambiente, de conformidad con la Ley.

7. Promover el mejoramiento económico y social de los habitantes del respectivo municipio.

8. Hacer cuanto pueda adelantar por sí mismo, en subsidio de otras entidades territoriales, mientras éstas proveen lo necesario.

9. Las demás que señale la Constitución y la Ley.”

Ilustración 17 - Organigrama (Administración municipal de La Ceja - Antioquia)



5.5.8 Organigrama

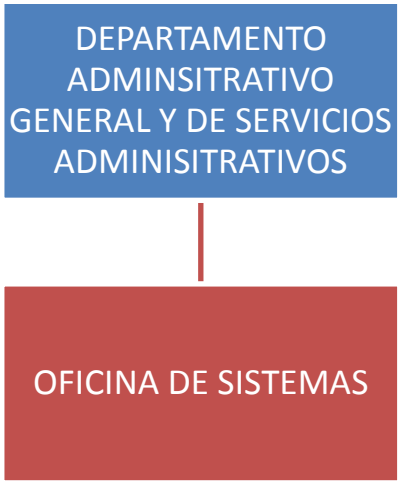
Conformación del equipo de trabajo de la administración municipal

- La administración municipal de La Ceja – Antioquia cuenta con:
  - 10 secretarias,
  - 5 subsecretarias,
  - 3 entidades descentralizadas
  - 5 oficinas adscritas al despacho del alcalde.

- En la actualidad laboran en la administración 320 personas entre empleados, trabajadores públicos, provisionales y contratistas.

5.5.9 Organigrama de la oficina de sistemas

El orden organizacional que se lleva en la dependencia de sistemas es el siguiente.



En la actualidad la oficina de sistemas cuenta con tres personas de tiempo completo (1 ingeniero de sistemas y 2 tecnólogos) cuyas funciones son

Ilustración 18 - Conformación Oficina de Sistemas

CARGO	TITULO	CANTIDAD DE FUNCIONARIOS	FUNCIONES
LÍDER	INGENIERO DE SISTEMAS	1	Diseñar, desarrollar, implantar, evaluar, supervisar, administrar y mantener las plataformas y soluciones tecnológicas que garantizan la operatividad, interconectividad, seguridad, fiabilidad, disponibilidad e integridad de los activos de información de la administración municipal.
TÉCNICO	TECNÓLOGO EN SISTEMAS	2	Prestar apoyo a la oficina de sistemas en actividades de mantenimiento preventivo y correctivo a la infraestructura tecnológica de la administración municipal.

5.5.10 Presupuesto oficina de sistemas

Para el año 2017 la administración municipal de La Ceja cuenta con un presupuesto de $65.202.684.000 y la para la oficina de sistemas en el componente del

presupuesto ORDENAMIENTO TERRITORIAL, programa PLANIFICACIÓN TERRITORIAL subprograma FORTALECIMIENTO DE LOS SISTEMAS DE INFORMACIÓN, le fue asignado $202.460.000. Estos recursos son insuficientes para todas las necesidades que en la actualidad requiere el manteamiento preventivo y correctivo de toda la infraestructura tecnológica que en la actualidad posee la administración municipal de La Ceja.

5.5.11 Tareas periódicas de la oficina de sistemas

Las tareas que se llevan a cabo de forma periódica son:

- Mensualmente se da mantenimiento a las UPS del centro de datos.
- Mensualmente se consideran mantenimientos de limpieza de los servidores de base de datos.
- Periódicamente se actualizan librerías de las aplicaciones informáticas con las que cuenta la administración municipal.
- Actualización diaria de las firmas de antivirus en los servidores Windows.
- Periódicamente se realizan backup de las bases de datos.
- Periódicamente se presta servicio de mantenimiento correctico a la infraestructura de la red por problemas de conexión.

5.5.12 Soporte técnico

Alrededor de 150 computadores, 20 portátiles y 40 impresoras son gestionados por el área técnica, encargada de la instalación, configuración, actualización y mantenimiento de las mismas. Algunas de las actividades que se realiza a la infraestructura tecnológica son por parte del personal de la oficina de sistemas son

- Formular y proponer políticas y normas de seguridad informática, e implementar soluciones de protección de las redes, equipos y sistemas.

- Efectuar la gestión técnica de los activos de tecnologías de información de la administración municipal, coordinando con la Oficina de bienes la Administración, el mantenimiento y actualización de los respectivos inventarios;

- Brindar soporte técnico a los usuarios de equipos y sistemas informáticos de la administración municipal,

- Administrar la infraestructura tecnológica informática y de comunicación de datos de la administración municipal, garantizando su operatividad, disponibilidad y seguridad;

- Efectuar la implementación y gestión del Plan de Contingencia Informático y el Plan de Continuidad de Negocios ante cualquier eventualidad o riesgo.

- Registrar y actualizar la información contenida en el portal institucional y el portal de transparencia del Ministerio, conforme a las normas sobre la materia y en coordinación con los órganos correspondientes, velando por la operatividad, disponibilidad y seguridad de los mismos;

- Coordinar, dirigir y supervisar el uso de los recursos informáticos y de comunicaciones de la administración municipal, proponiendo las directivas y lineamientos necesarios para garantizar su disponibilidad, legalidad y racionalidad;

- Supervisar los trabajos encargados a terceros relacionados a infraestructura tecnológica y aplicativa de la administración municipal.

5.5.13 Incidentes presentados en la infraestructura tecnológica.

- Las baterías de las UPS han cumplido su ciclo de vida y por ende se han presentado apagones ocasionados por descargas eléctricas.
- Algunos computadores de los funcionarios y servidores han sido víctimas de ataques por personas externas.
- Frecuentemente se desconecta el enlace principal con el proveedor de internet.
- La rápida adquisición de equipos produjo problemas de compatibilidad afectando la estabilidad de la red.
- Los funcionarios han descargado archivos adjuntos de correos los cuales estaban infectados por virus informáticos ocasionados pérdidas de información.
- Varios cooler de los servidores han fallado ocasionado en los servidores sobre tensiones y ruidos excesivos en su funcionamiento.
- Falta de material para realizar mantenimientos preventivos y correctivos.
- Algunas impresoras ya han cumplido de ciclo de vida y presentan fallas en su funcionamiento.
- El cableado estructurado es muy antiguo lo cual provoca una gran cantidad de problemas de funcionamiento, como por ejemplo, micro cortes de red, lentitud, cuellos de botella, riesgo de rotura.
- La arquitectura de red actual de la administración municipal está obsoleta y muchos de los dispositivos de conexión ya cumplieron su clico de vida útil lo que ocasiona continuamente altos tiempos de paros de servicios en la red en casos

de fallas, además un alto porcentaje de los equipos están en riesgo de vulnerabilidad de seguridad.

- Malestar en los usuarios internos y externos por fallas en la red de datos

5.5.14 Deficiencias en la infraestructura tecnológica.

- Procesos definidos para la administración de cuentas de usuarios.
- Procedimiento de respuesta ante incidentes
- Respectiva directiva de copias de seguridad
- Sistema de detección de intrusos
- Personal responsable de la seguridad de la información
- Cableado estructurado que cumpla las últimas normas técnicas.
- Ambientes óptimos para el centro de datos
- Red eléctrica deficiente.
- Dispositivos biométricos de acceso al centro de datos

5.5.15 Necesidades de seguridad física

- Acceso no autorizado al centro de datos
- Incumplimiento en el mantenimiento y chequeo del sistema de información
- Uso no autorizado del equipo informático.
- Uso de software infectado por malware.
- Hurto de documentos.
- Hurto de equipos informáticos.
- Destrucción de información.
- Divulgación de información.
- Fugas de información.
- Errores humanos.
- Acceso forzado al centro de datos.
- Manipulación del hardware.
- Sabotaje.
- Falla de suministro eléctrico.
- Falla del equipo informático.
- Errores de hardware.
- Errores de los funcionarios.
- Errores de actualización y mantenimiento de equipos.
- Amenazas a los equipos informáticos por las condiciones ambientales.
- Amansas naturales a la infraestructura tecnológica.
- El rack no cuenta con un sistema de seguridad que restringa el acceso al mismo.

- El rack no cuenta con un sistema de climatización que garantice el óptimo funcionamiento del mismo.
- La oficina donde se encuentra el centro de datos en la actualidad presenta afectaciones en sus techos por ser una edificación antiquísima.
- El control de acceso al edificio se resguarda por dos puertas, una de ellas es controlada por una persona en recepción que se encarga de llevar el control de las personas que ingresan y salen del edificio y la otra puerta no tiene ningún control, solo hay una cámara de seguridad en el primer y tercer piso del palacio consistorial.
- La oficina de sistemas no cuenta con la seguridad adecuada, ya que facialmente se puede ingresar a ella, ya que la edificación (casa consistorial) es una edificación antigua.
- Solo se encuentran interconectados el palacio municipal (casa consistorial), la secretaria de infraestructura y planeación municipal), las otras dependencias tienen el sistemas de voz y datos independientes.

5.5.16 Vulnerabilidades

- Falta de protección física en puertas.
- Acceso no protegido a las instalaciones informáticas.
- Sistemas contra incendios insuficientes.
- Diseño deficiente de edificios. (edificación muy antigua).
- Materiales inflamables en el centro de datos (piso de madera).
- Falta de protección física en las ventanas.
- Paredes que se pueden asaltar físicamente.
- Falta de revisiones de hardware.
- Sistemas sin proteger físicamente.
- Falta de procedimientos.
- Falta de planes de continuidad
- Falta de políticas de seguridad acordes a las nuevas realidades de seguridad informática
- Falta de procesos disciplinarios referentes a los incidentes de seguridad de la información
- Falta de revisiones reguladoras por parte de la dirección.

5.5.17 Clientes y proveedores de la administración municipal

Ilustración 19 - Proveedores, Contribuyentes y Contribuyentes

TIPO	CANTIDAD
PROVEEDORES y CONTRATISTAS	250 (PERSONAS NATURALES y JURÍDICAS)
CONTRIBUYENTES (personas registradas que declaran impuestos a través de su página web	2.227 (PERSONAS NATURALES y JURÍDICAS)
PREDIOS URBANOS	10.240
PREDIOS RURALES	1.200

Fuente: Autor

6 METODOLOGÍA

Para el desarrollo del proyecto se utilizara como metodología de desarrollo los lineamientos de la estrategia gobierno en línea bajo la NORMA TÉCNICA COLOMBIANA ISO 270001:2013 y como metodología para gestión de riegos la metodología MAGERIT

6.1 METODOLOGÍA ISO/IEC 27001:2013

Esta metodología especifica los requisitos que permite establecer, implementar, mantener y mejorar continuamente un sistema de gestión de la seguridad de la información dentro del contexto de la organización; esta metodología contempla ocho (8) fases secuenciales:

Tabla 7 - Requisitos de la NTC ISO/IEC 27001: 2013.

FASE	DESCRIPCIÓN
Herramienta de Diagnostico de Seguridad y Privacidad de la Información	Este instrumento permite establecer el estado de la gestión y adopción de controles técnicos y administrativos al interior de las Entidades Públicas, según lo definido en la Estrategia de Gobierno en Línea. *Este proceso debe generar el documento con el* ***análisis del diagnóstico inicial del SGSI.***
Obtener la aprobación del Dirección para inicial el proyecto	Organizar una reunión con la jefe líder del departamento administrativo general y con la jefe de la oficina de control interno en donde se indicaran los objetivos que se desarrollaran durante la ejecución del proyecto de investigación que se pretende y donde se especificara los beneficios implemera un SGSI en base al estándar ISO/IEC 27001:2013. *Este proceso debe generar el documento requerido por el estándar ISO/IEC 27001:2013 de* ***Soporte y Aprobación por la Dirección****.*
Definir el alcance y los límites del SGSI	Determinar los procesos sobre los cuáles aplicará el Sistema de Gestión de la Seguridad de la Información en la entidad.

	Este proceso debe generar el documento requerido por el estándar ISO/IEC 27001:2013 de ***Alcance del Sistema de Gestión de la Seguridad de la Información.***
Definir la Política de Seguridad.	Actualizar la actual política de información de la entidad. *Este proceso debe generar el documento requerido por el estándar ISO/IEC 27001:2013* ***de Políticas de Seguridad de la Información.***
Identificar los Activos de Información.	Se identifican los activos de información que serán afectados por SGSI, esto permitirá identificar sus responsables, clasificación y su valoración de acuerdo a sus dimensiones (confiabilidad, integridad y disponibilidad), todo ello con el fin de realizar el análisis de Riesgos en base a ellos. *Este proceso debe generar el documento requerido por el estándar ISO/IEC 27001:2013* ***de Inventario de Activos de Información.***
Definir la Metodología de Análisis y Evaluación de Riesgos.	La definición de la metodología para de Evaluación de Riesgos permitirá: • Realizar un inventario de los activos de información de la entidad. • Identificar las vulnerabilidades y amenazas • Determinar el impacto sobre cada uno de los activos cuando se materialice una amenaza. • Definir los controles que permitan minimiza o mitigar el riego. Para esta fase se utilizara la metodología MAGERIT para la gestión de riesgos. *Este proceso debe genera el documento requerido por el estándar ISO/IEC 27001:2013* ***de Metodología de Análisis y Evaluación de Riesgos.***
Plan de Tratamiento de Riesgos.	Definir la forma en cómo se tratarán los riesgos (*mitigarlos, asumirlos, transferirlos a terceros o eliminarlos*).

	Este proceso debe generar los documentos requeridos por el estándar ISO/IEC 27001:2013 de ***Declaración de Aplicabilidad*** *y* ***Plan de Tratamiento de Riesgos****.*
Definir el Plan de Continuidad del Negocio.	Realizar una encuesta a los empleados relativa a la seguridad de la información, su puesto de trabajo y área, con el fin de determinar los servicios críticos que afectan la entidad. *Este proceso debe generar el documento de* ***Plan de Continuidad del Negocio****.*

Fuente: Autor

7 DESARROLLO DEL PROYECTO

Para el desarrollo del proyecto llevaremos a cabo las siguientes actividades

Ilustración 20 - Actividades desarrollo del proyecto

Act.	ACTIVIDAD
1	Análisis diferencial o de brecha
2	Políticas de seguridad de la información
3	Análisis y evaluación de riegos
4	Declaración de aplicabilidad
5	Plan de tratamiento de riesgos
6	Plan de continuidad del negocio

Fuente: Autor

7.1 ANÁLISIS DIFERENCIAL O DE BRECHA

7.1.1 Autodiagnóstico SGSI logro 1: Definición de Marco de Seguridad y Privacidad de la entidad (30%)

Para realizar la evaluación del estado actual en seguridad de la información de la administración municipal de La Ceja - Antioquia objeto de este estudio, se realizó un análisis de brechas “GAP” de las norma ISO 27001:2013 e ISO 27002:2013.

La norma o estándar ISO/IEC 27001:2013 requiere el cumplimiento de ciertos criterios para establecer, implementar, mantener y mejorar continuamente el Sistema de Gestión de la Seguridad de la Información (SGSI) en el contexto de una organización.

Para verificar el estado actual del cumplimiento del estándar ISO/IEC 27001:2013 en la administración municipal de La Ceja-Antioquia, se realiza un Análisis Diferencial de:

- Los numerales obligatorios 4 al 10 (Requisitos de la Norma ISO/IEC 27001:2013) y
- El Anexo A (Dominios, Objetivos de Control y Controles de Seguridad).

Los objetivos del Análisis Diferencial se resumen en:

- Conocer la aplicabilidad y el diferencial referente a los estándares ISO/IEC 27001.
- Obtener una valoración independiente sobre el estado actual de las medidas de seguridad adoptadas por la organización.
- Determinar un Plan de Mejora de la Seguridad adaptado y específico a la organización.
- Oportunidad para concienciar y responsabilizar a las diferentes áreas de la empresa sobre la importancia de la seguridad de la información desde un punto de vista de gestión.

Este análisis permite comparar las condiciones actuales con el fin de encontrar las deficiencias existentes y el nivel de cumplimiento en base al estándar y desarrollar un plan de mejoramiento de acuerdo a los objetivos de seguridad deseados.

Tabla 8 - Valoración cualitativa nivel de cumplimiento del SGSI

Estado	DESCRIPCIÓN
Cumple satisfactoriamente	Existe, es gestionado, se está cumpliendo con lo que la norma ISO27001 versión 2013 solicita, está documentado, es conocido y aplicado por todos los involucrados en el SGSI. **Cumple 100%.**
Cumple parcialmente	Lo que la norma requiere (ISO27001 versión 2013) se está haciendo de manera parcial, se está haciendo diferente, no está documentado, se definió y aprobó pero no se gestiona.

No cumple	No existe y/o no se está haciendo.

Fuente: Autor

Tabla 9- Valoración de cumplimiento del SGSI en la administración municipal de La Ceja-Antioquia

PLANEAR			
ÍTEM	**PREGUNTA**	**VALORACIÓN**	**RECOMENDACIÓN**
1	La entidad cuenta con un autodiagnóstico realizado para medir el avance en el establecimiento, implementación, mantenimiento y mejora continua de su SGSI (Sistema de Gestión de Seguridad de la información?	No cumple	Diligenciar autodiagnóstico de seguridad de la información.
2	La entidad creó un caso de estudio o plan inicial del proyecto, donde se incluyen las prioridades y objetivos para la implementación del SGSI?	Cumple parcialmente	Crear caso de estudio o plan inicial del proyecto que incluya prioridades y objetivos del SGSI, estructura del SGSI.
3	La entidad contó con la aprobación de la dirección para iniciar el proyecto del SGSI?	Cumple satisfactoriamente	Debe existir un documento preliminar de aprobación firmado por parte de la dirección donde se aprueba el inicio del proyecto.
4	La entidad ha identificado los aspectos internos y externos que pueden afectar en el desarrollo del proyecto de implementación del sistema de gestión de seguridad de la información?	No cumple	Se deben identificar los temas tanto externos como internos que pueden afectar el desarrollo de los resultados del sistema.
5	La entidad ha identificado las partes interesadas, necesidades y expectativas de estas respecto al Sistema de Gestión de Seguridad de la Información?	No cumple	Se requiere que se identifiquen las partes interesadas tanto internas como externas, detallando cuáles son sus necesidades y expectativas en la implantación del Sistema de Gestión de Seguridad de la Información.
6	La entidad ha evaluado los objetivos y las necesidades respecto a la Seguridad de la Información?	Cumple parcialmente	Realizar la identificación de los objetivos y las necesidades que tiene la entidad respecto a la seguridad de la Información.

7	En la entidad se ha definido un Comité de Seguridad de la Información?	No cumple	Definir mediante acto administrativo el comité de seguridad de la información que describa las responsabilidades de los integrantes, reuniones entre otros.
8	La entidad cuenta con una definición del alcance y los límites del Sistema de Gestión de Seguridad de la Información?	No cumple	Crear un documento de alcance del Sistema de Gestión de Seguridad de la Información y sus respectivos límites en cuanto a TIC, límites físicos, temas internos y externos.
9	En la entidad existe un documento de política del Sistema de Gestión de Seguridad de la Información, el cual ha sido aprobado por la Dirección?	No cumple	Crear un documento que defina la política general del Sistema de Gestión de Seguridad de la Información y sus respectivos límites. Tener en cuenta objetivos del SGSI, marco regulatorio, el cual debe estar debidamente documentado y socializado.
10	En la entidad existe un documento de roles, responsabilidades y autoridades en seguridad de la información?	No cumple	Se deben definir roles y responsabilidades para cada etapa de la Implementación.
11	La entidad tiene establecido algún proceso para identificar, analizar, valorar y tratar los riesgos de seguridad de la información?	No cumple	Se debe seleccionar una metodología para gestionar los riesgos y describir en una matriz de riesgos los resultados de acuerdo a los criterios de aceptación de los mismos. Nota: Si la entidad ya tiene una matriz de riesgos, se deben identificar los riesgos que apunten a la seguridad de la información.
12	La entidad ha realizado una declaración de aplicabilidad que contenga los controles requeridos por la entidad?	No cumple	Crear documento de declaración de aplicabilidad donde se justifique la inclusión y exclusión de controles del Anexo A de la norma ISO27001 versión 2013.

13	La entidad ha evaluado las competencias de las personas que realizan, bajo su control, un trabajo que afecta el desempeño de la seguridad de la Información?	Cumple parcialmente	Se debe conservar la información que evidencie las competencias del personal que se encuentre involucrado con la seguridad de la información de la entidad. Se debe definir un plan de capacitación con el fin de que dichas personas adquieran las competencias respectivas.
14	La entidad tiene definido un modelo de comunicaciones tanto internas como externas respecto a la seguridad de la información?	Cumple parcialmente	Se debe desarrollar un modelo que indique el contenido de la comunicación; fechas, a quién se comunica y quién comunica.
15	La entidad tiene la información referente al Sistema de Gestión de Seguridad de la Información debidamente documentada y controlada?	No cumple	Toda la documentación generada del Sistema de Gestión de Seguridad de la Información debe estar debidamente documentada.
Fuente: Autor - NTC-ISO-IEC 27001:2013			

7.1.2 Autodiagnóstico SGSI logro 2: implementación del Plan de Seguridad y Privacidad de la Información (40%)

Tabla 10 - Valoración implementación plan de seguridad y privacidad de la información

ESTADO	SIGNIFICADO
Cumple satisfactoriamente	Existe, es gestionado, se está cumpliendo con lo que la norma solicita, está documentado, es conocido y aplicado por todos los involucrados en el SGSI. **Cumple 100%.**
Cumple parcialmente	Lo que la norma requiere se está haciendo de manera parcial, se está haciendo diferente, no está documentado, **se definió pero no se gestiona.**
No cumple	**No existe y/o no se está haciendo.**
No aplica	**El control no es aplicable para la entidad.** En el campo evidencia por favor indicar la justificación respectiva de su no aplicabilidad.

Fuente: Autor

Tabla 11 – Autodiagnóstico. Implementación del Plan de Seguridad y Privacidad de la Información

ANEXO			ESTADO
A5	**POLÍTICAS DE LA SEGURIDAD DE LA INFORMACIÓN**		
A5.1	Orientación de la dirección para la gestión de la seguridad de la información		
Objetivo: Brindar orientación y soporte, por parte de la dirección, para la seguridad de la información de acuerdo con los requisitos del negocio y con las leyes y reglamentos pertinentes			
A5.1.1	Políticas para la seguridad de la información	Control: Se debe definir un conjunto de políticas para la seguridad de la información, aprobada por la dirección, publicada y comunicada a los empleados y a las partes externas pertinentes.	Cumple parcialmente

A5.1.2	Revisión de las políticas para la seguridad de la información.	Control: Las políticas para la seguridad de la información se deben revisar a intervalos planificados o si ocurren cambios significativos, para para asegurar su conveniencia, adecuación y eficacia continuas.	Cumple parcialmente
A6	**ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN**		
A6.1	Organización interna		
Objetivo: Establecer un marco de referencia de gestión para iniciar y controlar la implementación y operación de la seguridad de la información dentro de la organización.			
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.	No cumple
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 organización	No cumple
A6.1.3	Contacto con las autoridades	Control: Se deben mantener contactos apropiados con las autoridades pertinentes.	No cumple
A6.1.4	Contacto con grupos de interés especial	Control: Se deben mantener contactos apropiados con grupos de interés especial u otros foros y asociaciones profesionales especializadas en seguridad	No cumple
A6.1.5	Seguridad de la información en la gestión de proyectos.	Control: La seguridad de la información se debe tratar en la gestión de proyectos, independientemente del tipo de proyecto.	No cumple
A6.2	Dispositivos móviles y teletrabajo		
Objetivo: Garantizar la seguridad del teletrabajo y el uso de dispositivos móviles			

A6.2.1	Política para dispositivos móviles	Control: Se deben adoptar una política y unas medidas de seguridad de soporte, para gestionar los riesgos introducidos por el uso de dispositivos móviles.	No cumple
A6.2.2	Teletrabajo	Control: Se deben implementar una política y unas medidas de seguridad de soporte, para proteger la información a la que se tiene acceso, que es procesada o almacenada en los lugares en los que se realiza teletrabajo.	No cumple
A7	**SEGURIDAD DE LOS RECURSOS HUMANOS**		
A7.1	Antes de asumir el empleo		
Objetivo: Asegurar que los empleados y contratistas comprenden sus responsabilidades y son idóneos en los roles para los que se consideran.			
A7.1.1	Selección	Control: Las verificación antecedentes antes de ingresar a laborar en la entidad.	Cumple parcialmente
A7.1.2	Términos y condiciones del empleo	Control: Los contratos laborales deben establecer sus responsabilidades y de la organización en cuanto a la seguridad de la información.	Cumple parcialmente
A7.2	Durante la ejecución del empleo		
Objetivo: Asegurarse de que los empleados y contratistas tomen conciencia de sus responsabilidades de seguridad de la información y las cumplan.			
A7.2.1	Responsabilidades de la dirección	Control: La dirección debe exigir a todos los empleados y contratistas la aplicación de la seguridad de la información de acuerdo con las políticas y procedimientos establecidos por la entidad.	Cumple parcialmente

A7.2.2	Toma de conciencia, educación y formación en la seguridad de la información.	Control: Todos los empleados de la organización, deben recibir capacitación referida a la seguridad de la información y protección de los activos suministrados por la entidad para la ejecución de sus actividades laborales.	Cumple parcialmente
A7.2.3	Proceso disciplinario	Control: Se debe contar con un proceso formal, el cual debe ser comunicado, para emprender acciones contra empleados que hayan cometido una violación a la seguridad de la información.	No cumple
A7.3	Terminación y cambio de empleo		
Objetivo: Proteger los intereses de la organización como parte del proceso de cambio o terminación de empleo			
A7.3.1	Terminación o cambio de responsabilidades de empleo	Control: Se debe comunicar a todas las personas que ingresan a laborar a la entidad en sus contratos de trabajo las responsabilidades y los deberes de seguridad de la información que deben cumplir después de la terminación o cambio de empleo en la entidad.	No cumple
A8	**GESTIÓN DE ACTIVOS**		
A8.1	Responsabilidad por los activos		
Objetivo: Identificar los activos organizacionales y definir las responsabilidades de protección adecuadas.			
A8.1.1	Inventario de activos	Control: Se deben identificar y mantener actualizado el inventario de los activos utilizados en el procesamiento y almacenamiento de los datos en la entidad	Cumple parcialmente
A8.1.2	Propiedad de los activos	Control: Se debe asignar un responsable a los activos de información de la entidad.	Cumple parcialmente

A8.1.3	Uso aceptable de los activos	Control: Se deben identificar, documentar e implementar reglas para el uso aceptable de información y de activos asociados con información e instalaciones de procesamiento de información.	No cumple
A8.1.4	Devolución de activos	Control: Todos los empleados y usuarios de partes externas deben devolver todos los activos de la entidad que se encuentren a su cargo, al terminar su empleo, contrato o acuerdo.	Cumple parcialmente
A8.2	Clasificación de la información		
Objetivo: Asegurar que la información recibe un nivel apropiado de protección, de acuerdo con su importancia para la organización.			
A8.2.1	Clasificación de la información, etiquetado y manejo de activos	Control: La información se debe clasificar en función de los requisitos legales, a su disponibilidad, integridad y confidencialidad.	No cumple
A8.2.2	Etiquetado de la información	Control: Se debe implementar el procedimiento para el etiquetado de la información de acuerdo a sus dimensiones de integridad, confidencialidad y disponibilidad.	No cumple
A8.2.3	Manejo de activos	Control: Se deben implementar procedimientos que permitan el manejo de activos de acurdo a su clasificación.	No cumple
A8.3	Manejo de medios		
Objetivo: Evitar la divulgación, la modificación, el retiro o la destrucción no autorizados de información almacenada en los medios			
A8.3.1	Gestión de medio removibles	Control: Se deben implementar procedimientos que permitan un manejo adecuado de la información almacenada en los medios extraíbles.	No cumple

A8.3.2	Disposición de los medios	Control: Se debe desarrollar un procedimiento que permita disponer en forma segura de los medios extraíbles cuando ya no se requieran.	No cumple
A8.3.3	Transferencia de medios físicos	Control: De debe desarrollar un procedimiento para garantizar la confiablidad e integridad de la información almacenada en medios extraíbles.	No cumple
A9	**CONTROL DE ACCESO**		
A9.1	Requisitos del negocio para el control de acceso		
Objetivo: Limitar el acceso a información y a instalaciones de procesamiento de información.			
A9.1.1	Política de control de acceso	Control: Se debe actualizar la política de seguridad en cuanto al control de acceso a la infraestructura tecnológica y el acceso a la información.	No cumple
A9.1.2	Acceso a redes y a servicios en red	Control: Se deben establecer los controles específicos que permitan que solo las personas autorizadas puedan acceder a los servicios de la red de datos de la entidad.	No cumple
A9.2	Gestión de acceso de usuarios		
Objetivo: Asegurar el acceso de los usuarios autorizados y evitar el acceso no autorizado a sistemas y servicios.			
A9.2.1	Registro y cancelación del registro de usuarios	Control: Se debe desarrollar un proceso de registro y cancelación de usuarios en los sistemas de información de la entidad.	No cumple
A9.2.2	Suministro de acceso de usuarios	Control: Se debe implementar un proceso que permita la asignación de claves de uso y cancelación de las mismas en los sistemas de información de la entidad.	No cumple
A9.2.3	Gestión de derechos de acceso privilegiado	Control: Se debe desarrollar un procedimiento que permita el control de acceso con privilegios a los en los sistemas de información de la entidad.	Cumple parcialmente

A9.2.4	Gestión de información de autenticación secreta de usuarios	Control: Se debe desarrollar un procedimiento de autenticación de acuerdo las normatividad vigente.	No cumple
A9.2.5	Revisión de los derechos de acceso de usuarios	Control: La oficina de sistemas debe revisar constantemente la asignación de permisos que se le han dado a cada uno de los usuarios que utilizan las herramientas tecnológicas de la entidad.	No cumple
A9.2.6	Retiro o ajuste de los derechos de acceso	Control: La oficina de gestión humana debe informar a la oficina de sistemas cuando un empleado, contratista o practicante termina o tiene un cambio en su contrato de trabajo con la entidad para que ésta realice los respectivos ajustes de los derechos de acceso a los sistemas de información de la entidad.	No cumple
A9.3	Responsabilidades de los usuarios		
Objetivo: Hacer que los usuarios rindan cuentas por la salvaguarda de su información de autenticación.			
A9.3.1	Uso de información de autenticación secreta	Control: Los usuarios deben cumplir con la política de seguridad de la información en lo referente a la autenticación secreta.	No cumple
A9.4	Control de acceso a sistemas y aplicaciones		
Objetivo: Evitar el acceso no autorizado a sistemas y aplicaciones.			
A9.4.1	Restricción de acceso a la información	Control: El acceso a los sistemas de información de la entidad se hará de acuerdo a la política de seguridad de la entidad.	No cumple
A9.4.2	Procedimiento de ingreso seguro	Control: Se debe establecer una política de acceso seguro a los sistemas de información y a la infraestructura tecnológica de la entidad.	No cumple
A9.4.3	Sistema de gestión de contraseñas	Control: Se deben establecer procedimientos para la gestión de contraseñas en la entidad.	No cumple

A9.4.4	Uso de programas utilitarios privilegiados	Control: Se deben restringir las aplicaciones que no estén autorizadas por la entidad.	No cumple
A9.4.5	Control de acceso a códigos fuente de programas	Control: Solo podrá acceder al código fuente de las aplicaciones la empresa que provee el software de la entidad, en este caso SAIMYR S.A.S	No cumple
A10	**CRIPTOGRAFÍA**		
A10.1	Controles criptográficos		
Objetivo: Asegurar el uso apropiado y eficaz de la criptografía para proteger la confidencialidad, autenticidad y/o la integridad de la información			
A10.1.1	Política sobre el uso de controles criptográficos	Control: Se debe aplicar controles criptográficos para la protección de información de reserva o privilegiada que comprometa la seguridad de la entidad.	No cumple
A10.1.2	Gestión de llaves	Control: Se debe implementar programas que permitan la protección de los datos mediante herramientas criptográficas.	No cumple
A11	**SEGURIDAD FÍSICA Y DEL ENTORNO**		
A11.1	Áreas seguras		
Objetivo: Prevenir el acceso físico no autorizado, el daño e la interferencia a la información y a las instalaciones de procesamiento de información de la organización.			
A11.1.1	Perímetro de seguridad física	Control: La entidad debe definir los perímetros de seguridad física que permitan proteger información confidencial o critica de la misma.	No cumple
A11.1.2	Controles de acceso físicos	Control: Se deben establecer controles para las áreas seguras.	No cumple

A11.1.3	Seguridad de oficinas, recintos e instalaciones.	Control: Se deben diseñar y aplicar procedimientos encaminados a la protección física de las áreas destinadas para el procesamiento y almacenamiento de la información.	No cumple
A11.1.4	Protección contra amenazas externas y ambientales.	Control: Se deben diseñar y aplicar procedimientos que permitan protección física contra desastres naturales, ataques maliciosos o accidentes.	Cumple parcialmente
A11.1.5	Trabajo en áreas seguras.	Control: Se deben diseñar y aplicar procedimientos para trabajo en áreas seguras.	No cumple
A11.1.6	Áreas de carga, despacho y acceso público	Control: Se debe controlar el acceso de personas por lugares no permitidos, o aislar estos punto de tal manera que se prohíba el ingreso a las instalaciones de la entidad por ellos.	Cumple parcialmente
A11.2	Equipos		
Objetivo: Prevenir la perdida, daño, robo o compromiso de activos, y la interrupción de las operaciones de la organización.			
A11.2.1	Ubicación y protección de los equipos	Control: Los equipos utilizados para el almacenamiento y procesamiento de la información se deben ubicar en espacios físicos seguros con las debidas medias de seguridad para evitar el acceso a ellos por personas no autorizadas.	Cumple parcialmente
A11.2.2	Servicios de suministro	Control: Instalar dispositivos (UPS) que garanticen el suministro de energía cuando se presentan fallas.	Cumple parcialmente
A11.2.3	Seguridad en el cableado.	Control: Establecer sistemas de cableado eléctrico y de datos de acuerdo a la norma técnica.	No cumple

A11.2.4	Mantenimiento de los equipos.	Control: Se debe establecer un programa de mantenimiento preventivo que permita aumentar la disponibilidad de los equipos y su tiempo de vida útil.	Cumple parcialmente
A11.2.5	Retiro de activos	Control: Se debe establecer un procedimiento para el retiro de los equipos de la entidad, indicando la razón o circunstancia del retiro.	Cumple parcialmente
A11.2.6	Seguridad de equipos y activos fuera de las instalaciones	Control: Se debe implementar medidas que permitan garantizar la seguridad de los equipos de la entidad cuando son retirados de las instalaciones para la realización de trabajo en campo por pare de los funcionarios.	No cumple
A11.2.7	Disposición segura o reutilización de equipos	Control: Se deben definir procedimientos que permitan la reutilización de equipos por parte de otros funcionarios garantizando que la información almacenada en ellos fue correctamente gestionada por la oficina de sistemas de la entidad.	Cumple parcialmente
A11.2.8	Equipos de usuario desatendido	Control: Se debe definir un procedimiento para la salvaguarda de los equipos desatendidos que hacen parte de la infraestructura tecnológica de la entidad.	No cumple
A11.2.9	Política de escritorio limpio y pantalla limpia	Control: Se debe definir una política de escritorio y pantalla limpia en la entidad con el fin de garantizar la seguridad tanto en la documentación física como la seguridad de la información en los equipos de computo.	No cumple
A12	**SEGURIDAD DE LAS OPERACIONES**		
A12.1	Procedimientos operacionales y responsabilidades		
Objetivo: Asegurar las operaciones correctas y seguras de las instalaciones de procesamiento de información.			
A12.1.1	Procedimientos de operación documentados	Control: Se debe llevar registro escrito de cada uno de los procedimientos que están encaminados a la protección y preservación de la información.	No cumple

A12.1.2	Gestión de cambios	Control: Se deber generar documentación escrita acerca de los cambios que se van realizando en la entidad y que afecten la seguridad de la información.	No cumple
A12.1.3	Gestión de capacidad	Control: Se debe realizar monitoreo continuo a los sistemas de información de la entidad de tal manera que se pueda medir su capacidad de respuesta y desempeño a futuro.	No cumple
A12.1.4	Separación de los ambientes de desarrollo, pruebas y operación	Control: Se debe establecer equipos tecnológicos destinados a los ambientes de desarrollo independientes de los equipos de trabajo y así garantizar la integridad de la información.	No cumple
A12.2	Protección contra códigos maliciosos		
Objetivo: Asegurarse de que la información y las instalaciones de procesamiento de información estén protegidas contra códigos maliciosos.			
A12.2.1	Controles contra códigos maliciosos	Control: Se debe instalar software de antivirus en todos los equipos de cómputo y tener un control del mismo desde la oficina de sistemas mediante la instalación de una consola que permita su monitorización y gestión.	Cumple parcialmente
A12.3	Copias de respaldo		
Objetivo: Proteger contra la perdida de datos			
A12.3.1	Respaldo de la información	Control: Se debe establecer un procedimiento que permita la realización periódica de backups y su debida gestión.	Cumple parcialmente
A12.4	Registro y seguimiento		
Objetivo: Registrar eventos y generar evidencia			
A12.4.1	Registro de eventos	Control: Se debe elaborar una base de datos donde se registre cada una de las eventualidades referidas a la seguridad de la información, para poder realizar un seguimiento de las mismas y poder gestionar su debido tratamiento.	No cumple

A12.4.2	Protección de la información de registro	Control: La información referida al registro de eventos se debe proteger en cuanto su integridad y disponibilidad.	No cumple
A12.4.3	Registros del administrador y del operador	Control: Se debe documentar por parte del jefe de la oficina de sistemas cada una de las eventualidades presentadas en la entidad de tal forma que se pueda hacer un seguimiento a las mismas.	No cumple
A12.4.4	Sincronización de relojes	Control: Se deben sincronizar todos los dispositivos que tengan un reloj cronológico instalado, de tal manera que permitan realizar monitorios oportunos a los mismos.	No cumple
A12.5	Control de software operacional		
Objetivo: Asegurarse de la integridad de los sistemas operacionales			
A12.5.1	Instalación de software en sistemas operativos	Control: Se deben implementar procedimientos que no permitan la instalación de software que no haya sido autorizado por la entidad.	No cumple
A12.6	Gestión de la vulnerabilidad técnica		
Objetivo: Prevenir el aprovechamiento de las vulnerabilidades técnicas			
A12.6.1	Gestión de las vulnerabilidades técnicas	Control: Se debe capacitar a los usuarios de los sistemas de información de la entidad sobre el deber de informar a la oficina de sistemas cualquier falla o vulnerabilidad detectada en los equipos asignados, con el fin de actuar de manera rápida y disminuir el riesgo o eliminarlo.	No cumple
A12.6.2	Restricciones sobre la instalación de software	Control: Se deben establecer e implementar dispositivos de seguridad perimetral que no permitan la instalación de software por parte de los usuarios sin la previa autorización de la oficina de sistemas.	No cumple
A12.7	Consideraciones sobre auditorias de sistemas de información		
Objetivo: Minimizar el impacto de las actividades de auditoria sobre los sistemas operativos			
A12.7.1	Controles de auditorías de sistemas de información	Control: Se deben establecer auditorias periódicas que permitan la verificación del cumplimiento legal de los sistemas operativos (licenciamiento).	No cumple
A13	**SEGURIDAD DE LAS COMUNICACIONES**		

A13.1	Gestión de la seguridad de las redes		
Objetivo: Asegurar la protección de la información en las redes, y sus instalaciones de procesamiento de información de soporte.			
A13.1.1	Controles de redes	Control: Se debe realizar monitoreo permanente a la red de datos, para verificar su integridad y disponibilidad.	No cumple
A13.1.2	Seguridad de los servicios de red	Control: Se deben implementar mecanismos de seguridad en la red de datos de tal manera que permitan prevenir y supervisar accesos no autorizados, su uso indebido o la modificación o denegación del servicio por personas no autorizadas.	Cumple parcialmente
A13.1.3	Separación en las redes	Control: Se debe de establecer vVlans o redes lógicas dentro de la misma red de datos para un mejor control de la seguridad y la gestión de equipos.	No cumple
A13.2	Transferencia de información		
Objetivo: Mantener la seguridad de la información transferida dentro de una organización y con cualquier entidad externa.			
A13.2.1	Políticas y procedimientos de transferencia de información	Control: Se debe definir un procedimiento en donde se defina cuál será la forma para la trasferencia de la información, de tal manera que se garantice su confiablidad e integridad.	No cumple
A13.2.2	Acuerdos sobre transferencia de información	Control: Se deben definir acuerdos cuando hay trasferencia de información crítica entre la entidad y terceras partes externas.	No cumple
A13.2.3	Mensajería electrónica	Control: Se debe definir un procedimiento que permita la trasferencia de información de la entidad a través del correo electrónico institucional.	No cumple

A13.2.4	Acuerdos de confidencialidad o de no divulgación	Control: Se deben establecer acuerdos de confidencialidad o de no divulgación con terceros de tal manera que se proteja la información crítica de la entidad.	No cumple
A14	**Adquisición, desarrollo y mantenimiento de sistemas**		
A14.1	Requisitos de seguridad de los sistemas de información		
Objetivo: Asegurar que la seguridad de la información sea una parte integral de los sistemas de información durante todo el ciclo de vida. Esto incluye también los requisitos para sistemas de información que prestan servicios sobre redes.			
A.14.1.1	Análisis y especificación de requisitos de seguridad de la información	Control: Todos los requisitos que permitan el análisis de información deben de estar alineados con la política de seguridad de la información y el SGSI de la entidad.	No cumple
A.14.1.2	Seguridad de servicios de las aplicaciones en redes públicas	Control: Se deben establecer sistemas de seguridad que permitan proteger la red de datos de la entidad de actividades que involucren el robo o pérdida de información a través de aplicaciones fraudulentas y que afecten la integridad, confiablidad y disponibilidad de la información.	No cumple
A.14.1.3	Protección de transacciones de los servicios de las aplicaciones.	Control: Se deben de establecer mecanismos de seguridad que permitan la protección de las transacciones que se realizan a través de la red de datos y que permitan garantizar su integridad.	No cumple
A14.2	Seguridad en los procesos de Desarrollo y de Soporte		
Objetivo: Asegurar que la seguridad de la información este diseñada e implementada dentro del ciclo de vida de desarrollo de los sistemas de información.			
A.14.2.1	Política de desarrollo seguro	Control: Se debe aplicar la política de seguridad de información referida al desarrollo seguro si se llegase a desarrollar alguna aplicación por parte de la oficina de sistemas, aplicando las buenas prácticas en cuanto seguridad	No aplica

		de la información.	
A.14.2.2	Procedimientos de control de cambios en sistemas	Control: Si se llegase a desarrollar alguna aplicación por parte de la oficina de sistemas se deberán aplicar los procedimientos existentes en cuanto al control de los cambios.	No aplica
A.14.2.3	Revisión técnica de las aplicaciones después de cambios en la plataforma de operación	Control: Se deberá revisar las aplicaciones desarrollada por la entidad antes de su lanzamiento y puesta en funcionamiento para evitar posibles fallas en el desarrollo y en la seguridad de la información.	No aplica
A.14.2.7	Desarrollo contratado externamente	Control: Se debe supervisar y hacer seguimiento a los desarrollos de sistemas contratados externamente mediante la firma de contratos de confidencialidad y no divulgación de la información de la entidad.	Cumple parcialmente
A15	**RELACIONES CON LOS PROVEEDORES**		
A15.1	Seguridad de la información en las relaciones con los proveedores.		
Objetivo: Asegurar la protección de los activos de la organización que sean accesibles a los proveedores.			
A15.1.1	Política de seguridad de la información para las relaciones con proveedores	Control: Se debe establecer un procedimiento que permita el establecimiento de reglas claras referidas al manejo de información con proveedores y el acceso de estos a los activos de información cuando se requiera.	No cumple
A15.1.2	Tratamiento de la seguridad dentro de los acuerdos con proveedores	Control: Se deben establecer y acordar todos los requisitos de seguridad de la información pertinentes con cada proveedor que pueda tener acceso, procesar, almacenar, comunicar o suministrar componentes de infraestructura de TI para la información de la organización.	No cumple
A15.1.3	Cadena de suministro de tecnología de información y comunicación	Control: Los acuerdos con proveedores deben incluir requisitos para tratar los riesgos de seguridad de la información asociados con la cadena de suministro de productos y servicios de tecnología de información y comunicación.	No cumple

A15.2	Gestión de la prestación de servicios de proveedores		
Objetivo: Mantener el nivel acordado de seguridad de la información y de prestación del servicio en línea con los acuerdos con los proveedores			
A15.2.1	Seguimiento y revisión de los servicios de los proveedores	Control: La entidad debe hacer seguimiento, revisar y auditar con regularidad la prestación de servicios de los proveedores.	No cumple
A15.2.2	Gestión del cambio en los servicios de los proveedores	Control: Se deben gestionar los cambios en el suministro de servicios por parte de los proveedores, incluido el mantenimiento y las mejoras de las políticas, procedimientos y controles de seguridad de la información existentes, teniendo en cuenta la criticidad de la información, sistemas y procesos de negocio involucrados.	No cumple
A16	**GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN**		
A16.1	Gestión de incidentes y mejoras en la seguridad de la información		
Objetivo: Asegurar un enfoque coherente y eficaz para la gestión de incidentes de seguridad de la información, incluida la comunicación sobre eventos de seguridad y debilidades.			
A16.1.1	Responsabilidades y procedimientos	Control: Se deben establecer procedimientos que permitan determinar el cómo se procede ante el establecimiento de responsabilidades y actuaciones en cuanto al manejo y seguridad de la información.	Cumple parcialmente
A16.1.2	Reporte de eventos de seguridad de la información	Control: Los usuarios de la infraestructura tecnológica de la entidad deben informar a través de los canales de comunicación apropiados, las eventualidades que en materia de seguridad de la información surjan en el desarrollo de sus actividades tan pronto como sea posible.	Cumple parcialmente
A16.1.3	Reporte de debilidades de seguridad de la información	Control: Se debe reportar a la oficina de sistemas cualquier debilidad que en materia de seguridad de la información sea detectada por los usuarios de los sistemas de información de la entidad.	Cumple parcialmente

A16.1.4	Evaluación de eventos de seguridad de la información y decisiones sobre ellos	Control: Cada evento que afecte la seguridad de la información se debe evaluar y tomar las medidas necesarias para mitigarlo o eliminarlo.	No cumple
A16.1.5	Respuesta a incidentes de seguridad de la información	Control: Se debe dar respuesta a los incidentes de seguridad de la información que se presenten en la entidad de acuerdo con procedimientos documentados.	No cumple
A16.1.6	Aprendizaje obtenido de los incidentes de seguridad de la información	Control: Se debe revisar constantemente el reporte de los riegos que se presenten en cuanto a la seguridad de la información y su tratamiento, los cuales servirían de aprendizaje para la mitigación de otros.	No cumple
A16.1.7	Recolección de evidencia	Control: La organización debe definir y aplicar procedimientos para la identificación, recolección, adquisición y preservación de información que pueda servir como evidencia.	No cumple
A17	**ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN DE LA GESTIÓN DE CONTINUIDAD DE NEGOCIO**		
A17.1	Continuidad de Seguridad de la información		
Objetivo: La continuidad de seguridad de la información se debe incluir en los sistemas de gestión de la continuidad de negocio de la organización.			
A17.1.1	Planificación de la continuidad de la seguridad de la información	Control: La organización debe determinar sus requisitos para la seguridad de la información y la continuidad de la gestión de la seguridad de la información en situaciones adversas, por ejemplo, durante una crisis o desastre.	No cumple
A17.1.2	Implementación de la continuidad de la seguridad de la información	Control: La entidad debe establecer los procedimientos y controles para asegurar el nivel de continuidad requerido para la seguridad de la información durante una situación adversa.	No cumple

A17.1.3	Verificación, revisión y evaluación de la continuidad de la seguridad de la información	Control: La organización debe verificar constantemente 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.	No cumple
A17.2	Redundancias		
Objetivo: Asegurar la disponibilidad de instalaciones de procesamiento de información.			
A17.2.1	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.	No cumple
A18	**CUMPLIMIENTO**		
A18.1	Cumplimiento de requisitos legales y contractuales		
Objetivo: Evitar el incumplimiento de las obligaciones legales, estatutarias, de reglamentación o contractuales relacionadas con seguridad de la información y de cualquier requisito de seguridad.			
A18.1.1	Identificación de la legislación aplicable.	Control: Se debe identificar la legislación vigente acerca de la seguridad de la información y aplicarla de acuerdo a las normas y procedimientos establecidos, además de su debida documentación como insumo del Sistemas Integrado de Gestión Organizacional (SIGO) y de la oficina de control interno.	No cumple
A18.1.2	Derechos propiedad intelectual (DPI)	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.	No cumple

A18.1.3	Protección de registros	Control: Los registros se deben proteger contra perdida, destrucción, falsificación, acceso no autorizado y liberación no autorizada, de acuerdo con los requisitos legislativos, de reglamentación, contractuales y de negocio.	No cumple
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.	No cumple
A18.1.5	Reglamentación de controles criptográficos.	Control: Se deben usar controles criptográficos, en cumplimiento de todos los acuerdos, legislación y reglamentación pertinentes.	No cumple
A18.2	Revisiones de seguridad de la información		
Objetivo: Asegurar que la seguridad de la información se implemente y opere de acuerdo con las políticas y procedimientos organizacionales.			
A18.2.1	Revisión independiente de la seguridad de la información	Control: El SGSI debe ser revisado y actualizo constantemente por las entidades de control de la entidad de tal manera que el Sistema se encuentre alineado con la legislación y normatividad vigente.	No cumple
A18.2.2	Cumplimiento con las políticas y normas de seguridad	Control: La oficina de sistemas, la oficina de control interno, el departamento general y la oficina de gestión humana deben revisar constantemente el cumplimiento del SGSI.	No cumple
A18.2.3	Revisión del cumplimiento técnico	Control: El SGSI se deben revisar periódicamente para determinar el cumplimiento con las políticas gubernamentales y normas de seguridad de la información vigentes.	No cumple
Fuente: Autor - NTC-ISO-IEC 27001:2013			

7.1.3 Autodiagnóstico SGSI logro 3: Monitoreo y Mejoramiento Continúo (30 %)

Estado	DESCRIPCIÓN
Cumple satisfactoriamente	Existe, es gestionado, se está cumpliendo con lo que la norma ISO27001 versión 2013 solicita, está documentado, es conocido y aplicado por todos los involucrados en el SGSI. **Cumple 100%.**
Cumple parcialmente	Lo que la norma requiere (ISO27001 versión 2013) se está haciendo de manera parcial, se está haciendo diferente, no está documentado, **se definió y aprobó pero no se gestiona.**
No cumple	**No existe y/o no se está haciendo.**

Tabla 12 – Autodiagnóstico. Monitoreo y Mejoramiento Continúo

ÍTEM	PREGUNTA	VALORACIÓN	RECOMENDACIÓN
1	¿La entidad tiene una metodología para realizar seguimiento, medición y análisis permanente al desempeño de la Seguridad de la Información?	No cumple	Se debe tener en cuenta: • Que se desea medir, • Cuando, • Quien realizará la medición y • Cuando se analizaran los resultados.
2	¿La entidad ha realizado auditorías internas al Sistema de Gestión de Seguridad de la Información?	Cumple parcialmente	Se deben programar auditorias periódicamente con el fin de evaluar y verificar el nivel de cumplimiento del SGSI.
3	¿La entidad cuenta con programas de auditorías aplicables al SGSI donde se incluye frecuencia, métodos, responsabilidades, elaboración de informes?	No cumple	Se debe establecer un plan de auditorías que permitan establecer las frecuencias, métodos y responsabilidades en la elaboración de la documentación requerida por SGSI:.

4	¿La alta dirección realiza revisiones periódicas al Sistema de Gestión de Seguridad de la Información?	No cumple	Se deben realizar revisiones del SGSI por parte de la alta dirección.
5	¿En las revisiones realizadas al sistema por la Dirección, se realizan procesos de retroalimentación sobre el desempeño de la seguridad de la información?	No cumple	Se deben realizar reuniones de retroalimentación en donde realice evaluaciones al SGSI
6	¿Las revisiones realizadas por la Dirección al Sistema de Gestión de Seguridad de la Información, están debidamente documentadas?	No cumple	Se debe documentar las revisiones realizadas por la Alta Dirección con el fin de verificar el estado del SGSI,.

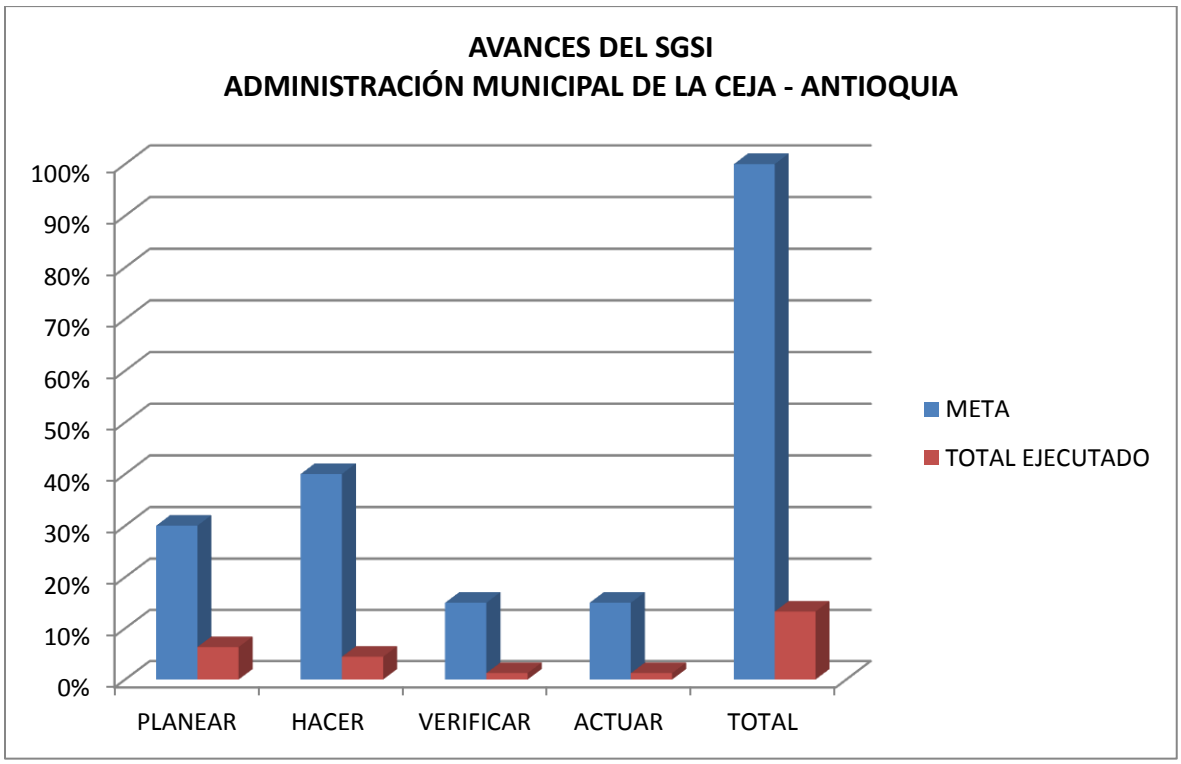
ÍTEM	PREGUNTA	VALORACIÓN	RECOMENDACIÓN
7	¿La entidad da respuesta a las no conformidades referentes a la seguridad de la información presentadas en los planes de auditoria?	Cumple parcialmente	Se deben establecer planes que permitan eliminar las causas de las no conformidades referidas a la seguridad de la información.
8	¿La entidad ha implementado acciones a las no conformidades de seguridad de la información presentadas?	No cumple	Toda la información de acciones realizadas al SGSI debe ser documentada.
9	¿La entidad revisa la eficacia de las acciones correctivas tomadas por la presencia de una no conformidad de seguridad de la información?	No cumple	Se debe evaluar la eficacia de las acciones correctivas con el fin de verificar que la no conformidad no se vuelva a presentar.
10	¿La entidad realiza cambios al Sistema de Gestión de Seguridad de la Información después de las acciones tomadas?	No cumple	Toda la información de cambios al SGSI debe ser documentada.

11	¿La entidad documenta la información referente a las acciones correctivas que toma respecto a la seguridad de la información?	No cumple	Toda la información de cambios al Sistema de Gestión de Seguridad de la Información debe ser documentada.
12	¿La entidad realiza procesos de mejora continua para el Sistema de Gestión de Seguridad de la Información?	No cumple	Toda la información de mejora al Sistema de Gestión de Seguridad de la Información debe ser documentada.

Fuente: Autor

	FASE	META	TOTAL EJECUTADO
LOGRO1	PLANEAR	30%	6,3%
LOGRO2	HACER	40%	4,4%
LOGRO3	VERIFICAR	15%	1,3%
	ACTUAR	15%	1,3%
	TOTAL	100%	13,3%

Tabla 13 - Análisis avances SGSI en la entidad



Fuente: Autor

Tabla 14 - Nivel de cumplimiento del SGSI

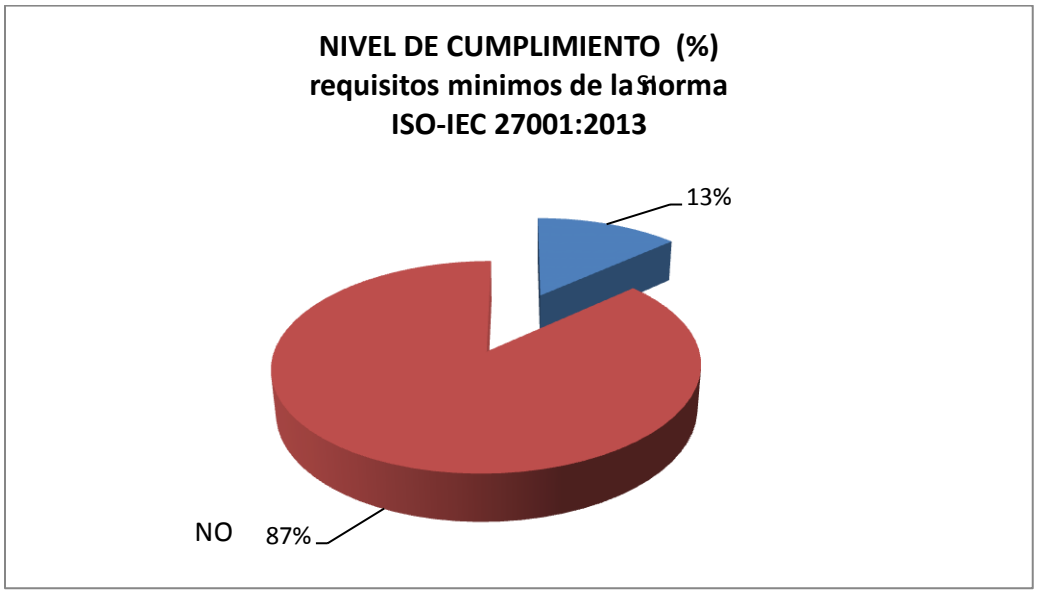


Tabla 15 - Cumplimiento del SGSI por dominio

POR DOMINIO DE CONTROL						
NOMBRE DOMINIOS DE CONTROL	CONTROLES QUE APLICAN	PESO CONTROLES IMPLEMENTADOS Y PARCIALMENTE IMPLEMENTADOS	IMPLEMENTADOS	PARCIALMENTE	NO CUMPLE	NO APLICA
DOMINIO 5 – POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN	2	1	0	2	0	0
DOMINIO 6 – ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN	7	0	0	0	7	0
DOMINIO 7 – SEGURIDAD DE LOS RECURSOS HUMANOS	6	2	0	4	2	0
DOMINIO 8 – GESTIÓN DE ACTIVOS	10	1,5	0	3	7	0
DOMINIO 9 – CONTROL DE ACCESO	14	0,5	0	1	13	0
DOMINIO 10 – CRIPTOGRAFÍA	2	0	0	0	2	0
DOMINIO 11 – SEGURIDAD FÍSICA Y DEL ENTORNO	15	3,5	0	7	8	0
DOMINIO 12 – SEGURIDAD DE LAS OPERACIONES	14	1	0	2	12	0
DOMINIO 13 – SEGURIDAD DE LAS COMUNICACIONES	7	0,5	0	1	6	0

DOMINIO 14 – ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS	7	0,5	0	1	6	6
DOMINIO 15 – RELACIÓN CON LOS PROVEEDORES	5	0	0	0	5	0
DOMINIO 16 – GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN	7	1,5	0	3	4	0
DOMINIO 17 – ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN DE LA GESTIÓN DE CONTINUIDAD DE NEGOCIO	4	0	0	0	4	0
DOMINIO 18 – SEGURIDAD DE LAS COMUNICACIONES	8	0	0	0	8	0
	108					

Ilustración 21 - Grafico (Análisis por dominios NTC ISO 27001:2013

Fuente: Autor

Al revisar detalladamente el estado de cada dominio, se encuentra lo siguiente:

- A5. Política de Seguridad.

La administración municipal de La Ceja-Antioquia dispone de una política de seguridad de la información, pero no se tienen claro en qué momento deben realizan revisiones periódicas de la misma.

- A6. Organización de la seguridad de la Información.

Se evidencia un compromiso por parte de la dirección al abordar la implementación de buenas prácticas en seguridad de la información alineadas a la norma ISO27001 y al manual 3.1 de Gobierno en Línea. Sin embargo, se debe establecer un Comité de Seguridad de la Información, que tenga las funciones de promover la seguridad de la información en cada uno de los funcionarios y contratistas de la entidad, además que realice controles de forma periódica al cumplimiento de las políticas.

A7. Seguridad de Recurso Humano.

Se evidencia un nivel de implementación para los controles de este dominio muy bajo en algunos aspectos.

A8. Gestión de Activos.

Respecto a este dominio la entidad no cuenta con un avance importante, se necesitan algunas mejoras para llegar al nivel que garantice la seguridad de la información.

A9. Control de Acceso.

Este dominio cuenta con un nivel bajo de implementación en el cual se estableció que existen pocos controles avanzados, Sin embargo, se debe considerar la importancia que tiene el manejo de las contraseñas y concientizar que este control puede mitigar algunos riesgos.

A10. Criptografía.

En este dominio la corporación no tiene ningún avance.

A11. Seguridad Física y Ambiental.

En este dominio también se evidencia algunas falencias en cuanto a controles destinados a la seguridad física y ambiental.

A12. Gestión de Comunicaciones y Operaciones.
En este dominio se detectó ausencia de documentación o falta de instrucción técnica que describa la implementación de muchos controles que se analizan en este dominio, pero es un control avanzado que puede crecer rápidamente.

A13. Seguridad de las Comunicaciones.
En este dominio se detectó ausencia de documentación o falta de instrucción técnica que describa la implementación de muchos controles que se analizan en este dominio, pero es un control avanzado que puede crecer rápidamente.

A14. Adquisición, desarrollo y mantenimiento de los sistemas de información.
Se aprecia un nivel muy preocupante en los controles que se implementan en este dominio y es importante plantear una metodología para reducir la brecha y cumplir con los objetivos pactados para el desarrollo del SGSI.

A15. Relaciones con los Proveedores.
En cuanto a este dominio, los controles se encuentran de una forma inexistente y es en el que la entidad debe trabajar más fuerte para cumplir con el objetivo planteado.

A16. Gestión de Incidentes de la Seguridad de la Información.
En cuanto a este dominio, los controles se encuentran de una forma inexistente y es en el que la entidad debe trabajar más fuerte para cumplir con el objetivo planteado.

A17. Gestión de la Continuidad de Negocio.
La implementación de este control se ve apoyada en el proyecto planteado por la Oficina de sistemas, que generaría un nivel de seguridad, confianza y respaldo a la información almacenada, garantizando la continuidad del negocio y mitigando muchos riesgos que se pueden presentar.

A.18 Cumplimiento.
Se debe trabajar en la implementación de los siguientes controles:

- Identificación de la legislación aplicable y tratamiento de datos de carácter personal conforme la ley 1581 (protección de datos personales)
- Reglamentación de controles criptográficos.
- SGSI basado en las normas ISO/IEC 27001:
- Protección de los registros de la organización.
- Cumplimiento con las políticas y normas de seguridad.
- Controles de auditoría de los sistemas de información.

- Protección de las herramientas de auditoría de los sistemas de información.

Los controles críticos (aquellos que aún no están implementados) son los siguientes:

- 5.1.2 Revisión de la política de seguridad de la información.
- 6.1.1 Asignación de responsabilidades para la seguridad de la información.
- 6.1.2 Distribución de funciones.
- 6.1.4 Contactos con grupos de interés especiales
- 6.2.2 Trabajo remoto
- 7.1.1 Selección
- 7.1.2 Términos y condiciones laborales.
- 7.2.1 Responsabilidades de la dirección.
- 7.2.2 Educación, formación y concienciación sobre seguridad de la información.
- 7.3.1 Responsabilidades en la terminación.
- 8.2.2 Etiquetado de información
- 8.2.3 Manejo de información
- 8.3.2 Eliminación de los medios
- 9.2.4 Gestión de contraseñas para usuarios.
- 9.4.5 Control de acceso al código fuente de los programas.
- 10.1.1 Política sobre el uso de controles criptográficos.
- 10.1.2 Gestión de llaves.
- 11.1.2 Controles de acceso físico
- SGSI basado en las normas ISO/IEC 27001:2013
- 11.1.3 Seguridad de oficinas, recintos e instalaciones
- 11.1.5 Trabajo en áreas seguras
- 11.1.6 Áreas de carga, despacho y acceso público.
- 11.2.1 Ubicación y protección de los equipos.
- 11.2.5 Seguridad de los equipos fuera de las instalaciones.
- 12.1.1 Documentación de los procedimientos de operación
- 12.1.2 Gestión del cambio.
- 12.1.4 Separación de las instalaciones de desarrollo, prueba y producción.
- 12.6.1 Control de vulnerabilidades técnicas
- 12.7.1 Controles de auditoría de los sistemas de información.
- 13.1.3 Separación en las redes.
- 13.2.4 Acuerdos de confidencialidad.
- 14.1.1 Análisis y especificación de los requisitos de seguridad.
- 14.1.2 Seguridad de servicios de las aplicaciones en redes públicas

- 14.2.3 Revisión técnica de las aplicaciones después de los cambios en el sistema operativo.
- 14.2.6 Ambiente de desarrollo seguro
- 14.2.7 Desarrollo de software contratado externamente.
- 14.2.8 Pruebas de seguridad del sistema
- 14.2.9 Pruebas de aceptación del sistema.
- 14.3.1 Protección de los datos de prueba del sistema.
- SGSI basado en las normas ISO/IEC 27001:
- 15.1.1 Identificación de los riesgos relacionados con las partes externas.
- 15.1.2 Consideraciones de seguridad en los acuerdos con terceras partes.
- 15.1.3 Cadena de suministro de tecnología de información y comunicación
- 15.2.1 Monitoreo y revisión de los servicios por terceras partes.
- 15.2.2 Gestión de los cambios en los servicios por terceras partes.
- 16.1.1 Responsabilidades y procedimientos
- 16.1.2 Reporte sobre eventos de seguridad de la información
- 16.1.3 Reporte sobre las debilidades de la seguridad
- 16.1.4 Evaluación de eventos de seguridad de la información y decisiones sobre ellos
- 16.1.5 Respuesta a incidentes de seguridad de la información
- 16.1.6 Aprendizaje debido a los incidentes de seguridad de la información.
- 16.1.7 Recolección de evidencia.
- 17.1.3 Verificación, evaluación y revisión de la continuidad de la seguridad de la información
- 18.1.3 Protección de los registros de la organización.
- 18.1.4 Protección de los datos y privacidad de la Información Personal.
- 18.1.5 Reglamentación de los controles criptográficos.
- 18.2.1 Revisión independiente de la seguridad de la información.
- 18.2.2 Cumplimiento con las políticas y normas de seguridad.
- 18.2.3 Verificación del cumplimiento técnico

Mediante este Análisis Diferencial es posible determinar que en la administración municipal de La Ceja, no cumple con la mayoría de los Dominios, Objetivos de Control y Controles de Seguridad propuestos en la norma ISO/IEC 27001:2013.

Esto se refleja en que no se tiene la documentación correspondiente al estándar ISO/IEC 27001:2013 así como tampoco el empleo de mecanismos de seguridad en la transmisión de la información.

Por otro lado, aunque las instalaciones físicas estén protegidas con algunos controles de acceso y vigilancia, el personal y algunos activos informáticos no están lo suficientemente protegidos ante una eventualidad de orden mayor, y no existen procedimientos de contingencia para garantizar la continuidad de las operaciones.

7.2 POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

7.2.1 Introducción

La política de alto nivel o política general, aborda la necesidad de la implementación de un sistema de gestión de seguridad de la información (SGSI) planteado desde la descripción del quién, qué, por qué, cuándo y cómo, en torno al desarrollo de la implementación del SGSI.

La administración municipal del municipio de La Ceja – Antioquia determina la información como un activo estratégico y de alta importancia para la entidad que permite el desarrollo continuo de la misión y el cumplimiento del objetivo de la misma, lo cual genera la necesidad de implementar reglas y medidas que permitan proteger la confidencialidad, integridad y disponibilidad en todo el ciclo de vida de la información.

El presente manual se establece las políticas de seguridad de la información las cuales deben ser adoptadas por los funcionarios, contratistas, personal en comisión administrativa, visitantes y terceros que presten sus servicios o tengan algún tipo de relación con la administración municipal; estas se encuentran enfocadas al cumplimiento de la normatividad legal Colombiana vigente y a las buenas prácticas de seguridad de la información, basadas en la norma ISO 27001/2013 y al modelo de seguridad y privacidad de la información de la estrategia Gobierno en Línea (GEL) del Ministerio de Tecnologías de la Información y las Comunicaciones de Colombia, la legislación de la Ley de Protección de Datos Personales, Transparencia y Acceso a la Información Pública, entre otras, las cuales se deben tener en cuenta para la gestión de la información.

Con la implementación de un SGSI por parte de las Entidades del Estado se busca contribuir al incremento de la transparencia en la Gestión Pública, promoviendo el uso de las mejores prácticas de Seguridad de la Información como base de la aplicación del concepto de Seguridad Digital.

De acuerdo con lo anterior, esta política aplica a la Entidad según como se defina en el alcance, sus funcionarios, terceros, aprendices, practicantes, proveedores y

la ciudadanía en general, teniendo en cuenta que los principios sobre los que se basa el desarrollo de las acciones o toma de decisiones alrededor del SGSI estarán determinados por las siguientes premisas:

- Minimizar el riesgo en las funciones más importantes de la entidad.
- Cumplir con los principios de seguridad de la información.
- Cumplir con los principios de la función administrativa.
- Mantener la confianza de sus clientes, socios y empleados.
- Apoyar la innovación tecnológica.
- Proteger los activos tecnológicos.
- Establecer las políticas, procedimientos e instructivos en materia de seguridad de la información.

Esta política de seguridad de la información es una adaptación de otras políticas de entidades oficiales, que a través del tiempo las han actualizado a las nuevas realidades tecnologías y a las nuevas amenazas que día a día surgen contra la seguridad de la información, además se toma como referente los controles planteados por la norma ISO270001

7.2.2 Objetivos

7.2.2.1 GENERAL

- Mantener un ambiente razonablemente seguro, alineado a la misión de la administración municipal y que permita proteger los activos de información de la misma, así como el uso adecuado de los recursos y gestión del riesgo, con el fin de preservar la disponibilidad, integridad y confidencialidad de la información y el aseguramiento de la continuidad del negocio.

7.2.2.2 ESPECÍFICOS

- Proteger los activos de información de la administración municipal, con base en los criterios de confidencialidad, integridad y disponibilidad.

- Definir las directrices de la administración municipal para la correcta valoración, análisis y evaluación de los riesgos de seguridad asociados a la información y su impacto, identificando y evaluando diferentes opciones para su tratamiento con el fin de garantizar la continuidad e integridad de los sistemas de información.

- Administrar los riesgos de seguridad de la información para mantenerlos en niveles aceptables.

- Sensibilizar y capacitar a los servidores públicos, proveedores y partes interesadas acerca del Sistema de Gestión de Seguridad de la Información – SGSI, fortaleciendo el nivel de conciencia de los mismos, en cuanto a la necesidad de salvaguardar los activos de información institucionales.

- Monitorear el cumplimiento de los requisitos de seguridad de la información, mediante el uso de herramientas de diagnóstico, revisiones por parte de la Alta Dirección y auditorías internas planificadas a intervalos regulares.

- Implementar acciones correctivas y de mejora para el Sistema de Gestión de Seguridad de la Información - SGSI.

- Mantener la Política de Seguridad de la Información actualizada, vigente, auditada dentro del marco determinado por los riesgos globales y específicos de la administración municipal para asegurar su permanencia y nivel de eficacia.

7.2.3 Alcance

Las Políticas de Seguridad de la Información son aplicables para todos los aspectos administrativos y de control que deben ser cumplidos por los directivos, funcionarios, contratistas y terceros que presten sus servicios o tengan algún tipo de relación con la administración municipal, para el adecuado cumplimiento de sus funciones y para conseguir un adecuado nivel de protección de las características de calidad y seguridad de la información, dentro de un marco de legalidad, de adaptación dinámica y puntual de las condiciones variables del entorno y de la protección adecuada de los objetivos de misionales de la entidad .

7.2.4 Términos y definiciones

- **SEGURIDAD DE LA INFORMACIÓN**

La Seguridad de la Información consiste en asegurar que los recursos del Sistema de Información de una organización se utilicen de la forma que ha sido decidido y el acceso de información se encuentra contenida, así como controlar que la

modificación solo sea posible por parte de las personas autorizadas para tal fin y por supuesto, siempre dentro de los límites de la autorización.[5]
La seguridad de la información se entiende como la preservación de las siguientes características:

- ✓ **Confidencialidad**: se garantiza que la información sea accesible sólo a aquellas personas autorizadas a tener acceso a la misma.
- ✓ **Integridad**: se salvaguarda la exactitud y totalidad de la información y los métodos de procesamiento.
- ✓ **Disponibilidad**: se garantiza que los usuarios autorizados tengan acceso a la información y a los recursos relacionados con la misma, toda vez que lo requieran.

Adicionalmente se deberán considerar los siguientes conceptos:

- **Activo**: Es todo aquello que tiene valor para su empresa.

- **Activos de información**: Son los elementos que la Seguridad de la Información debe proteger. Por lo que son tres elementos lo que forman los activos:

    - **Información**: es el objeto de mayor valor para la empresa.
    - **Equipos**: suelen ser software, hardware y la propia organización.
    - **Usuarios**: son las personas que usan la tecnología de la organización.

    - **Datos**: Son todos aquellos elementos básicos de la información (en cualquier formato) que se generan, recogen, gestionan, y se transmite información.

    - **Aplicaciones**: Es todo el software que se utiliza para la gestión de la información. Ejemplo: SAIMYR.

    - **Personal**: Es todo el personal de la administración municipal, los funcionarios, los contratistas, los clientes, usuarios y en general, todos aquellos que tengan acceso de una manera u otra a los activos de información de la entidad.
    - **Tecnología**: Son todos los equipos utilizados para gestionar la información y las comunicaciones Ejemplo: equipo de cómputo, teléfonos, impresoras.

- **Instalaciones**: Son todos los lugares en los que se alojan los sistemas de información.

[5] https://www.pmg-ssi.com/2015/05/iso-27001-que-significa-la-seguridad-de-la-informacion/

- **Equipamiento auxiliar:** Son todos aquellos activos que dan soporte a los sistemas de información.

- **Administración de incidentes de seguridad:** Procedimientos, estrategias y herramientas de control, enfocados a una correcta evaluación de las amenazas existentes, en este caso hacia toda la infraestructura de TI, se basa en un análisis continuo y mejorado del desempeño de todos los activos y recursos gerenciales que tiene la entidad.

Su objetivo principal es atender y orientar las acciones inmediatas para solucionar cualquier situación que cause una interrupción de los diferentes servicios que presta la entidad, de manera rápida y eficaz. No se limita a la solución de problemas específicos sino a buscar las causas que determinaron el incidente limitando el marco de acción de futuras ocurrencias, su enfoque se base en tres pilares fundamentales:

• Detectar cualquier alteración en los servicios TI.
• Registrar y clasificar estas alteraciones.
• Asignar el personal encargado de restaurar el servicio.

- **Alcance**: Ámbito de la organización que queda sometido al Sistema de Gestión de Seguridad de la Información - SGSI. Debe incluir la identificación clara de las dependencias, interfaces y límites con el entorno, sobre todo si sólo incluye una parte de la organización.

- **Alerta**: Una notificación formal de que se ha producido un incidente relacionado con la seguridad de la información que puede evolucionar hasta convertirse en desastre.

- **Amenaza**: Según [ISO/IEC 13335-1:2004): causa potencial de un incidente no deseado, el cual puede causar el daño a un sistema o la organización.

- **Autenticación:** Proceso que tiene por objetivo asegurar la identificación de una persona o sistema.

- **Autenticidad**: Los activos de información solo pueden estar disponibles verificando la identidad de un sujeto o recurso, es la propiedad que garantiza que la identidad de un sujeto o recurso es la que declara y se aplica a entidades tales como usuarios, procesos, sistemas de información.

- **Checklist**: Lista de apoyo para el auditor con los puntos a auditar, que ayuda a mantener claros los objetivos de la auditoría, sirve de evidencia del plan de auditoría, asegura su continuidad y profundidad y reduce los prejuicios del auditor y su carga de trabajo, Este tipo de listas también se pueden utilizar durante la implantación del SGSI para facilitar su desarrollo.

- **Confiabilidad**: Se puede definir como la capacidad de un producto de realizar su función de la manera prevista, De otra forma, la confiabilidad se puede definir también como la probabilidad en que un producto realizará su función prevista sin incidentes por un período de tiempo especificado y bajo condiciones indicadas.

- **Confidencialidad**: Acceso a la información por parte únicamente de quienes estén autorizados, Según [ISO/IEC 13335-1:2004]:" característica/propiedad por la que la información no está disponible o revelada a individuos, entidades, o procesos no autorizados.

- **Control**: son todas aquellas políticas, procedimientos, prácticas y las estructuras organizativas concebidas para mantener los riesgos de seguridad de la información por debajo del nivel de riesgo asumido, (Nota: Control es también utilizado como sinónimo de salvaguarda).

- **Denegación de servicios:** Acción iniciada por agentes externos (personas, grupos, organizaciones) con el objetivo de imposibilitar el acceso a los servicios y recursos de una organización durante un período indefinido de tiempo. La mayoría de ocasiones se busca dejar fuera de servicio los servidores informáticos de una compañía o en su defecto en situaciones más complejas ocasionar graves daños, para que no puedan utilizarse ni consultarse servicios importantes. Un aspecto a resaltar es el gran daño a la imagen y reputación de las entidades que estas acciones dejan en el ambiente público.

- **Desastre**: Cualquier evento accidental, natural o malintencionado que interrumpe las operaciones o servicios habituales de una organización durante el tiempo suficiente como para verse afectada de manera significativa.

- **Gusano (Worm):** Es un programa malicioso de computador que tiene la capacidad de duplicarse a sí mismo. A diferencia del virus, no altera

información, aunque casi siempre causan problemas de red debido al consumo de ancho de banda y su gran facilidad para mutar.

- **Impacto**: Resultado de un incidente de seguridad de la información.

- **Incidente:** Según [ISO/IEC TR 18044:2004]: Evento único o serie de eventos de seguridad de la información inesperados o no deseados que poseen una probabilidad significativa de comprometer las operaciones del negocio y amenazar la seguridad de la información.

- **Información**: La información constituye un importante activo, esencial para las actividades de una organización y, en consecuencia, necesita una protección adecuada. La información puede existir de muchas maneras, es decir puede estar impresa o escrita en papel, puede estar almacenada electrónicamente, ser transmitida por correo o por medios electrónicos, se la puede mostrar en videos, o exponer oralmente en conversaciones.

- **Ingeniería Social:** Es la manipulación de las personas para conseguir que hagan que algo debilite la seguridad de la red o faciliten información con clasificación confidencial o superior.

En el campo de la seguridad informática, es un método o forma de ataque con técnicas que buscan persuadir al atacado ganando su confianza, obteniendo información privilegiada de carácter personal (contraseñas de cuentas bancarias, datos personales), igualmente apropiarse de información vital para una organización. Existen en la actualidad diversidad de medios para llevar a cabo esta actividad, un uso común es a través de correos electrónicos o llamadas al lugar de trabajo o residencia, de ahí la importancia de tener una buena cultura digital respecto a que información suministramos.

- **Inventario de activos:** Lista de todos aquellos recursos (físicos, de información, software, documentos, servicios, personas, reputación de la organización, etc.) dentro del alcance del SGSI, que tengan valor para la organización y necesiten por tanto ser protegidos de potenciales riesgos.

- **IPS**: Sistema de prevención de intrusos. Es un dispositivo que ejerce el control de acceso en una red informática para proteger a los sistemas computacionales de ataques y abusos.

- **ISO**: Organización Internacional de Normalización, con sede en Ginebra (Suiza). Es una agrupación de organizaciones nacionales de normalización cuyo objetivo es establecer, promocionar y gestionar estándares.

- **ISO 27001**: Estándar para sistemas de gestión de la seguridad de la información adoptado por ISO transcribiendo la segunda parte de BS 7799. Es certificable. Primera publicación en 2005, segunda publicación en 2013.

- **Keyloggers**: Son software o aplicaciones que almacenan información digitada mediante el teclado de un computador por un usuario; es común relacionar este termino con malware del tipo daemon (demonio), es decir, actúa como un proceso informático que no interactúa con el usuario, ya que se ejecuta en segundo plano. Usualmente puede ser un tipo de software o un dispositivo hardware que se encarga de registrar las pulsaciones que se hacen con el teclado, para posteriormente memorizarlas en un archivo o enviarlas a través de internet.

- **Legalidad**: El principio de legalidad o Primacía de la ley es un principio fundamental del Derecho público conforme al cual todo ejercicio del poder público debería estar sometido a la voluntad de la ley de su jurisdicción y no a la voluntad de las personas (ej. el Estado sometido a la constitución o al Imperio de la ley). Por esta razón se dice que el principio de legalidad establece la seguridad jurídica, Seguridad de Información, Seguridad informática y garantía de la información.

- **No conformidad**: Situación aislada que, basada en evidencias objetivas, demuestra el incumplimiento de algún aspecto de un requerimiento de control que permita dudar de la adecuación de las medidas para preservar la confidencialidad, integridad o disponibilidad de información sensible, o representa un riesgo menor.

- **Phishing**: Tipo de delito encuadrado dentro del ámbito de las estafas, que se comete mediante el uso de un tipo de ingeniería social caracterizado por intentar adquirir información confidencial de forma fraudulenta (como puede ser una contraseña o información detallada sobre tarjetas de crédito u otra información bancaria), mediante una aparente comunicación oficial electrónica.

- **Plan de continuidad del negocio** (Bussines Continuity Plan): Plan orientado a permitir la continuación de las principales funciones de la Entidad en el caso de un evento imprevisto que las ponga en peligro.

- **Plan de tratamiento de riesgos** (Risk treatment plan): Documento de gestión que define las acciones para reducir, prevenir, transferir o asumir los riesgos de seguridad de la información inaceptables e implantar los controles necesarios para proteger la misma.

- **Política de seguridad:** Documento que establece el compromiso de la Dirección y el enfoque de la organización en la gestión de la seguridad de la información. Según [ISO/IEC 27002:20005): intención y dirección general expresada formalmente por la Dirección.

Política de escritorio despejado: Se define como la política que establece e indica a los funcionarios, contratista y demás colaboradores del DAPRE a asegurar la información pública reservada o información pública clasificada (privada o semiprivada) en lugares que ofrezca la protección necesaria, así mismo los escritorios deben permanecer libres de documentos o informaciones susceptibles de ser afectados en su integridad, confidencialidad y/o disponibilidad.

- **Riesgo**: Posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información. Según [ISO Guía 73:2002]: combinación de la probabilidad de un evento y sus consecuencias.

- **Seguridad de la información:** Hace referencia a la preservación de la confidencialidad (propiedad de que la información, significa que no esté disponible o revelada a individuos no autorizados, entidades o procesos.), integridad (protección de la exactitud e integridad de los activos) y disponibilidad (propiedad de ser accesibles y utilizables a la demanda por una entidad autorizada) de la información.

- **Spamming**: Se llama spam, correo basura o sms basura a los mensajes no solicitados, habitualmente de tipo publicitario, enviados en grandes cantidades (incluso masivas) que perjudican de alguna o varias maneras al receptor. La acción de enviar dichos mensajes se denomina spamming. La vía más usada es el correo electrónico.

- **Sniffers**: Programa de captura de las tramas de red. Generalmente se usa para gestionar la red con una finalidad docente o de control, aunque también puede ser utilizado con fines maliciosos.

- **Servicio:** Es el conjunto de acciones o actividades de carácter misional diseñadas para incrementar la satisfacción del usuario, dándole valor agregado a las funciones de la entidad.

- **Spoofing**: Falsificación de la identidad origen en una sesión: la identidad es por una dirección IP o Mac Address.

- **Tipos de información:** cualquier tipo de información producida y/o recibida por las entidades públicas, sus dependencias y servidores públicos, y en general por cualquier persona que desarrolle actividades inherentes a la función de dicha entidad o que hayan sido delegados por esta, independientemente del soporte y medio de registro (análogo o digital) en que se produzcan, y que se conservan en:

  a) Documentos de Archivo (físicos y electrónicos).
  b) Archivos institucionales (físicos y electrónicos).
  c) Sistemas de Información Corporativos.
  d) Sistemas de Trabajo Colaborativo.
  e) Sistemas de Administración de Documentos.
  f) Sistemas de Mensajería Electrónica.
  g) Portales, Intranet y Extranet.
  h) Sistemas de Bases de Datos.
  i) Disco duros, servidores, discos o medios portables, cintas o medios de video y audio (análogo o digital), etc.
  j) Cintas y medios de soporte (back up o contingencia).
  k) Uso de tecnologías en la nube.

- **Troyano**: Aplicación que aparenta tener un uso legítimo pero que tiene funciones ocultas diseñadas para sobrepasar los sistemas de seguridad.

- **Usuario de la información:** Para la informática es un usuario aquella persona que utiliza un dispositivo o un ordenador y realiza múltiples operaciones con distintos propósitos. A menudo es un usuario aquel que adquiere una computadora o dispositivo electrónico y que lo emplea para comunicarse con otros usuarios, generar contenido y documentos, utilizar software de diverso tipo y muchas otras acciones posibles. El usuario no es necesariamente uno en particular instruido o entrenado en el uso de nuevas tecnologías, ni en programación o desarrollo, por lo cual la interfaz del dispositivo en cuestión debe ser sencilla y fácil de aprender. Sin embargo, cada tipo de desarrollo

tiene su propio usuario modelo y para algunas compañías el parámetro de cada usuario es distinto.

- **Virus**: Programas informáticos de carácter malicioso, que buscan alterar el normal funcionamiento de una red de sistemas o computador personal, por lo general su acción es transparente al usuario y este tarda tiempo en descubrir su infección; buscan dañar, modificar o destruir archivos o datos almacenados.

- **Vulnerabilidad**: Debilidad en la seguridad de la información de una organización que potencialmente permite que una amenaza afecte a un activo. Según [ISOIIEC 13335-1:2004]: debilidad de un activo o conjunto de activos que puede ser explotado por una amenaza.

- **Gestión de riesgos:** Es un enfoque estructurado para manejar la incertidumbre relativa a una amenaza, a través de una secuencia de actividades humanas que incluyen evaluación de riesgo, estrategias de desarrollo para manejarlo y mitigación del riesgo utilizando recursos gerenciales. Las estrategias incluyen transferir el riesgo a otra parte, evadir el riesgo, reducir los efectos negativos del riesgo y aceptar algunas o todas las consecuencias de un riesgo particular.[6]

- **Análisis de riesgos:** Tiene como propósito determinar los componentes de un sistema que requieren protección, sus vulnerabilidades que los debilitan y las amenazas que lo ponen en peligro, con el fin de valorar su grado de riesgo.

  El activo más importante que tiene la organización la propia información, por lo que tienen que existir técnicas que las mantengan seguras, mucho más allá de la seguridad física que se puede estableces gracias a los equipos con los que cuenta la organización para almacenar dicha información. La información se blinda con seguridad lógica, es decir, aplicar barreras y procedimientos que resguardan el acceso a todos los datos y restringe el acceso a las personas autorizadas.[7]

- **Evaluación de riesgos:** Es la actividad fundamental que la Ley establece que debe llevarse a cabo inicialmente y cuando se efectúen determinados cambios, para poder detectar los riesgos que puedan existir en todos y cada uno de los

[6] https://es.wikipedia.org/wiki/Gesti%C3%B3n_de_riesgos
[7] https://protejete.wordpress.com/gdr_principal/analisis_riesgo/

puestos de trabajo de la empresa y que puedan afectar a la seguridad y salud de los trabajadores.[8]

Se entiende por evaluación de riesgos a la evaluación de las amenazas y vulnerabilidades relativas a la información y a las instalaciones de procesamiento de la misma, la probabilidad de que ocurran y su potencial impacto en la operatoria del Organismo.

- **Administración de riesgos:** La Administración de riesgos es un término aplicado a un método lógico y sistemático de establecer el contexto, identificar, analizar, evaluar, tratar, monitorear y comunicar los riesgos asociados con una actividad, función o proceso de una forma que permita a las organizaciones minimizar pérdidas y maximizar oportunidades.[9]

- **Comité de seguridad de la información:** El Comité de Seguridad de la Información, es un cuerpo integrado por representantes de todas las áreas sustantivas del Organismo, destinado a garantizar el apoyo manifiesto de las autoridades a las iniciativas de seguridad para lograr un trabajo eficaz y seguro.[10]

- **RESPONSABLE DE SEGURIDAD INFORMÁTICA**
  - ✓ Será responsable de planear, coordinar y administrar los procesos de seguridad informática de la entidad.
  - ✓ Deberá asegurar el buen funcionamiento del proceso de seguridad informática,
  - ✓ Debe guiar a los usuarios sobre cómo desarrollar procedimientos para protección de los recursos de software y hardware.
  - ✓ Es el encargado de preparar a los usuarios de la empresa ante incidentes de seguridad mediante un plan de respuesta de accidentes, propone y coordina los análisis de riegos en seguridad y desarrolla procedimientos de seguridad.
  - ✓ Es responsable de crear y actualizar las políticas de seguridad de informática.
  - ✓ Debe responder a las notificaciones de sospecha de incidentes de seguridad o incidentes reales.
  - ✓ Coordinará la realización periódica de auditorías a las prácticas de seguridad informática.

[8] http://www.fremm.es/riesgoslaborales/autonomos/que_es_la_evaluacion.html
[9] https://www.gestiopolis.com/administracion-de-riesgos-empresariales-definicion-y-proceso/
[10] https://seguinfo.wordpress.com/2012/03/22/que-es-el-comite-de-seguridad-de-la-informacion/

- ✓ Debe dar seguimiento a las recomendaciones que hayan resultado de cada auditoria.
- ✓ Es el responsable de la revisión de problemas de seguridad de la información existentes y de aquellos que se consideran potenciales.[11]
- ✓ Es la persona que cumple la función de supervisar el cumplimiento de la presente Política y de asesorar en materia de seguridad de la información a los integrantes de la entidad que así lo requieran.

- **Incidente de seguridad:** Un Incidente de Seguridad de la Información es la violación o amenaza inminente a la Política de Seguridad de la Información implícita o explícita.

  Según la norma ISO 27035, un Incidente de Seguridad de la Información es indicado por un único o una serie de eventos seguridad de la información indeseados o inesperados, que tienen una probabilidad significativa de comprometer las operaciones de negocio y de amenazar la seguridad de la información. [12]

  Un incidente de seguridad es un evento adverso en un sistema de computadoras, o red de computadoras, que compromete la confidencialidad, integridad o disponibilidad, la legalidad y confiabilidad de la información. Puede ser causado mediante la explotación de alguna vulnerabilidad o un intento o amenaza de romper los mecanismos de seguridad existentes.

[11] https://www.usac.edu.gt/empleos/archivos/_Anuncio_-Jefe-de-Seguridad-Informatica-Febrero-2016.pdf
[12] https://www.cert.uy/inicio/incidentes/que_es-un-incidente/

7.2.5 Políticas, procedimientos y controles aspectos generales

Esta política se conforma de una serie de pautas sobre aspectos específicos de la seguridad de la información, que incluyen los siguientes tópicos

• Organización de la Seguridad
Orientado a administrar la seguridad de la información dentro de la entidad y establecer un marco gerencial para controlar su implementación.

• Clasificación y Control de Activos
Destinado a mantener una adecuada protección de los activos de la entidad.

• Seguridad del Personal
Orientado a reducir los riesgos de error humano, comisión de ilícitos contra la entidad o uso inadecuado de instalaciones.

• Seguridad Física y Ambiental
Destinado a impedir accesos no autorizados, daños e interferencia a las sedes e información de la entidad
.

• Gestión de las Comunicaciones y las Operaciones
Dirigido a garantizar el funcionamiento correcto y seguro de las instalaciones de procesamiento de la información y medios de comunicación.

• Control de Acceso
Orientado a controlar el acceso lógico a la información.

• Desarrollo y Mantenimiento de los Sistemas
Orientado a garantizar la incorporación de medidas de seguridad en los sistemas de información desde su desarrollo y/o implementación y durante su mantenimiento.

• Administración de la Continuidad de las Actividades del Organismo
Orientado a contrarrestar las interrupciones de las actividades y proteger los procesos críticos de los efectos de fallas significativas o desastres.

• Cumplimiento
Destinado a impedir infracciones y violaciones de las leyes del derecho civil y penal; de las obligaciones establecidas por leyes, estatutos, normas, reglamentos o contratos; y de los requisitos de seguridad.

7.2.6 Sanciones previstas por incumplimiento

El incumplimiento de la Política de Seguridad de la Información tendrá como resultado la aplicación de diversas sanciones, conforme a la magnitud y característica del aspecto no cumplido.

7.2.7 Políticas de seguridad de la información

- La administración municipal de La Ceja-Antioquia actualizara constantemente su política de seguridad de acuerdo a los lineamientos establecidos en el SGSI y las directrices establecidas por MinTic.

- Mediante la aplicación de la política de seguridad la administración municipal de La Ceja-Antioquia, se compromete al cumplimiento del marco legal de protección de datos garantizando la confiabilidad, integridad y disponibilidad de la información.

7.2.8 Responsabilidades frente a la seguridad de la información y al Sistema de Gestión de Seguridad de la Información.

- **RESPONSABILIDADES OFICINA DE SISTEMAS**
  - Establecer, mantener y divulgar la política de seguridad de la información.
  - Garantizar la confiablidad, integridad y disponibilidad de los backups que se generan en la entidad.
  - Hacer parte del comité de seguridad de la información.
  - Informar y solucionar cada uno de los eventos que se presenten en la entidad y que afecten la seguridad de la información y la infraestructura tecnológica utilizada en su procesamiento y almacenamiento.
  - Establecer los controles de seguridad descritos en el SGSI.
  - Implementar estrategias que permitan el mejoramiento continuo en los procesos que se realizan en la oficina de sistemas de tal manera que se optimicen los recursos y se preste un mejor servicio de soporte a los usuarios de la entidad.

- Promover el uso de la mesa de ayuda para poder brindar de una manera más efectiva el soporte a los usuarios.

- **RESPONSABILIDADES DE LOS PROPIETARIOS DE LA INFORMACIÓN**
  - Son propietarios de la información las personas que generan, procesan y mantienen información de la entidad y que es propia por el desarrollo de sus funciones dentro de la misma.

  - Los propietarios de la información deben de clasificar la información de acuerdo a sus dimensiones de integridad confiablidad y disponibilidad.

  - Los propietarios de la información aplicaran tablas de retención documental para determinar los tiempos de conservación de la misma, esto se hará en conjunto con el archivo central.

- **RESPONSABILIDADES DE LOS FUNCIONARIOS, CONTRATISTAS Y PRACTICANTES USUARIOS DE LA INFORMACIÓN**
  - Aplicar los lineamientos establecidos en el SGSI, de tal manera que se garantice la seguridad de la información evitando su perdida, alteración, destrucción o uso indebido

  - Informar a la oficina de sistemas los Incidentes de seguridad que puedan afectar la seguridad de la información.

  - Cuidar la infraestructura tecnológica que les fue asignada para el desarrollo de sus funciones dentro de la entidad.

7.2.9 Lineamientos política de seguridad de la información

7.2.9.1 Lineamiento 1: clasificación de los activos

Se identificarán los activos importantes asociados a cada sistema de información, sus respectivos propietarios y su ubicación, para luego elaborar un inventario con dicha información.

Se tendrán en cuenta las siguientes consideraciones:

- El mismo será actualizado ante cualquier modificación de la información registrada y revisado con una periodicidad de 6 meses.

- Los encargados de elaborar el inventario y mantenerlo actualizado serán:
  - La Oficina de bienes
  - La Oficina de sistemas
  - Los jefes de cada dependencia.

7.2.9.2 Lineamiento 2: clasificación de la información

Para clasificar un Activo de Información, se evaluarán las tres características de la información en las cuales se basa la seguridad: confidencialidad, integridad y disponibilidad. *(Ver clasificación de la información)*

7.2.9.3 Lineamiento 2: rotulado de la información

La oficina de bienes realizará el procedimiento para el rotulado y manejo de los activos de información, de acuerdo al esquema de clasificación definido por la entidad para la clasificación de los mismos.

Se tendrá en cuenta para el rotulado de los activos de información en sus descripciones los siguientes aspectos.

- Si el activo es sujeto a Backup;
- Si el activo almacena algún tipo de información y el nivel de criticidad la misma.
- Forma de envío de la información por correo físico, fax, correo electrónico o en forma oral.

7.2.9.4 Lineamiento 3: Uso de usuarios y contraseñas

La asignación de usuarios y contraseñas es un permiso que la administración municipal otorga a sus funcionarios, contratistas o practicantes con el fin de que tengan acceso a los recursos tecnológicos como a las plataformas y sistemas de información que permiten la operación, consulta y resguardo de la información institucional.

- La asignación de credenciales: usuarios (Login) y contraseñas (Clave o Password) a los diferentes funcionarios, contratistas o practicantes así como su desactivación de los sistemas se harán de acuerdo a los procedimientos establecidos en el SGSI y estará a cargo del funcionario responsable de la dependencia quien solicitara por medio de un correo electrónico su correspondiente activación o desactivación y esta solicitud se le realizara a la oficina de sistemas con el visto bueno de la oficina de gestión humana.

- La utilización de los medios tecnológicos de la entidad, solo los podrán acceder los funcionarios, contratistas o practicantes con su respectivo usuario y contraseña. La trasferencia de un usuario y su respectiva contraseña a otro funcionario, solo se podrá realizar si se cuenta con la debida autorización del jefe de la dependía y la oficina de sistemas

- **TIPOS DE CUENTAS DE USUARIO**

Se definen dos tipos de cuentas:

a) Cuenta de Usuario de Sistema de Información:

Corresponden a todos los usuarios que utilizan la infraestructura tecnológica de la entidad y que requieren de un usuario y un password para poder acceder a estos, este tipo de cuenta de usuario solo permite

- El acceso para consulta
- Modificación
- Actualización
- Eliminación de información,

El jefe de cada dependencia enviara un correo a la oficina de sistemas explicando los roles que cada usuario tendrá en las diferentes aplicaciones con las cuales desarrollara sus actividades

b) Cuenta de Administración de Sistema de Información:

Estas cuentas están asignadas directamente al jefe de la oficina de sistemas y su gestión estará supervisada por el comité de la seguridad de la información.

Uso apropiado de usuarios y contraseñas:

- Las credenciales de acceso que se le asignen a los funcionarios serán de uso exclusivo para fines laborales.
- Los usuarios cambiaran periódicamente las contraseñas para evitar cualquier amenaza sobre los activos de información de la entidad.

Responsabilidades de los funcionarios, contratistas y practicantes con usuarios y contraseñas asignados

- Es responsabilidad de los funcionarios, contratistas y practicantes de la entidad hacer un buen uso de sus credenciales de acceso a los sistemas de

información de la entidad, además de informar a la oficina de sistemas cualquier dificultad o fallo de seguridad identificados en los mismos.

Monitoreo:

- La oficina de sistemas realizara lecturas periódicas de las auditorias (logs) que en la actualidad poseen los sistemas de información de la entidad y en las cuales se detallan cada uno de los eventos o acciones que afectan a los procesos informáticos.

7.2.9.5 Lineamiento 4: uso del servicio de correo electrónico

El correo electrónico es un servicio basado en el intercambio de información a través de la red y el cual es provisto por la administración municipal para los funcionarios, contratistas, practicantes previamente autorizados para su acceso.

Los objetivos específicos de los lineamientos para el uso del correo electrónico son:

- Incentivar el uso del servicio de correo electrónico para fines estrictamente laborales de la entidad.
- Asegurar el correcto manejo de la información privada de la institución por parte de los funcionarios, contratistas o practicantes de la administración municipal.
- Garantizar la confidencialidad, la privacidad y el uso adecuado y moderado de la información a través de este servicio.

La administración municipal a criterio propio puede otorgar el acceso a los servicios de correo electrónico para la realización de actividades institucionales a los funcionarios, contratistas y proveedores. El acceso incluye la preparación, transmisión, recepción y almacenamiento de mensajes de correo electrónico y sus adjuntos. Los Directores, Secretarios de despacho, Jefes o Coordinadores tienen la autonomía de otorgar y solicitar el acceso de sus funcionarios, contratistas o practicantes a este servicio.

Uso apropiado de los servicios de correo electrónico de la administración municipal.

- Conservar normas de respeto, confidencialidad y criterio ético por parte de todos los funcionarios, contratistas y practicantes con acceso a este servicio.

- Usar el correo electrónico Institucional exclusivamente para fines laborales: para la difusión o el envío de circulares, memorandos, oficios y archivos de trabajo, cuando sea necesario en cumplimiento de las funciones asignadas.
- Los correos enviados a través del correo institucional contendrán mensajes serios, claros, concisos, corteses y respetuosos.
- La oficina de comunicaciones tendrá a su cargo la asignación de los correos institucionales a los funcionarios que lo soliciten, previa autorización de su jefe inmediato y de la oficina de gestión humana.

Uso indebido del servicio de correo electrónico de la administración municipal.

- Utilizar el correo institucional para el envío de correo Spam.
- Utilizar el correo institucional para el envió de cualquier información clasificada o reservada de la administración municipal.
- Utilizar el correo institucional para descargar, enviar, imprimir o copiar documentos que no hagan parte del quehacer institucional de la entidad.
- Descargar de un correo electrónico recibido cualquier software o archivo adjunto sin tomar las medidas de precaución necesarias que permitan la activación de virus informático dentro de los sistemas de información de la entidad.
- Utilizar el correo electrónico institucional para propósitos ajenos a la entidad.

Responsabilidades de los funcionarios, contratistas y practicantes que sean usuarios de los servicios de correo electrónico de la administración municipal.

- El correo electrónico institucional será el único medio empleado por la administración municipal para el envío y recepción de información entre sus dependencias y con otras entidades externas, es por ello que es fundamental que cada funcionario encargado de una cuenta de correo institucional lo revise contantemente e informe a su jefe inmediato cada una de las comunicaciones recibidas por este medio, conservando su confidencialidad e integridad.
- Cuando un funcionario, contratista o practicante abandona su puesto de trabajo temporalmente, este debe cerrar totalmente la sesión de lectura y envío de correos para evitar la suplantación.
- Dar aviso al a la Oficina de sistemas, a través de los medios establecidos, de cualquier fallo de seguridad en su cuenta de correo, incluyendo su uso no autorizado, pérdida de la contraseña, suplantación, etc.

- Realizar backus en forma periódica de los correos y enviarlos a la oficina de sistemas para correspondiente almacenamiento y disposición.
- Reenviar los correos cuyo contenido sea esencial para la entidad al archivo central para que desde esta oficina se realice su respectiva gestión.

Monitoreo

- La administración municipal tiene el derecho a acceder y revelar los contenidos electrónicos de los correos electrónicos institucionales de sus funcionarios, contratistas y practicantes y estos deben dar su consentimiento a la administración municipal en caso de que algún ente fiscalizador a nivel interno o externo requiera esta información. Priman las exigencias de carácter legal o disciplinario.
- El comité de seguridad de la información puede realizar auditorías internas a los equipos informáticos que hacen parte de la infraestructura tecnológica de la entidad para revisar la gestión que cada funcionario, contratista o practicante realiza con los correos electrónicos institucionales que le fueron asignados, todo ello enmarcado en SGSI.

7.2.9.6 Lineamiento 5: uso del servicio de internet/intranet de la administración municipal

Los objetivos específicos del uso de servicio de internet/intranet son:

- Incentivar el uso del servicio de Internet/Intranet para fines estrictamente laborales de la administración municipal
- Asegurar el correcto manejo de la información privada de la entidad atreves de esta red.
- Garantizar la confidencialidad, la privacidad y de uso adecuado y moderado de la información a través de este servicio que brinda la entidad.

Cada Secretario, Director, Jefe de dependencia tiene la autonomía de otorgar y solicitar el acceso de sus funcionarios, contratistas o practicantes a este servicio, de acuerdo al procedimientos vigentes.

El ingreso a este servicio se realiza por medio de la plataforma que la entidad destina, que para este caso es el navegador de internet instalado en cada máquina.

El punto de inicio para acceder a este servicio se hace desde la página web institucional a través de la dirección: http://www.laceja-antioquia.gov.co

Uso apropiado del servicio de Internet/Intranet

Todos los funcionarios, contratistas y practicantes que han sido autorizados para tener el servicio de internet deben:

- Utilizar este servicio exclusivamente para fines laborales.
- Conservar normas de respeto, confidencialidad y criterio ético por parte de todos los funcionarios, contratistas o practicantes con acceso a este servicio.
- Descargar documentos o archivo tomando las medidas de precaución para evitar el acceso de virus en las redes y equipos informáticos.

Uso indebido del servicio de Internet/Intranet:

- Acceder a sitios no permitidos y que expongan la red de datos a una riesgo de seguridad
- Utilizar software o servicios de mensajería instantánea (chat) y redes sociales no instalados o autorizados por la oficina de sistemas.
- Compartir en sitios web información propia de la administración municipal clasificada como reservada.
- Descargar e instalar software sin las respectivas licencias legales.
- Utilizar el servicio de Internet/Intranet para propósitos comerciales ajenos a la entidad.
- Realizar cambios en la configuración de los navegadores instalados en los equipos informáticos de la entidad o descargar otros sin la previs autorizacon de la oficina de sistemas.
- Acceder a sitios de contenido multimedia (videos, música, emisoras online, etc.) debido al alto consumo del canal de comunicaciones. Únicamente se autorizara el acceso a aquellos funcionarios, contratistas o practicantes que por sus actividades requieran monitorear estos sitios externos y tengan previa aprobación del Jefe Inmediato y la de la oficina de sistemas.

Responsabilidades de los Usuarios de Internet/Intranet en la administración municipal:

- Informar a la oficina de sistemas a través de los medios establecidos de cualquier fallo de seguridad que se presente por la utilización de este servicio en la entidad.

Monitoreo:

- La oficina de sistemas realizara informes periódicamente sobre los registros que constantemente realizan los dispositivos de seguridad perimetral y la consola del antivirus sobre las actividades de los usuarios en la internet, dichos informes serán evaluados por el comité de seguridad de la información.
- Si se determina que alguna de las páginas previamente restringidas por la Oficina de sistemas es requerida para el desempeño de funciones de algún funcionario, contratista o practicante esta será habilitada únicamente con el consentimiento y solicitud de su jefe directo y con el visto bueno de la Oficina.

7.2.9.7 Lineamiento 6: uso de dispositivos de almacenamiento externo

En este lineamiento entenderemos como medios de almacenamiento externo a los dispositivos diferentes a los equipos de cómputo, y que permite la movilidad de la información, como son: las unidades de red compartidas y los dispositivos de almacenamiento externo: USB, CD ROM, DVD ROM, los cuales constituyen una herramienta que sirve para la transferencia rápida y directa de información entre los funcionarios, contratistas o practicantes de la entidad.

Los objetivos específicos del uso de dispositivos de almacenamiento externo son:

- Establecer un plan de concientización a los funcionarios, contratistas o practicantes de la entidad sobre los riesgos asociados con el uso de los medios de almacenamiento, tanto para los sistemas de información como para la infraestructura tecnológica de la Entidad.
- Delimitar el uso de estos medios de almacenamiento en las diferentes áreas de la entidad donde exista información crítica de la misma.

El uso de dispositivos de almacenamiento externo está permitido en la administración municipal para los funcionarios, contratistas y practicantes; en general los funcionarios, contratistas o practicantes de la entidad, con el fin de facilitar el compartir y transportar información que no sea de carácter clasificado ni reservado de la entidad dentro de las normas y responsabilidades del manejo de información institucional.

Uso indebido de dispositivos de almacenamiento externo:

- Almacenar o transportar información clasificada o reservada de la administración municipal.

- Ejecutar cualquier tipo de programa no autorizado por la entidad desde cualquiera de las unidades de almacenamiento en mención.
- Emplear dispositivos de almacenamiento externo con el fin de almacenar o exponer información sensible o reservada de los usuarios o funcionarios, contratistas o practicantes de la entidad.

Responsabilidades de los usuarios de dispositivos de almacenamiento externo:

- Evitar la pérdida o robo de un dispositivo de almacenamiento externo y que contenga información sensible de la entidad porque esto pude afectar la seguridad de la información de la misma.
- No conectar estos dispositivos a equipos que no tengan un software antivirus actualizado ya que esto puede facilitar la ejecución de virus informáticos y la perdida de información en el dispositivo o daño en el mismo.

7.2.9.8 Lineamiento 7: uso de dispositivos de captura de imágenes y/o grabación de video

No se permite la captura de imágenes y/o grabación de video en las instalaciones o sedes de la administración municipal, parte de la ciudadanía, funcionarios, contratistas y practicantes del Instituto, sin previa autorización del departamento administrativo y la oficina de comunicaciones.

Monitoreo:

- La administración municipal puede controlar el acceso de dispositivos de captura de imágenes y/o grabación de video a sus instalaciones en las entradas a cada una de sus dependencias, por medio del personal de vigilancia y seguridad dispuesto en cada uno de los puntos de ingreso de la entidad.

7.2.9.9 Lineamiento 8: uso de escritorios y pantallas despejadas

Este lineamiento se refiere a que los funcionarios, contratistas y practicantes de la entidad mantengan su escritorio físico de trabajo libre documentos físicos visibles y al almacenamiento de archivos en carpetas fuera del escritorio virtual de los sistemas operativos.

Para su definición y aplicación se define de la siguiente manera:

Escritorios:

- Los documentos con información clasifica o reservada no deben de quedar a la vista o al alcance de cualquier tipo de persona tanto interna como externa, estos documentos deben permanecer en áreas con acceso restringido.

Pantallas:

- Los escritorios de los sistemas operativos deben tener la menor cantidad de documentos, solo se tendrán los accesos directos a las aplicaciones a los cuales puede acceder el usuario, los demás archivos deberán de estar almacenados en carpetas en las unidades de disco, y si es necesario se deberá asignar contraseñas para poder acceder a ellas.
- AL terminar la jornada laborar los funcionarios, contratistas y practicantes deben apagar los computadores asignados.
- El fondo de pantalla de cada computador es único para todas las estaciones de trabajo y para todos los usuarios y puede ser cambiado únicamente por la Oficina de sistemas.

Monitoreo:

La oficina de sistemas sin previo aviso, realizan brigadas de monitoreo para verificar el estado de los computadores, monitores y escritorios virtuales y generar el respectivo informe de lo encontrado.

7.2.10 Comité de seguridad de la información

Es indispensable crea el comité de seguridad de la información para la entidad, el cual tendrá a carga las siguientes funciones

- Coordinar la implementación del Sistema de Gestión y Seguridad de la Información al interior de la entidad.
- Revisar los diagnósticos del estado de la seguridad de la información en Nombre de la entidad.
- Acompañar e impulsar el desarrollo de proyectos de seguridad.
- Coordinar y dirigir acciones específicas que ayuden a proveer un ambiente seguro y establecer los recursos de información que sean consistentes con las metas y objetivos de Nombre de la entidad.
- Revisar la política de seguridad y realizar los respectivos ajustes de acuerdo a las necesidades de seguridad que surjan en la entidad.

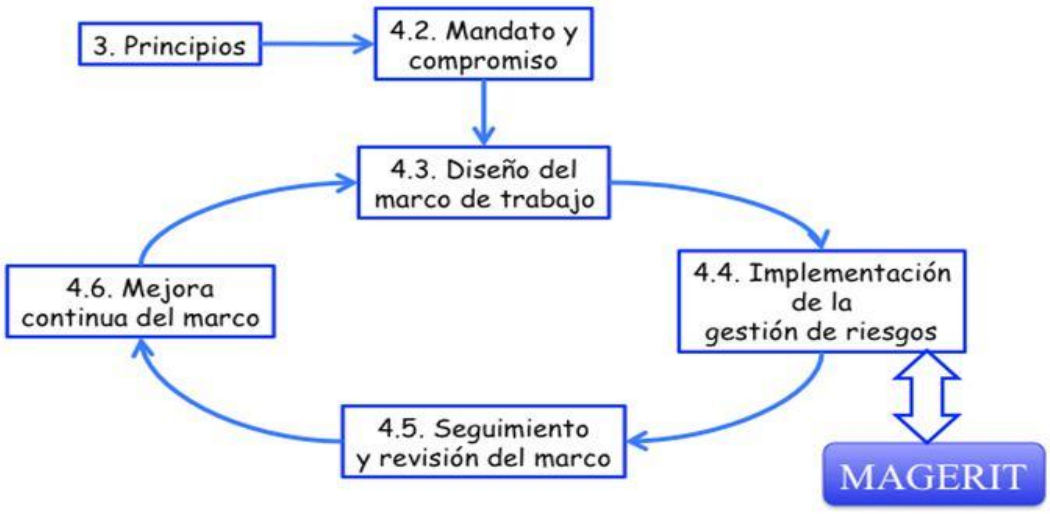
Estas responsabilidades son tomadas de la guía Nro.4 de MINTIC para la seguridad y privacidad de la Información.

7.3 METODOLOGÍA DE ANÁLISIS Y EVALUACIÓN DE RIESGOS Y REPORTE DE EVALUACIÓN DE RIESGOS "MAGERIT"

MAGERIT es la metodología de análisis y gestión de riesgos elaborada por el Consejo Superior de Administración Electrónica, como respuesta a la percepción de que la Administración, y, en general, toda la sociedad, dependen de forma creciente de las tecnologías de la información para el cumplimiento de su misión.(Amutio Gómez, 2012)

El método MAGERIT, son las siglas de Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información de la Administraciones, dicho método cubre la fase AGR (Análisis y Gestión de Riesgos). Si hablamos de Gestión global de la Seguridad de un Sistema de Seguridad de la Información basado en ISO 27001, MAGERIT, es el núcleo de toda actuación organizada en dicha materia, ya que influye en todas las fases que sean de tipo estratégico y se condiciona la profundidad de las fases de tipo logístico. ("ISO 27001: El método MAGERIT," n.d.)

Ilustración 22 - ISO 31000 - Marco de trabajo para la gestión de riesgos



Fuente: https://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_Magerit.html#.Wu5xeO8vzcc

MAGERIT persigue los siguientes objetivos:

- Concienciar a los responsables de las organizaciones de información de la existencia de riesgos y de la necesidad de gestionarlos
- Ofrecer un método sistemático para analizar los riesgos derivados del uso de tecnologías de la información y comunicaciones (TIC)
- Ayudar a descubrir y planificar el tratamiento oportuno para mantener los riesgos bajo control Indirectos:
- Preparar a la Organización para procesos de evaluación, auditoría, certificación o acreditación, según corresponda en cada caso

El objetivo principal de MAGERIT es proteger los activos informáticos en pro de ayudar al alcance de la misión de una organización de acuerdo a las Dimensiones de Seguridad propuestas:

Tabla 16 - Dimensiones de Seguridad de Magerit

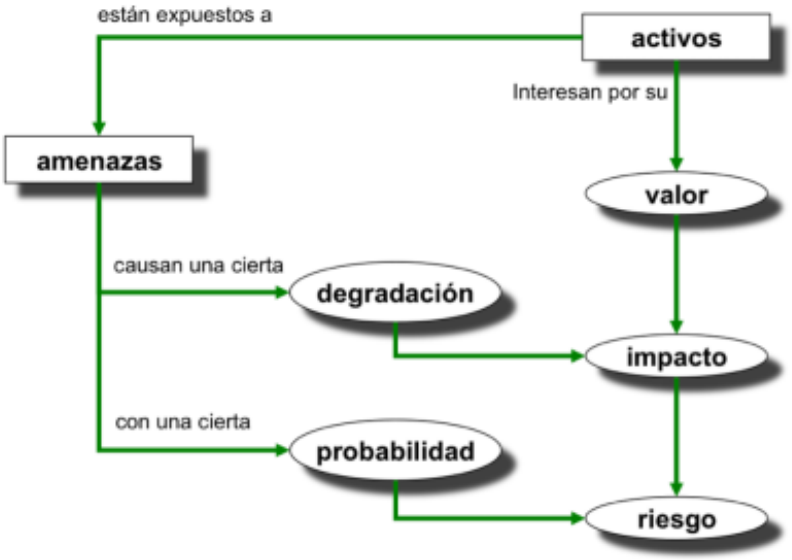
INTEGRIDAD **[I]** ¿Qué importancia tendría que los datos fueran modificados fuera de control?	Garantía de la exactitud y completitud de la información y los métodos de su procesamiento. Es necesario asegurar que los datos no sufran cambios no autorizados, la pérdida de integridad puede acabar en fraudes, decisiones erróneas o como paso a otros ataques. El sistema contiene información que debe ser protegida de modificaciones imprevistas, no autorizas o accidentales, como información de censo o sistemas de transacciones financieras.
DISPONIBILIDAD **[D]** ¿Qué importancia tendría que el activo no estuviera disponible?	Aseguramiento de que los usuarios autorizados tienen acceso cuando lo requieran a la información y sus activos asociados. Se refiere a la continuidad operativa de la entidad, la pérdida de disponibilidad puede implicar, la pérdida de productividad o de credibilidad de la entidad. El sistema contiene información o proporciona servicios que deben estar disponibles a tiempo para satisfacer requisitos o evitar pérdidas importantes, como sistemas esenciales de seguridad y protección de la vida.
CONFIDENCIALIDAD **[C]** ¿Qué importancia tendría que el dato fuera conocido por personas no autorizadas?	Aseguramiento de que la información es accesible sólo para aquellos autorizados a tener acceso. Se refiere a la protección de datos frente a la difusión no autorizada, la pérdida de confidencialidad puede resultar en problemas legales, pérdida del negocio o de credibilidad. El sistema contiene información que necesita protección contra la divulgación no autorizada, como información parcial de informes, información personal o información comercial patentada.

AUTENTICIDAD DE LOS USUARIOS DEL SERVICIO [A_D] ¿Qué importancia tendría que quien accede al servicio no sea realmente quien se cree?	Aseguramiento de la identidad u origen.
AUTENTICIDAD DEL ORIGEN DE LOS DATOS [A_S] ¿Qué importancia tendría que los datos no fueran realmente imputables a quien se cree?	

TRAZABILIDAD DEL SERVICIO [T_S] ¿Qué importancia tendría que no quedara constancia fehaciente del uso del servicio?	Aseguramiento de que en todo momento se podrá determinar quién hizo qué y en qué momento.
TRAZABILIDAD DE LOS DATOS [T_D] ¿Qué importancia tendría que no quedara constancia del acceso a los datos?	

Fuente: (“Principios de Seguridad Informatica | Seguridad Informatica,” n.d.)

Ilustración 23 - Elementos del análisis de riesgos potenciales.



Fuente: MAGERIT – versión 3.0 Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información Libro I - Método

El proceso principal de un proyecto de análisis y gestión de riesgos es el propio análisis de riesgos. Este a su vez se divide en 4 bloques:

Ilustración 24 - Aproximación metódica para determinar el riego

Fuente: https://es.slideshare.net/pedrogarciarepetto/ai03-agr

- Caracterización de activos,
- Caracterización de amenazas,
- Caracterización de salvaguardas y
- Estimación del estado del riesgo.

7.3.1 Caracterización de activos

- La primera etapa del análisis de riesgos es la realización de un inventario de activos, entendiendo por activo según MAGERIT: los recursos del sistema de información o relacionados con éste, necesarios para que la Organización funcione correctamente y alcance los objetivos propuestos por su dirección. Dicho de otro modo, los activos críticos están formados por todos los activos que se consideran de importancia para el negocio de la organización. Obviamente, esto comprende tantos activos de proceso de datos (hardware), ubicaciones físicas, activos de información (datos), imagen corporativa, etc. Es importante identificar la persona o el cargo responsable de cada activo. ("Análisis de riesgos con MAGERIT en el ENS (II) - Security Art Work," n.d.)

- La segunda etapa del análisis de riesgos dentro de la gestión de activos supone establecer las dependencias entre los distintos activos de un modo jerarquizado, evaluando el grado de vinculación entre activos y en función de los parámetros disponibilidad, integridad, confidencialidad.

La dependencia entre activos supone que en el caso de que una amenaza que afecte a un activo del que dependa otro activo superior, tendrá impacto directo sobre el activo superior. Para llevar a cabo la definición de dependencias la metodología empleada propone una estructura de 5 capas, las cuales se identifican a continuación empezando por la inferior:

1. Entorno: equipamiento auxiliar, personal y edificios.
2. Sistema de información: hardware, software, comunicaciones y soportes.
3. Información: Datos.
4. Funciones de la organización: Servicios finales.
5. Otros activos

Tabla 17 - Tipos de activos

TIPOS DE ACTIVOS		
SERVICIOS	[SERV]	Función que satisface una necesidad de los usuarios (del servicio). Para la prestación de un servicio se requieren una serie de medios. Los servicios aparecen como activos de un análisis de riesgos bien como: • Servicios finales (prestados por la Organización a terceros), • Servicios instrumentales (donde tanto los usuarios como los medios son propios). • Servicios contratados (a otra organización que los proporciona con sus propios medios).

Datos / Información	[DI]	Elementos de información que, de forma singular o agrupados de alguna forma, representan el conocimiento que se tiene de algo. Los datos son el corazón que permite a una organización prestar sus servicios. Son en cierto sentido un activo abstracto que será almacenado en equipos o soportes de información (normalmente agrupado en forma de bases de datos) o será transferido de un lugar a otro por los medios de transmisión de datos
Aplicaciones (software)	[SOFW]	Con múltiples denominaciones (programas, aplicativos, desarrollos, etc.) este epígrafe se refiere a tareas que han sido automatizadas para su desempeño por un equipo informático. Las aplicaciones gestionan, analizan y transforman los datos permitiendo la explotación de la información para la prestación de los servicios.
Equipos informáticos (hardware)	[HARD]	Dícese de bienes materiales, físicos, destinados a soportar directa o indirectamente los servicios que presta la organización, siendo pues depositarios temporales o permanentes de los datos, soporte de ejecución de las aplicaciones informáticas o responsables del procesado o la transmisión de datos.

Redes de comunicaciones	[COMU]	Incluyendo tanto instalaciones dedicadas como servicios de comunicaciones contratados a terceros; pero siempre centrándose en que son medios de transporte que llevan datos de un sitio a otro.
Soportes de información	[SINFO]	En este epígrafe se consideran dispositivos físicos que permiten almacenar información de forma permanente o, al menos, durante largos periodos de tiempo.
Equipamiento auxiliar	[EAX]	En este epígrafe se consideran otros equipos que sirven de soporte a los sistemas de información, sin estar directamente relacionados con datos.
Instalaciones	[INST]	En este epígrafe entran los lugares donde se hospedan los sistemas de información y comunicaciones.
Personal	[PER]	En este epígrafe aparecen las personas relacionadas con los sistemas de información.

Fuente: Tomado de: MAGERIT – versión 2 Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información.

7.3.2 Valoración de activos

Respecto a la valoración de los activos, ésta debe realizarse en base al valor del impacto que una amenaza puede ocasionar sobre dicho activo sobre el negocio.

En cuanto a dependencias los activos de las capas superiores serán los únicos que deben ser valorados, es decir los servicios finales y los datos, dado que los activos inferiores quedan valorados en base a las dependencias establecidas.

Para valorar los activos vale, teóricamente, cualquier escala de valores. A efectos prácticos es sin embargo muy importante que

- Se use una escala común para todas las dimensiones, permitiendo comparar riesgos,
- Se use una escala logarítmica, centrada en diferencias relativas de valor, que no en diferencias absolutas y
- Se use un criterio homogéneo que permita comparar análisis realizados por separado

Si la valoración es económica, hay poco más que hablar; pero frecuentemente la valoración es cualitativa, quedando a discreción del usuario; es decir, respondiendo a criterios subjetivos.

Se ha elegido una escala detallada de diez valores, dejando en valor 0 como determinante de lo que sería un valor despreciable (a efectos de riesgo). Si se realiza un análisis de riesgos de poco detalle, se puede optar por la tabla simplificada de 5 niveles.

Tabla 18 - Valoración cuantitativa de los activos.

VALOR	CRITERIO	
10	MUY ALTO	Daño muy grave a la organización
7-9	ALTO	Daño grave a la organización
4-6	MEDIO	Daño importante a la organización
1-3	BAJO	Daño menor a la organización
0	DESPRECIABLE	Irrelevante a efectos prácticos

Fuente: Autor

7.3.3 Caracterización de amenazas

Una vez finalizada la parte de activos, se debe en primer lugar identificar las amenazas que afectan a los activos, que únicamente se aplicarán sobre los activos que estén debajo del nivel de la capa de datos o inferior. En el documento de catálogo de MAGERIT se especifican una serie de amenazas y la tipología de activos que se ven afectados por cada amenaza. Una vez identificadas las amenazas, se debe establecer la valoración de las amenazas, mediante los siguientes dos parámetros:

- **Frecuencia**: tiempo de materialización de una amenaza.
- **Degradación**: impacto que tiene la materialización de la amenaza en el activo, aplicable a las 5 dimensiones de la seguridad.

Tabla 19 - Clasificación de las amenazas

AMENAZA	SÍMBOLO	DESCRIPCIÓN
DESASTRES NATURALES	[NAT]	Sucesos que pueden ocurrir sin intervención de los seres humanos como causa directa o indirecta.
DE ORIGEN INDUSTRIAL	[IND]	Sucesos que pueden ocurrir de forma accidental, derivados de la actividad humana de tipo industrial. Estas amenazas pueden darse de forma accidental o deliberada.
ERRORES Y FALLOS NO INTENCIONADOS	[ERR]	Fallos no intencionales causados por las personas.
ATAQUES INTENCIONADOS	[AT]	Fallos deliberados causados por las personas.

7.3.4 Valoración de Amenazas

Para establecer la valoración de las amenazas es necesario determinarla frecuencia o probabilidad de ocurrencia.

Para hacer una valoración más exacta es necesario estimar la frecuencia de ocurrencia y el porcentaje de degradación.

- **Probabilidad de ocurrencia:** Representa la tasa anual de ocurrencia cada cuanto se materializa la amenaza.
- **Porcentaje de Degradación:** Significa el daño causado por un incidente.

Se determina el grado de degradación y la frecuencia de ocurrencia de cada amenaza sobre cada activo con el fin de saber el impacto y riesgo potencial de dicha amenaza sobre el activo.

En MAGERIT, las frecuencias o probabilidades se muestran a continuación:

Tabla 20 - Valores típicos de las ocurrencias de las amenazas

MA	100	MUY FRECUENTE	A DIARIO
A	10	FRECUENTE	MENSUALMENTE
M	1	NORMAL	UNA VEZ AL AÑO
B	1/10	POCO FRECUENTE	CADA VARIOS AÑOS
MB	1/100	MUY POCO FRECUENTE	SIGLOS

Tomado de: Libro 1 Magerit versión 3 p.28

7.3.5 Valoración de Amenazas – Impacto

- **Impacto Potencial:** Se determina el nivel de daño o impacto que tendría un activo si se llegara a materializar una amenaza determinada en cada una de sus dimensiones de seguridad.

Tabla 21 - Impacto potencial

IMPACTO		DEGRADACIÓN		
		1%	10%	100%
VALOR	MA	M	A	MA
	A	B	M	A
	M	MB	B	M
	B	MB	MB	B
	MB	MB	MB	MB

Fuente: Libro 1 Magerit versión 3 p.28

7.3.6 Riesgo Potencial

El riesgo es la medida probable de daño sobre un sistema el cual es posible determinar directamente conociendo la probabilidad de ocurrencia de una amenaza sobre un activo y el impacto. Se denomina riesgo a la medida del daño probable sobre un sistema. Conociendo el impacto de las amenazas sobre los activos, es directo derivar el riesgo sin más que tener en cuenta la probabilidad de ocurrencia.

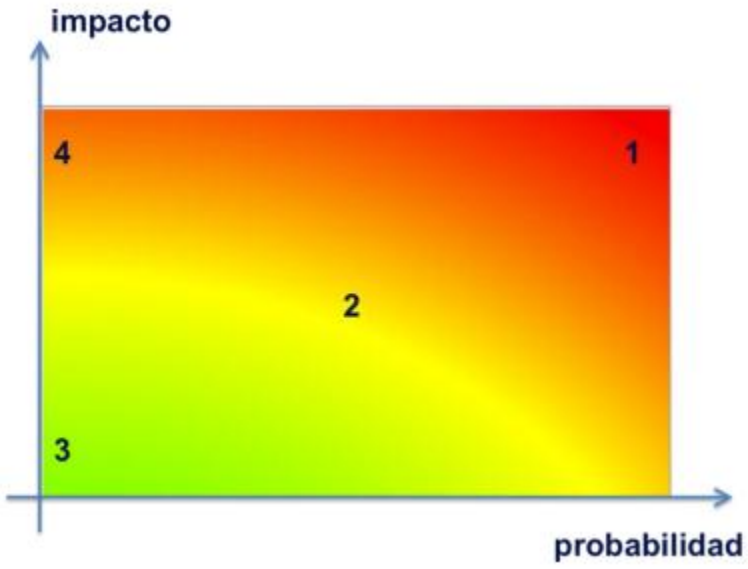
El riesgo crece con el impacto y con la probabilidad, pudiendo distinguirse una serie de zonas a tener en cuenta en el tratamiento del riesgo (que veremos más adelante):

- ✓ **ZONA 1:** Riesgos muy probables y de muy alto impacto.
- ✓ **ZONA 2:** Franja amarilla: cubre un amplio rango desde situaciones improbables y de impacto.
- ✓ **ZONA 3:** Riesgos improbables y de bajo impacto.
- ✓ **ZONA 4**: Riesgos improbables pero de muy alto impacto

Riesgo = Probabilidad x Impacto.

El riesgo crece con el impacto y con la probabilidad como se muestra en la siguiente ilustración:

Ilustración 25 - El riesgo en función del impacto y la probabilidad



Fuente: https://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_Magerit.html#.Wuo5kO8vzcc

Ilustración 26 - El RIESGO en función de Impacto y la Probabilidad

RIESGO		**Probabilidad**				
		MB	B	M	A	MA
Impacto	MA	A	MA	MA	MA	MA
	A	M	A	A	MA	MA
	M	B	M	M	A	A
	B	MB	B	B	M	M
	MB	MB	MB	MB	B	B

Fuente: Libro 1 Magerit versión 3 p.28

7.3.7 Controles de Seguridad (Salvaguardas)

Se definen las salvaguardas o contra medidas como aquellos procedimientos o mecanismos tecnológicos que reducen el riesgo. Hay amenazas que se conjuran simplemente organizándose adecuadamente, otras requieres elementos técnicos (programas o equipos), otras seguridad física y, por último, está la política de personal. (Amutio Gómez, 2012).

7.3.7.1 Selección de salvaguardas

Ante el amplio abanico de posibles salvaguardas a considerar, es necesario hacer una criba inicial para quedarnos con aquellas que son relevantes para lo que hay que proteger. En esta criba se deben tener en cuenta los siguientes aspectos:

1. Tipo de activos a proteger, pues cada tipo se protege de una forma específica
2. Dimensión o dimensiones de seguridad que requieren protección
3. Amenazas de las que necesitamos protegernos
4. Si existen salvaguardas alternativas

Tabla 22 - Caracterización de las salvaguardas

SALVAGUARDA	NOMENCLATURA
Protecciones generales u horizontales	HARD
Protección de los datos / información	DI
Protección de las claves criptográficas	K
Protección de los servicios	SINFO
Protección de las aplicaciones (software)	SOFT
Protección de los equipos (hardware)	HARD
Protección de las comunicaciones	COMU
Protección en los puntos de interconexión con otros sistemas	IP
Protección de los soportes de información	SINFO
Protección de los elementos auxiliares	AUX
Seguridad física – Protección de las instalaciones	INST
Salvaguardas relativas al personal	PER
Salvaguardas de tipo organizativo	ORG
Continuidad de operaciones	CONOPER
Externalización	EXT
Adquisición y desarrollo	NEWSOF

Fuente: https://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_Magerit.html#.Wuo5kO8vzcc

7.3.7.2 Efecto de las salvaguardas

- Reduciendo la probabilidad de las amenazas.
- Limitando el daño causado.

7.3.7.3 Tipo de protección

Tabla 23 - Tipos de salvaguardas

EFECTO	TIPO
Preventivas: Reducen la probabilidad	• [PRE] Preventivas • [DIS] Disuasorias • [ELI] Eliminatorias
Acotan la degradación	• [MIN] Minimizadoras • [COR] Correctivas • [REC] Recuperativas
Consolidan el efecto de las demás	• [MON] de monitorización • [DEC] de detección • [CON] de concienciación • [ADM] administrativas

7.4 FORMALIZACIÓN DE ACTIVIDADES DEL PROYECTO MÉTODO DE ANÁLISIS DE RIESGOS (MAR)

Este conjunto de actividades tiene los siguientes objetivos:

- Levantar un modelo del valor del sistema, identificando y valorando los activos relevantes.
- Levantar un mapa de riesgos del sistema, identificando y valorando las amenazas sobre aquellos activos.
- Levantar un conocimiento de la situación actual de salvaguardas.
- Evaluar el impacto posible sobre el sistema en estudio, tanto el impacto potencial (sin salvaguardas),
- como el impacto residual (incluyendo el efecto de las salvaguardas desplegadas para proteger el sistema).
- Evaluar el riesgo del sistema en estudio, tanto el riesgo potencial (sin salvaguardas), como el riesgo residual (incluyendo el efecto de las salvaguardas desplegadas para proteger el sistema).
- Informar de las áreas del sistema con mayor impacto y/o riesgo a fin de que se puedan tomar las decisiones de tratamiento con motivo justificado.

El análisis de los riesgos se lleva a cabo por medio de las siguientes tareas:

Método de Análisis de Riesgos (MAR)
M.A.R._1 – Caracterización de los activos M.A.R_11 – Identificación de los activos M.A.R_12 – Dependencias entre activos M.A.R_13 – Valoración de los activos
Esta actividad busca identificar los activos relevantes dentro del sistema a analizar, caracterizándolos por el tipo de activo, identificando las relaciones entre los diferentes activos, determinando en qué dimensiones de seguridad son importantes y valorando esta importancia. El resultado de esta actividad es el informe denominado **"modelo de valor".**

M.A.R_2 – Caracterización de las amenazas M.A.R_21 – Identificación de las amenazas M.A.R_22 – Valoración de las amenazas.
Esta actividad busca identificar las amenazas relevantes sobre el sistema a analizar, caracterizándolas por las estimaciones de ocurrencia (probabilidad) y daño causado (degradación). El resultado de esta actividad es el informe denominado **"mapa de riesgos".**

M.A.R_3 – Caracterización de las salvaguardas M.A.R_31 – Identificación de las salvaguardas pertinentes M.A.R_32 – Valoración de las salvaguardas
Esta actividad busca identificar las salvaguardas desplegadas en el sistema a analizar, calificándolas por su eficacia frente a las amenazas que pretenden mitigar. El resultado de esta actividad se concreta en varios informes: — declaración de aplicabilidad — evaluación de salvaguardas — insuficiencias (o vulnerabilidades del sistema de protección)

MAR.4 – Estimación del estado de riesgo M.A.R_41 – Estimación del impacto M.A.R_42 – Estimación del riesgo

Esta actividad procesa todos los datos recopilados en las actividades anteriores para

- Realizar un informe del estado de riesgo: estimación de impacto y riesgo
- Realizar un informe de insuficiencias: deficiencias o debilidades en el sistema de salvaguardas

7.4.1 M.A.R_1 Caracterización de los activos

7.4.1.1 M.A.R_11 Identificación de los activos

Tabla 24 - Identificación de activos de la entidad

Copia de Seguridad de los Sistemas de Información	Archivos de copias de seguridad de los diferentes Sistemas de Información, Aplicaciones y Ambientes Virtuales de Aprendizaje.
Código Fuente.	Archivos de códigos fuentes de los diferentes Sistemas de Información propios desarrollados.
Gestión de Identidades	Gestión de las identidades, usuarios, contraseñas y privilegios de las cuentas administrativas para el uso de las computadoras institucionales.
Servicios Internos	Servicios de uso interno para funcionarios, contratistas y practicantes que cuentan con datos de acceso institucionales. Software, Bases de datos y Atención al Usuario.
Páginas web de acceso público	Página, portales, sitios y aplicativos que son disponibles para el acceso al público.
Correo Electrónico	Cuentas de correo electrónico institucional.
Gestores de Bases de Datos	Administran y gestionan las bases de datos que se utilizan para soportar todo el software administrativo y demás que apoyan a los demás procesos institucionales.
Software de Antivirus	Software para prevenir y eliminar el *malware*.
Sistemas Operativos	Software que administra los recursos de las computadoras de uso institucional.
Dispositivos de Respaldo	Dispositivos que almacenan la información y son útiles para la recuperación de desastres.
Firewall	Controla el tráfico entrante/saliente de la red de datos aplicando reglas de seguridad.
Servidores	Computadoras especializadas en proveer los recursos, almacenar datos y ejecutar el software y diferentes aplicaciones a través de la red.
Computadoras Portátiles de Uso Institucional	Permiten la realización de tareas del personal administrativo conectadas a través de la red interna.
Computadoras de Escritorio de Uso Institucional	Permiten la realización de tareas del personal administrativo conectadas a través de la red interna.
Escáner	Dispositivos para transformar la información en formato digital.
Impresoras	Dispositivos para la impresión en papel.
Router	Redirige el tráfico de datos de la red interna con el exterior. Permite la conexión a internet a través del ISP (Proveedor de Servicios de Internet).

Switches	Administra las VLANS el permite realizar la segmentación de la red de datos y gestionar y optimizar el ancho de banda, así como expandir la conexión de las computadoras de uso institucional.
Puntos de Acceso Inalámbricos	Amplían la cobertura de la red por medio de conexiones inalámbricas.
Red de Área Local	Permite la interconexión de las computadoras institucionales así como el acceso a los diferentes servicios. Soporta el desarrollo normal de los procesos.
Rack	Aloja los servidores, *router*, *switches* y *firewall* protegiéndolos de la humedad, golpes o uso malintencionado.
Fuente de Alimentación (RED ELÉCTRICA REGULADA)	Provee y regula la energía a los Servidores.
Sistema de Alimentación Ininterrumpida UPS	Provee energía temporal a los Servidores y demás dispositivos vitales en caso de fallas eléctricas inesperadas.
Cableado Eléctrico	Provee energía eléctrica a las instalaciones y dispositivos.
Cableado estructurado	Se conoce como cableado estructurado al sistema de cables, conectores, canalizaciones y dispositivos que permiten establecer una infraestructura de telecomunicaciones en un edificio.
Equipos Auxiliares	Activos que son necesarios para que otros activos funciones correctamente y contribuyen a la prestación de servicios. • Antenas • Radios • Mobiliario • Otros.

Fuente: Autor

Estos activos se clasifican según el Tipo de Activo en la metodología MAGERIT de la siguiente manera:

Tabla 25 - Identificación de activos de la entidad de acuerdo a la metodología Magerit.

DATOS/INFORMACIÓN		
DESCRIPCIÓN	**CONTENIDO**	**RESPONSABLE**
Copias de Seguridad de los Sistemas de Información	Archivos de copias de seguridad de los diferentes Sistemas de Información, Aplicaciones y Ambientes Virtuales de Aprendizaje.	Jefe Oficina de sistemas
Contratos	Contratos laborales, licitaciones públicas, otros.	Jefe Contratación
Historial Laboral	Historial del tiempo laborado por los empleados, contratista, practicantes	Jefe Talento Humano
Registros de Actividad	Archivos de registros de actividad de los diferentes Sistemas de Información y Aplicaciones que posee en la actualidad la administración municipal.	Jefe Oficina de sistemas
Códigos Fuentes	Archivos de códigos fuentes de los diferentes Sistemas de Información propios y desarrollados por terceros.	Jefe Oficina de sistemas

SERVICIOS		
DESCRIPCIÓN	**CONTENIDO**	**RESPONSABLE**
Correo Electrónico	Correo electrónico de uso institucional para los funcionarios, contratistas y practicantes.	Jefe Oficina de sistemas
Gestión de Identidades	Gestión de las identidades, usuarios, contraseñas y privilegios de las cuentas administrativas para el uso de las computadoras institucionales.	Jefe Oficina de sistemas
Servicios Internos	Servicios de uso interno para los funcionarios, contratistas y practicantes que cuentan con datos de acceso institucionales. Software administrativo, Bases de Datos, Gestión Documental y Atención al Usuario.	Jefe Oficina de sistemas
Páginas web de acceso público	Páginas, portales, sitios y aplicativos que son disponibles para el acceso público.	Jefe Oficina de sistemas

SOFTWARE		
DESCRIPCIÓN	**CONTENIDO**	**RESPONSABLE**
Software de Desarrollo Propio	Software desarrollado internamente por la institución para cumplir sus necesidades a la medida.	Jefe Oficina de sistemas
Software Estándar	Software desarrollado por terceros y adaptado a la institución. Software que soporta los procesos administrativos y los procesos misionales de la entidad	Jefe Oficina de sistemas
Gestores de Bases de Datos	Administran y gestionan las bases de datos que se utilizan para soportar todo el software administrativo y demás que apoyan a los demás procesos institucionales.	Jefe Oficina de sistemas
Ofimática	Software necesario para la realización de las actividades, así como la producción de recursos.	Jefe Oficina de sistemas

Software de Antivirus	Software para prevenir y eliminar el *malware*.	Jefe Oficina de sistemas
Sistemas Operativos	Software que administra los recursos de las computadoras de uso institucional.	Jefe Oficina de sistemas

HARDWARE		
DESCRIPCIÓN	**CONTENIDO**	**RESPONSABLE**
Dispositivos de Respaldo	Dispositivos que almacenan la información y son útiles para la recuperación de desastres.	Jefe Oficina de sistemas
Firewall	Controla el tráfico entrante/saliente de la red de datos aplicando reglas de seguridad.	Jefe Oficina de sistemas
Antenas	Envío/Recepción de señales para la comunicación con otras dependencias de la administración municipal.	Jefe Oficina de sistemas
Servidores	Computadoras especializadas en proveer los recursos, almacenar datos y ejecutar el software y diferentes aplicaciones a través de la red.	Jefe Oficina de sistemas
Computadoras Portátiles de Uso Institucional	Permiten la realización de tareas del personal administrativo conectadas a través de la red interna.	Jefe Oficina de sistemas
Computadoras de Escritorio de Uso Institucional	Permiten la realización de tareas del personal administrativo conectadas a través de la red interna.	Jefe Oficina de sistemas
Impresoras	Dispositivos para la impresión en papel.	Jefe Oficina de sistemas
Router	Redirige el tráfico de datos de la red interna con el exterior. Permite la conexión a internet a través del ISP (Proveedor de Servicios de Internet).	Jefe Oficina de sistemas
Escáner	Dispositivos para transformar la información en formato digital.	Jefe Oficina de sistemas
Switch	Administra las VLAN, permite realizar la segmentación de la red de datos y gestionar y optimizar el ancho de banda, así como expandir la conexión de las computadoras de uso institucional.	Jefe Oficina de sistemas
Puntos de Acceso Inalámbricos	Amplían la cobertura de la red por medio de conexiones inalámbricas.	Jefe Oficina de sistemas

[COM] COMUNICACIONES		
DESCRIPCIÓN	**CONTENIDO**	**RESPONSABLE**
Internet	Permite el acceso a recursos de la web.	Jefe Oficina de sistemas
Red de Área Local	Permite la interconexión de las computadoras institucionales así como el acceso a los diferentes servicios. Soporta el desarrollo normal de los procesos.	Jefe Oficina de sistemas

Conectividad Inalámbrica	Permite la conectividad inalámbrica de las computadoras institucionales, así como amplía la cobertura.	Jefe Oficina de sistemas

EQUIPO AUXILIAR		
DESCRIPCIÓN	**CONTENIDO**	**RESPONSABLE**
Fibra Óptica	Provee transmisión de datos a alta velocidad.	Jefe Oficina de sistemas
Rack	Aloja los servidores, *router*, *switches* y *firewall* protegiéndoles de la humedad, golpes o uso malintencionado.	Jefe Oficina de sistemas
Fuente de Alimentación (RED ELÉCTRICA REGULADA)	Provee y regula la energía a los Servidores y al rack	Jefe Oficina de sistemas
Sistema de Alimentación Ininterrumpida	Provee energía temporal a los Servidores y demás dispositivos vitales en caso de fallas eléctricas inesperadas.	Jefe Oficina de sistemas
Cableado Eléctrico	Provee energía eléctrica a las instalaciones y dispositivos.	Jefe Oficina de sistemas
Cableado Estructurado	Sistema de cables, conectores, canalizaciones y dispositivos que permiten establecer una infraestructura de telecomunicaciones en un edificio.	Jefe Oficina de sistemas

INSTALACIONES

DESCRIPCIÓN	**CONTENIDO**	**RESPONSABLE**
Oficina de Sistemas de Información y Telemática	Estructura física que alberga la Oficina de Sistemas de Información y Telemática.	Secretario de Infraestructura, ambiente y hábitat

[P] PERSONAL		
DESCRIPCIÓN	**CONTENIDO**	**RESPONSABLE**
Administrador de Sistema	Persona encargada de administrar, gestionar, solucionar y ayudar en el correcto funcionamiento de los diferentes Sistemas de Información.	Jefe Oficina de sistemas
Administrador de red de datos	Persona encargada de administrar y gestionar el tráfico de datos en la red interna, así como configurar los diferentes dispositivos de comunicaciones que garanticen un óptimo rendimiento para el acceso a servicios y Sistemas de Información.	Jefe Oficina de sistemas

Administrador de Bases de Datos	Persona que administra, configura y optimiza el rendimiento de las diferentes bases de datos que utilizan los Sistemas de Información para el soporte de los procesos institucionales.	Jefe Oficina de sistemas
Desarrolladores de Software	Persona que se encarga de programar el código fuente para los Sistemas de Información en su defecto en el desarrollado por terceros para satisfacer las necesidades institucionales.	Jefe Oficina de sistemas

Fuente: Autor

7.4.1.2 M.AR_12 Valoración de los activos de acuerdo al impacto

Se determina la valoración de los activos de la oficina de acuerdo al tipo Cualitativo que establece MAGERIT y el impacto que tiene en la entidad, de acuerdo a la siguiente escala:

Tabla 26 - Valoración cualitativa de los activos informáticos en MAGERIT.

IMPACTO	NOMENCLATURA	VALOR	DESCRIPCIÓN
MUY ALTO	**MA**	**10**	El daño tiene consecuencias muy graves para la entidad y podrían ser irreversibles.
ALTO	**A**	**7-9**	El daño tiene consecuencias muy graves para la entidad.
MEDIO	**M**	**4-6**	El daño contiene consecuencias relevantes para la entidad y su operación.
BAJO	**B**	**1-3**	El daño contiene consecuencias relevantes, pero no afecta a una gran parte de la entidad.
MUY BAJO	**MB**	**0**	El daño no contiene consecuencias relevantes para la entidad.

Fuente: Autor

Tabla 27 - Valoración de los activos de acuerdo al impacto

DATOS / INFORMACIÓN		
DESCRIPCIÓN	**IMPACTO**	**RAZÓN**
Copias de Seguridad de los Sistemas de Información	**MUY ALTO**	Son importantes para la recuperación de la información ante un desastre
Contratos	**MUY ALTO**	Los contratos son esenciales para los procesos jurídicos-administrativos.
Historial Laboral	**MUY ALTO**	Archivos esenciales para el historial laboral de los funcionarios, contratistas, practicantes.
Registros de Actividad	**MUY ALTO**	Los archivos de registros son esenciales para realizar seguimiento a fallos en los Sistemas de Información para determinar posibles causas de malfuncionamiento o acceso no autorizado.
Códigos Fuentes	**MUY ALTO**	Los archivos de código fuente contienen información de cómo se ejecutan los procesos internos en los Sistemas de Información desarrollados para la institución.

SERVICIOS INTERNOS		
DESCRIPCIÓN	**IMPACTO**	**RAZÓN**
Correo Electrónico	**MUY ALTO**	Los correos institucionales proporcionan comunicación entre las mismas dependencias y con otras entidades del estado.
Gestión de Identidades	**MUY ALTO**	Acceso de los funcionarios, contratistas y practicantes a los servicios de información de la entidad.
Servicios Internos	**MUY ALTO**	Acceso a los servicios internos institucionales para el desarrollo normal de los procesos.
Páginas web de acceso público	**ALTO**	Acceso a la página web institucional, Intranet y otros sitos que ofrecen servicios a los funcionarios, contratistas, practicantes y los usuarios externos de la administración municipal.

SOFTWARE		
DESCRIPCIÓN	**IMPACTO**	**RAZÓN**
Software de Desarrollo Propio	**BAJO**	En la administración municipal se desarrollan pocas aplicaciones.
Software Estándar	**MUY ALTO**	Utilizados para el normal desarrollo de los procesos institucionales. En la administración municipal se utiliza la aplicación SAIMYR, esta aplicación contiene todos los módulos utilizados para el normal desarrollo de los procesos institucionales.
Gestores de Bases de Datos	**MUY ALTO**	Almacena toda la información de los diferentes Sistemas de Información, así como el soporte para el desarrollo normal de los procesos y tomas de decisiones. Dentro de ellos se encuentran Oracle 11g, SQL Server 2012 y MySQL.
Ofimática	**BAJO**	Utilizado para la ejecución de tareas tipo ofimática.

Software de Antivirus	**ALTO**	Utilizado para la prevención y eliminación de software malintencionado, así como evitar la propagación de malware por la red.
Sistemas Operativos	**MEDIO**	Gestionan los recursos de los equipos informáticos. (hardware y software)

HARDWARE		
DESCRIPCIÓN	**IMPACTO**	**RAZÓN**
Dispositivos de Respaldo	**MUY ALTO**	Utilizados para la recuperación de información después de un desastre o eventualidad
Firewall	**MUY ALTO**	Dispositivo de seguridad perimetral, dispositivo que filtra los paquetes de datos. Esencial para la configuración de seguridad de la red.
Antenas	**MUY ALTO**	Esencial para establecer los enlaces de comunicación con las diferentes dependencias de la administración municipal.
Servidores	**MUY ALTO**	Dispositivos esenciales para el correcto funcionamiento de los diferentes Sistemas de Información que soportan los procesos institucionales. Dentro de ellos se encuentran los Servidores de Aplicaciones, DNS y Bases de Datos.
Computadoras Portátiles de Uso Institucional	**BAJO**	Dispositivos para la ejecución de tareas.
Computadoras de Escritorio de Uso Institucional	**BAJO**	Dispositivos para la ejecución de tareas.
Impresoras	**MUY BAJO**	Dispositivo para realizar impresiones en papel.
Router	**ALTO**	Esencial para direccionar el tráfico de datos interno y externo. A su vez, hace el papel de Gateway para dar salida a Internet.
Escáner	**BAJO**	Dispositivos para la ejecución de tareas.
Switch	**ALTO**	Esencial para direccionar el tráfico de datos interno, administración de VLAN y segmentar el ancho de banda con el fin de optimizarla.
Puntos de Acceso Inalámbricos	**BAJO**	Dispositivos que amplían la cobertura de la red para dar acceso inalámbrico.

COMUNICACIONES		
DESCRIPCIÓN	**IMPACTO**	**RAZÓN**
Internet	**ALTO**	Esencial para la comunión con otras redes externas.
Red de Área Local	**MUY ALTO**	Esencial para la transmisión de datos y dar soporte al normal funcionamiento de los servicios internos institucionales, además para la comunicación entre los servidores de aplicación y de base de datos con los equipos de los usuarios de la red.
Conectividad Inalámbrica	**BAJO**	Amplía la cobertura y otorga acceso inalámbrico a estos tipos de dispositivos.

EQUIPO AUXILIAR		
DESCRIPCIÓN	**IMPACTO**	**RAZÓN**
Fibra Óptica	**MUY ALTO**	Otorga alta velocidad de transmisión en el tráfico de datos interno. Da soporte de conectividad a toda la entidad.
Rack	**ALTO**	Mantiene los dispositivos de red como el router, switches, firewall y servidores organizados y asegurados.
Fuente de Alimentación (RED eléctrica)	**MUY ALTO**	Esencial para el funcionamiento normal de todos los dispositivos que soportan los Sistemas de Información y procesos institucionales.
Sistema de Alimentación Ininterrumpida	**ALTO**	Esencial para mantener funcionando a los dispositivos en caso de una eventual falla en el suministro eléctrico, así como también evita el daño parcial o total del hardware.
Cableado Eléctrico	**MUY ALTO**	Cableado esencial para mantener en funcionamiento los dispositivos y el normal desarrollo de los procesos institucionales.
Cableado Estructurado	**ALTO**	Cableado esencial para mantener la comunicación entre los diferentes dispositivos de red y los equipos de cómputo con los diferentes servidores.

INSTALACIONES		
DESCRIPCIÓN	**IMPACTO**	**RAZÓN**
Oficina de Sistemas de Información y Telemática	**MUY ALTO**	Esencial para el normal funcionamiento de todos los Sistemas de Información que soportan los procesos institucionales.

[P] PERSONAL		
DESCRIPCIÓN	**IMPACTO**	**RAZÓN**
Administrador de Sistema	**MUY ALTO**	Personas encargadas de administrar los diferentes Sistemas de Información que dan soporte a los procesos institucionales y sus servicios.
Administrador de red de datos	**MUY ALTO**	Personas encargadas de administrar, configurar y operar las redes de comunicación de datos que dan soporte al normal funcionamiento de los servicios internos
Administrador de Bases de Datos	**MUY ALTO**	Persona encargada de administrar, configurar y optimizar el rendimiento de las bases de datos que contienen los datos de los diferentes Sistemas de Información, así como velar por la seguridad de que éstos se mantengan confidenciales, disponibles e íntegros.
Desarrolladores de Software	**ALTO**	Personas encargadas de desarrollar y/o programar el software que se ajuste a las necesidades de la institución.

Fuente: Autor

7.4.1.3 M.A.R_13 Valoración de los activos de acuerdo a sus dimensiones

Tabla 28 - Valoración de los activos de acuerdo a sus dimensiones

DATOS/INFORMACIÓN					
DESCRIPCIÓN	**DIMENSIONES**				
	[D]	**[I]**	**[C]**	**[A]**	**[T]**
Copias de Seguridad de los Sistemas de Información	10	5	6		
• Pudiera causar la interrupción de actividades propias de la Organización					
Contratos	8	8	8		
• Probablemente quebrante seriamente la ley o algún reglamento de protección de información personal. • Constituye un serio incumplimiento de obligaciones contractuales relativas a la seguridad de la información proporcionada por terceros.					
Historial Laboral	6	2	3		
• Pudiera causar molestias a un individuo					
Registros de Actividad	7	7	7		
• Pudiera causar una merma en la seguridad o dificultar la investigación de un incidente.					
Códigos Fuentes	4	5	6		
• Probablemente perjudique la eficacia o seguridad de la misión operativa o logística.					

SERVICIOS					
DESCRIPCIÓN	**DIMENSIONES**				
	[D]	**[I]**	**[C]**	**[A]**	**[T]**
Correo Electrónico	7				
• Probablemente cause la interrupción de actividades propias de la Organización					
Gestión de Identidades			10	10	
• Probablemente cause un incumplimiento excepcionalmente grave de una ley o regulación. • probablemente sea causa de un grave incidente de seguridad o dificulte la investigación de incidentes graves. • Impida la investigación de delitos graves o facilite su comisión.					
Servicios Internos	5	5	5		
• Probablemente cause la interrupción de actividades propias de la Organización • Probablemente sea causa de un serio incidente de seguridad o dificulte la investigación de incidentes serios					

Páginas web de acceso público	7	4	8		
• Pudiera causar molestias a un individuo					

SOFTWARE					
DESCRIPCIÓN	**DIMENSIONES**				
	[D]	**[I]**	**[C]**	**[A]**	**[T]**
Software de Desarrollo Propio		3	3		
• Probablemente perjudique la eficacia o seguridad de la misión operativa o logística.					
Software Estándar		8	10		
• Probablemente perjudique la eficacia o seguridad de la misión operativa o logística.					
Gestores de Bases de Datos	10	10	10		
• Probablemente cause una interrupción seria de las actividades propias de la Organización con un impacto significativo en otras organizaciones.					
Ofimática	2				
• Pudiera causar molestias a un individuo.					
Software de Antivirus	5				
• Probablemente perjudique la eficacia o seguridad de la misión operativa o logística.					
Sistemas Operativos	2				
• Pudiera causar molestias a un individuo.					

HARDWARE					
DESCRIPCIÓN	**DIMENSIONES**				
	[D]	**[I]**	**[C]**	**[A]**	**[T]**
Dispositivos de Respaldo	10	5			
• Probablemente impediría la operación efectiva de la Organización.					
Firewall	6		8		
• Probablemente impediría la operación efectiva de la Organización.					
Antenas	10	5			
• Pudiera impedir la operación efectiva de una parte de la Organización.					
Servidores	10	10	10		
• Probablemente impediría la operación efectiva de la Organización.					

Computadoras Portátiles de Uso Institucional	5				
• Pudiera impedir la operación efectiva de una parte de la Organización.					
Computadoras de Escritorio de Uso Institucional	5				
• Pudiera impedir la operación efectiva de una parte de la Organización.					
Impresoras	2				
• Pudiera causar molestias a un individuo.					
Router	5				
• Probablemente cause la interrupción de actividades propias de la Organización.					
Escáner	2				
• Pudiera causar molestias a un individuo.					
Switch	5				
• Probablemente cause la interrupción de actividades propias de la Organización.					
Puntos de Acceso Inalámbricos	2				
• Pudiera causar molestias a un individuo.					

COMUNICACIONES					
DESCRIPCIÓN	**DIMENSIONES**				
	[D]	**[I]**	**[C]**	**[A]**	**[T]**
Internet	7				
• Probablemente impediría la operación efectiva de más de una parte de la Organización					
Red de Área Local	10	8			
• Probablemente impediría la operación efectiva de la Organización					
Conectividad Inalámbrica	3				
• Pudiera impedir la operación efectiva de una parte de la Organización					

EQUIPO AUXILIAR					
DESCRIPCIÓN	**DIMENSIONES**				
	[D]	**[I]**	**[C]**	**[A]**	**[T]**
Fibra Óptica	10				
• Pudiera causar la interrupción de actividades propias de la Organización.					
Rack	5				
• Pudiera causar la interrupción de actividades propias de la Organización.					
Fuente de Alimentación (RED eléctrica)	10				
• Pudiera causar la interrupción de actividades propias de la Organización.					

Sistema de Alimentación Ininterrumpida	7				
• Pudiera causar la interrupción de actividades propias de la Organización.					
Cableado Eléctrico	10				
• Pudiera causar la interrupción de actividades propias de la Organización.					
Cableado Estructurado	8				

INSTALACIONES					
DESCRIPCIÓN	**DIMENSIONES**				
	[D]	**[I]**	**[C]**	**[A]**	**[T]**
Oficina de Sistemas de Información y Telemática	10				
• Probablemente impediría seriamente la operación efectiva de la Organización, pudiendo llegar a su cierre.					

PERSONAL						
CÓDIGO	**SUBTIPO**	**DESCRIPCIÓN**	**DIMENSIONES**				
			[D]	**[I]**	**[C]**	**[A]**	**[T]**
Administrador de Sistema			10		10		
• Pudiera impedir la operación efectiva de una parte de la Organización.							
Administrador de red de datos			10		10		
• Pudiera impedir la operación efectiva de una parte de la Organización.							
Administrador de Bases de Datos			10		10		
• Pudiera impedir la operación efectiva de una parte de la Organización.							
Desarrolladores de Software			8	8	8		
• Pudiera impedir la operación efectiva de una parte de la Organización.							

Fuente: Autor

7.4.2 M.A.R_2 Caracterización de las amenazas

7.4.2.1 M.A.R_21 Identificación y valoración de las Amenazas.

De acuerdo a las amenazas que se identifican en MAGERIT, éstas se establecen para cada activo determinando su probabilidad o frecuencia de ocurrencia y el impacto que tiene en cada una de las dimensiones de seguridad.

7.4.2.2 M.A_22 Valoración de las Amenazas.

Las amenazas se valoran de acuerdo al impacto que están tienen sobre cada uno de los activos de información en sus dimensiones:

DIMENSIONES	**[D]**	DISPONIBILIDAD
	[I]	INTEGRIDAD
	[C]	CONFIDENCIALIDAD
	[A]	AUTENTICIDAD
	[T]	TRAZABILIDAD

Tabla 29- Valoración cuantitativa de la amenazas

PROBABILIDAD	RANGO	VALOR
FRECUENCIA MUY ALTA	1 VEZ AL DÍA	**100**
FRECUENCIA ALTA	1 VEZ CADA SEMANA	**75**
FRECUENCIA MEDIA	1 VEZ CADA MES	**50**
FRECUENCIA BAJA	1 VEZ CADA 6 MESES	**25**
FRECUENCIA MUY BAJA	1 VEZ CADA AÑO	**1**

Fuente: Autor

DATOS/INFORMACIÓN

Tabla 30 - Valoración Cualitativa de las amenazas en cuanto a sus dimensiones

Copias de Seguridad de los Sistemas de Información						
AMENAZA	**FRECUENCIA**	**DIMENSIONES %**				
		[D]	**[I]**	**[C]**	**[A]**	**[T]**
Errores de los usuarios	25	**100**	**100**	**100**		
Errores del administrador	25	**100**	**100**	**100**		
Destrucción de información	25	**100**				

Contratos						
AMENAZA	**FRECUENCIA**	**DIMENSIONES %**				
		[D]	**[I]**	**[C]**	**[A]**	**[T]**
Errores de los usuarios	25		**100**	**100**		
Alteración accidental de la información	25		**100**			
Destrucción de información	25	**100**				
Fugas de información	25			**100**		
Suplantación de la identidad del usuario	25	**100**	**100**	**100**		
Abuso de privilegios de acceso	25	**100**	**100**	**100**		

Historial Laboral						
AMENAZA	**FRECUENCIA**	**DIMENSIONES %**				
		[D]	**[I]**	**[C]**	**[A]**	**[T]**
Errores de los usuarios	25	**100**	**100**	**100**		
Alteración accidental de la información	25		**100**			
Destrucción de información	25	**100**				
Fugas de información	25			**100**		
Suplantación de la identidad del usuario	25	**100**	**100**	**100**		
Abuso de privilegios de acceso	25	**100**	**100**	**100**		

Registros de Actividad						
AMENAZA	**FRECUENCIA**	**DIMENSIONES %**				
		[D]	**[I]**	**[C]**	**[A]**	**[T]**
Errores del administrador	25	**100**	**100**	**100**		
Errores de monitorización (log)	25		**100**			**100**
Manipulación de los registros de actividad (log)	25		**100**			**100**
Manipulación de la configuración	25	**100**	**100**	**100**		

Códigos Fuentes						
AMENAZA	**FRECUENCIA**	**DIMENSIONES %**				
		[D]	**[I]**	**[C]**	**[A]**	**[T]**
Avería de origen físico o lógico	50					
Alteración accidental de la información	25		**100**			
Destrucción de información	25	**100**				
Fugas de información	25			**100**		

SERVICIOS

Correo Electrónico						
AMENAZA	**FRECUENCIA**	**DIMENSIONES %**				
		[D]	**[I]**	**[C]**	**[A]**	**[T]**
Errores de los usuarios	25	**100**	**100**	**100**		
Destrucción de información	25	**100**				
Fugas de información	25			**100**		
Suplantación de la identidad del usuario	25	**100**	**100**	**100**		
Abuso de privilegios de acceso	25	**100**	**100**	**100**		
Uso no previsto	25	**100**	**100**	**100**		

Gestión de Identidades						
AMENAZA	**FRECUENCIA**	**DIMENSIONES %**				
		[D]	**[I]**	**[C]**	**[A]**	**[T]**
Errores del administrador	25	**100**	**100**	**100**		
Suplantación de la identidad del usuario	25	**100**	**100**	**100**		
Abuso de privilegios de acceso	25	**100**	**100**	**100**		

Servicios Internos						
AMENAZA	**FRECUENCIA**	**DIMENSIONES %**				
		[D]	**[I]**	**[C]**	**[A]**	**[T]**
Avería de origen físico o lógico	50	**100**				
Errores de los usuarios	50	**100**	**100**	**100**		
Alteración accidental de la información	25		**100**			
Destrucción de información	25	**100**				
Fugas de información	50			**100**		
Caída del sistema por agotamiento de recursos	50	**100**				
Pérdida de equipos	25	**100**		**100**		
Suplantación de la identidad del usuario	25	**100**	**100**	**100**		
Abuso de privilegios de acceso	25	**100**	**100**	**100**		
Uso no previsto	25	**100**	**100**	**100**		

Páginas web de acceso público						
AMENAZA	**FRECUENCIA**	**DIMENSIONES %**				
		[D]	**[I]**	**[C]**	**[A]**	**[T]**
Errores de los usuarios	50	**100**	**100**	**100**		
Suplantación de la identidad del usuario	25	**100**	**100**	**100**		
Uso no previsto	25	**100**	**100**	**100**		

SOFTWARE

Software Estándar						
AMENAZA	**FRECUENCIA**	**DIMENSIONES %**				
		[D]	**[I]**	**[C]**	**[A]**	**[T]**
Avería de origen físico o lógico	50					
Errores de los usuarios	25	**100**	**100**	**100**		
Destrucción de información	25	**100**				
Fugas de información	25			**100**		
Vulnerabilidades de los programas (software)	50			**100**		
Errores de mantenimiento / actualización de programas (software)	50	**100**	**100**			
Abuso de privilegios de acceso	25	**100**	**100**	**100**		
Uso no previsto	25	**100**	**100**	**100**		

Gestores de Bases de Datos						
AMENAZA	**FRECUENCIA**	**DIMENSIONES %**				
		[D]	**[I]**	**[C]**	**[A]**	**[T]**
Avería de origen físico o lógico	50					
Errores del administrador	25	**100**	**100**	**100**		
Destrucción de información	25	**100**				
Fugas de información	25			**100**		

Vulnerabilidades de los programas (software)	25			**100**		
Errores de mantenimiento / actualización de programas (software)	50	**100**	**100**			
Suplantación de la identidad del usuario	25	**100**	**100**	**100**		
Abuso de privilegios de acceso	25	**100**	**100**	**100**		
Uso no previsto	25	**100**	**100**	**100**		

Ofimática						
AMENAZA	**FRECUENCIA**	**DIMENSIONES %**				
		[D]	**[I]**	**[C]**	**[A]**	**[T]**
Avería de origen físico o lógico	75					
Errores de los usuarios	50	**100**	**100**	**100**		
Errores de mantenimiento / actualización de programas (software)	50	**100**	**100**			
Uso no previsto	25	**100**	**100**	**100**		

Software de Antivirus						
AMENAZA	**FRECUENCIA**	**DIMENSIONES %**				
		[D]	**[I]**	**[C]**	**[A]**	**[T]**
Avería de origen físico o lógico	25	**100**	**100**	**100**		
Errores del administrador	25	**100**	**100**	**100**		
Errores de mantenimiento / actualización de programas (software)	50	**100**	**100**			

Sistemas Operativos						
AMENAZA	**FRECUENCIA**	**DIMENSIONES %**				
		[D]	**[I]**	**[C]**	**[A]**	**[T]**
Avería de origen físico o lógico	25	**100**				
Vulnerabilidades de los programas (software)	25	**100**	**100**	**100**		
Errores de mantenimiento / actualización de programas (software)	25	**100**	**100**			
Abuso de privilegios de acceso	25	**100**	**100**	**100**		
Uso no previsto	25	**100**	**100**			

HARDWARE

Dispositivos de Respaldo						
AMENAZA	**FRECUENCIA**	**DIMENSIONES %**				
		[D]	**[I]**	**[C]**	**[A]**	**[T]**
Fuego	1	**100**				
Daños por agua	25	**100**				
Desastres naturales	25	**100**				
Corte del suministro eléctrico	50	**100**				
Condiciones inadecuadas de temperatura o humedad	50	**100**				

Degradación de los soportes de almacenamiento de la información	25	**100**				
Emanaciones electromagnéticas	25			**100**		
Errores del administrador	25	**100**	**100**	**100**		
Destrucción de información	25	**100**				

Firewall						
AMENAZA	**FRECUENCIA**	**DIMENSIONES %**				
		[D]	**[I]**	**[C]**	**[A]**	**[T]**
Fuego	1	**100**				
Daños por agua	25	**100**				
Desastres naturales	25	**100**				
Corte del suministro eléctrico	50	**100**				
Condiciones inadecuadas de temperatura o humedad	25	**100**				
Emanaciones electromagnéticas	25			**100**		
Errores del administrador	25	**100**	**100**	**100**		
Errores de configuración	25		**100**			
Errores de mantenimiento / actualización de programas (software)	25	**100**	**100**			
Caída del sistema por agotamiento de recursos	1	**100**				

Antenas						
AMENAZA	**FRECUENCIA**	**DIMENSIONES %**				
		[D]	**[I]**	**[C]**	**[A]**	**[T]**
Fuego	1	**100**				
Daños por agua	25	**100**				
Desastres naturales	25	**100**				
Condiciones inadecuadas de temperatura o humedad	25	**100**				
Emanaciones electromagnéticas	25	**100**				
Caída del sistema por agotamiento de recursos	1	**100**				

Servidores						
AMENAZA	**FRECUENCIA**	**DIMENSIONES %**				
		[D]	**[I]**	**[C]**	**[A]**	**[T]**
Fuego	1	**100**				
Daños por agua	25	**100**				
Desastres naturales	25	**100**				
Corte del suministro eléctrico	25	**100**				
Condiciones inadecuadas de temperatura o humedad	50	**100**				
Emanaciones electromagnéticas	25	**100**				
Errores del administrador	25	**100**	**100**	**100**		
Errores de configuración	25		**100**			
Destrucción de información	25	**100**				
Fugas de información	25	**100**				
Caída del sistema por agotamiento de recursos	25	**100**				
Abuso de privilegios de acceso	25	**100**	**100**	**100**		
Uso no previsto	25	**100**	**100**	**100**		

Computadoras Portátiles de Uso Institucional						
AMENAZA	**FRECUENCIA**	**DIMENSIONES %**				
		[D]	**[I]**	**[C]**	**[A]**	**[T]**
Fuego	1	**100**				
Daños por agua	25	**100**				
Desastres naturales	25	**100**				
Condiciones inadecuadas de temperatura o humedad	25	**100**				
Destrucción de información	25	**100**				
Fugas de información	50	**100**				
Pérdida de equipos	25	**100**		**100**		
Uso no previsto	25	**100**	**100**	**100**		

Computadoras de Escritorio de Uso Institucional						
AMENAZA	**FRECUENCIA**	**DIMENSIONES %**				
		[D]	**[I]**	**[C]**	**[A]**	**[T]**
Fuego	1	**100**				
Daños por agua	25	**100**				
Desastres naturales	25	**100**				
Corte del suministro eléctrico	50	**100**				
Condiciones inadecuadas de temperatura o humedad	25	**100**				
Destrucción de información	25	**100**				
Fugas de información	25	**100**				
Pérdida de equipos	25	**100**		**100**		
Uso no previsto	25	**100**	**100**	**100**		

Impresoras						
AMENAZA	**FRECUENCIA**	**DIMENSIONES %**				
		[D]	**[I]**	**[C]**	**[A]**	**[T]**
Fuego	1	**100**				
Daños por agua	25	**100**				
Desastres naturales	25	**100**				
Corte del suministro eléctrico	50	**100**				
Condiciones inadecuadas de temperatura o humedad	25	**100**				
Interrupción de otros servicios y suministros esenciales	50	**100**				
Uso no previsto	25	**100**	**100**	**100**		

Router						
AMENAZA	**FRECUENCIA**	**DIMENSIONES %**				
		[D]	**[I]**	**[C]**	**[A]**	**[T]**
Fuego	1	**100**				
Daños por agua	25	**100**				
Desastres naturales	25	**100**				
Corte del suministro eléctrico	50	**100**				
Condiciones inadecuadas de temperatura o humedad	25	**100**				
Caída del sistema por agotamiento de recursos	25	**100**				
Pérdida de equipos	25	**100**		**100**		

Escáner						
AMENAZA	**FRECUENCIA**	**DIMENSIONES %**				
		[D]	**[I]**	**[C]**	**[A]**	**[T]**
Fuego	1	**100**				
Daños por agua	25	**100**				
Desastres naturales	25	**100**				
Corte del suministro eléctrico	50	**100**				
Condiciones inadecuadas de temperatura o humedad	25	**100**				
Uso no previsto	25	**100**	**100**	**100**		

Switch						
AMENAZA	**FRECUENCIA**	**DIMENSIONES %**				
		[D]	**[I]**	**[C]**	**[A]**	**[T]**
Fuego	1	**100**				
Daños por agua	25	**100**				
Desastres naturales	25	**100**				
Corte del suministro eléctrico	50	**100**				
Condiciones inadecuadas de temperatura o humedad	25	**100**				
Caída del sistema por agotamiento de recursos	25	**100**				
Pérdida de equipos	25	**100**		**100**		

Puntos de Acceso Inalámbricos						
AMENAZA	**FRECUENCIA**	**DIMENSIONES %**				
		[D]	**[I]**	**[C]**	**[A]**	**[T]**
Fuego	1	**100**				
Daños por agua	25	**100**				
Desastres naturales	25	**100**				
Corte del suministro eléctrico	50	**100**				
Condiciones inadecuadas de temperatura o humedad	25	**100**				
Emanaciones electromagnéticas	25	**100**				
Caída del sistema por agotamiento de recursos	25	**100**				
Pérdida de equipos	25	**100**		**100**		
Suplantación de la identidad del usuario	25	**100**	**100**	**100**		
Abuso de privilegios de acceso	25	**100**	**100**	**100**		
Uso no previsto	25	**100**	**100**	**100**		

COMUNICACIONES

Internet						
AMENAZA	**FRECUENCIA**	**DIMENSIONES %**				
		[D]	**[I]**	**[C]**	**[A]**	**[T]**
Fallo de servicios de comunicaciones	50	**100**				
Suplantación de la identidad del usuario	25	**100**	**100**	**100**		
Abuso de privilegios de acceso	25	**100**	**100**	**100**		
Uso no previsto	25	**100**	**100**	**100**		

Red de Área Local						
AMENAZA	**FRECUENCIA**	**DIMENSIONES %**				
		[D]	**[I]**	**[C]**	**[A]**	**[T]**
Fallo de servicios de comunicaciones	50	**100**				
Errores del administrador	50	**100**	**100**	**100**		
Fugas de información	25	**100**				
Caída del sistema por agotamiento de recursos	25	**100**				
Suplantación de la identidad del usuario	25	**100**	**100**	**100**		
Uso no previsto	25	**100**	**100**			

Conectividad Inalámbrica						
AMENAZA	**FRECUENCIA**	**DIMENSIONES %**				
		[D]	**[I]**	**[C]**	**[A]**	**[T]**
Avería de origen físico o lógico	25	**100**				
Fallo de servicios de comunicaciones	50	**100**				
Emanaciones electromagnéticas	25			**100**		
Fugas de información	25			**100**		
Caída del sistema por agotamiento de recursos	25	**100**				
Suplantación de la identidad del usuario	25	**100**	**100**	**100**		
Abuso de privilegios de acceso	25	**100**	**100**	**100**		
Uso no previsto	25	**100**	**100**	**100**		

EQUIPO AUXILIAR

Fibra Óptica						
AMENAZA	**FRECUENCIA**	**DIMENSIONES %**				
		[D]	**[I]**	**[C]**	**[A]**	**[T]**
Fuego	1	**100**				
Daños por agua	1	**100**				
Desastres naturales	25	**100**				
Avería de origen físico o lógico	25	**100**				
Corte del suministro eléctrico	50	**100**				
Condiciones inadecuadas de temperatura o humedad	25	**100**				
Fallo de servicios de comunicaciones	25	**100**				
Caída del sistema por agotamiento de recursos	25	**100**				

Rack						
AMENAZA	**FRECUENCIA**	**DIMENSIONES %**				
		[D]	**[I]**	**[C]**	**[A]**	**[T]**
Fuego	25	**100**				
Daños por agua	25	**100**				
Desastres naturales	25	**100**				
Corte del suministro eléctrico	25	**100**				
Condiciones inadecuadas de temperatura o humedad	25	**100**				
Emanaciones electromagnéticas	25			**100**		

Fuente de Alimentación (RED eléctrica)						
AMENAZA	**FRECUENCIA**	**DIMENSIONES %**				
		[D]	**[I]**	**[C]**	**[A]**	**[T]**
Fuego	1	**100**				
Daños por agua	25	**100**				
Desastres naturales	25	**100**				
Avería de origen físico o lógico	25	**100**				
Corte del suministro eléctrico	50	**100**				
Condiciones inadecuadas de temperatura o humedad	25	**100**				

Sistema de Alimentación Ininterrumpida						
AMENAZA	**FRECUENCIA**	**DIMENSIONES %**				
		[D]	**[I]**	**[C]**	**[A]**	**[T]**
Fuego	1	**100**				
Daños por agua	25	**100**				
Desastres naturales	25	**100**				
Avería de origen físico o lógico	25	**100**				
Corte del suministro eléctrico	50	**100**				
Condiciones inadecuadas de temperatura o humedad	25	**100**				
Caída del sistema por agotamiento de recursos	25	**100**				

Cableado Eléctrico						
AMENAZA	**FRECUENCIA**	**DIMENSIONES %**				
		[D]	**[I]**	**[C]**	**[A]**	**[T]**
Fuego	1	**100**				
Daños por agua	25	**100**				
Desastres naturales	25	**100**				
Condiciones inadecuadas de temperatura o humedad	25	**100**				

Cableado Estructurado						
AMENAZA	**FRECUENCIA**	**DIMENSIONES %**				
		[D]	**[I]**	**[C]**	**[A]**	**[T]**
Fuego	1	**100**				
Daños por agua	50	**100**				
Desastres naturales	25	**100**				
Condiciones inadecuadas de temperatura o humedad	25	**100**				

INSTALACIONES

Oficina de Sistemas de Información y Telemática						
AMENAZA	**FRECUENCIA**	**DIMENSIONES %**				
		[D]	**[I]**	**[C]**	**[A]**	**[T]**
Fuego	1	**100**				
Daños por agua	50	**100**				

Desastres naturales	25	**100**				
Corte del suministro eléctrico	50	**100**				
Condiciones inadecuadas de temperatura o humedad	25	**100**				
Emanaciones electromagnéticas	25			**100**		
Destrucción de información	25	**100**				
Fugas de información	25			**100**		

PERSONAL

Administrador de Sistema						
AMENAZA	**FRECUENCIA**	**DIMENSIONES %**				
		[D]	**[I]**	**[C]**	**[A]**	**[T]**
Deficiencias en la organización	25	**100**				
Fugas de información	25			**100**		
Indisponibilidad del personal	25	**100**				
Abuso de privilegios de acceso	25	**100**	**100**	**100**		
Uso no previsto		**100**	**100**	**100**		

Administrador de red de datos						
AMENAZA	**FRECUENCIA**	**DIMENSIONES %**				
		[D]	**[I]**	**[C]**	**[A]**	**[T]**
Deficiencias en la organización	25	**100**				
Fugas de información	25			**100**		
Indisponibilidad del personal	25	**100**				
Abuso de privilegios de acceso	25	**100**	**100**	**100**		
Uso no previsto	25	**100**	**100**	**100**		

Administrador de Bases de Datos						
AMENAZA	**FRECUENCIA**	**DIMENSIONES %**				
		[D]	**[I]**	**[C]**	**[A]**	**[T]**
Deficiencias en la organización	25	**100**				
Fugas de información	25			**100**		
Indisponibilidad del personal	25	**100**				
Abuso de privilegios de acceso	25	**100**	**100**	**100**		
Uso no previsto	25	**100**	**100**	**100**		

Desarrolladores de Software						
AMENAZA	**FRECUENCIA**	**DIMENSIONES %**				
		[D]	**[I]**	**[C]**	**[A]**	**[T]**
Avería de origen físico o lógico	50	**100**				
Fugas de información	25			**100**		
Vulnerabilidades de los programas (software)	25	**100**	**100**	**100**		
Errores de mantenimiento / actualización de programas (software)	50	**100**	**100**			
Suplantación de la identidad del usuario	25	**100**	**100**	**100**		
Abuso de privilegios de acceso	25	**100**	**100**	**100**		
Uso no previsto	25	**100**	**100**	**100**		

Fuente: Autor

7.4.3 Estimación del riesgo potencial

Se denomina impacto a la medida del daño sobre un activo derivado de la materialización de una amenaza. Luego de conocer el valor de los activos (en varias dimensiones) y la degradación de causan las amenazas, se puede definir el impacto que estas tendrán sobre cada uno de ellos.

GRUPO DE AMENAZAS	SIMBOLOGÍA
Desastres naturales	[N]
De origen industrial	[I]
Errores y fallos no intencionados	[E]
Ataques intencionados	[A]

DATOS/INFORMACIÓN

Tabla 31 - Estimación del riesgo potencial

DESCRIPCIÓN	IMPACTO	AMENAZA	RIESGO
Copias de Seguridad de los Sistemas de Información	MA	[E] [A]	MA
Contratos	MA	[E] [A]	A
Historial Laboral	MA	[E] [A]	A
Registros de Actividad	MA	[E] [A]	MA
Códigos Fuentes	MA	[E] [A]	MA

SERVICIOS

DESCRIPCIÓN	IMPACTO	AMENAZA	RIESGO
Correo Electrónico	MA	[E] [A]	A
Gestión de Identidades	MA	[E] [A]	MA
Servicios Internos	MA	[E] [A]	A
Páginas web de acceso público	A	[E] [A]	A

SOFTWARE

DESCRIPCIÓN	IMPACTO	AMENAZA	RIESGO
Software Estándar	MA	[E] [A]	A
Gestores de Bases de Datos	MA	[E] [A]	MA
Ofimática	B	[E] [A]	B
Software de Antivirus	A	[E] [A]	A
Sistemas Operativos	M	[E] [A]	M

HARDWARE

DESCRIPCIÓN	IMPACTO	AMENAZA	RIESGO
Dispositivos de Respaldo	MA	[I] [E] [A]	MA
Firewall	MA	[I] [E] [A]	MA
Antenas	MA	[I] [E] [A]	A
Servidores	MA	[I] [E] [A]	MA
Computadoras Portátiles de Uso Institucional	B	[I] [E] [A]	B
Computadoras de Escritorio de Uso Institucional	B	[I] [E] [A]	B
Impresoras	MB	[I] [E] [A]	MB
Router	A	[I] [E] [A]	A
Escáner	B	[I] [E] [A]	B
Switch	A	[I] [E] [A]	A
Puntos de Acceso Inalámbricos	B	[I] [E] [A]	B

COMUNICACIONES

DESCRIPCIÓN	IMPACTO	AMENAZA	RIESGO
Internet	A	[I] [E] [A]	A
Red de Área Local	MA	[I] [E] [A]	MA
Conectividad Inalámbrica	B	[I] [E] [A]	B

QUIPO AUXILIAR

DESCRIPCIÓN	IMPACTO	AMENAZA	RIESGO
Fibra Óptica	MA	[I] [E] [A]	A
Rack	A	[I] [E] [A]	A
Fuente de Alimentación (RED eléctrica)	MA	[I] [E] [A]	MA
Sistema de Alimentación Ininterrumpida	A	[I] [E] [A]	A
Cableado Eléctrico	MA	[I] [E] [A]	MA
Cableado Estructurado	A	[I] [E] [A]	A

INSTALACIONES

DESCRIPCIÓN	IMPACTO	AMENAZA	RIESGO
Oficina de Sistemas de Información y Telemática	MA	[I] [E] [A]	MA

PERSONAL

DESCRIPCIÓN	IMPACTO	AMENAZA	RIESGO
Administrador de Sistema	MA	[E] [A]	M
Administrador de red de datos	MA	[E] [A]	M
Administrador de Bases de Datos	MA	[E] [A]	M
Desarrolladores de Software	A	[E] [A]	M

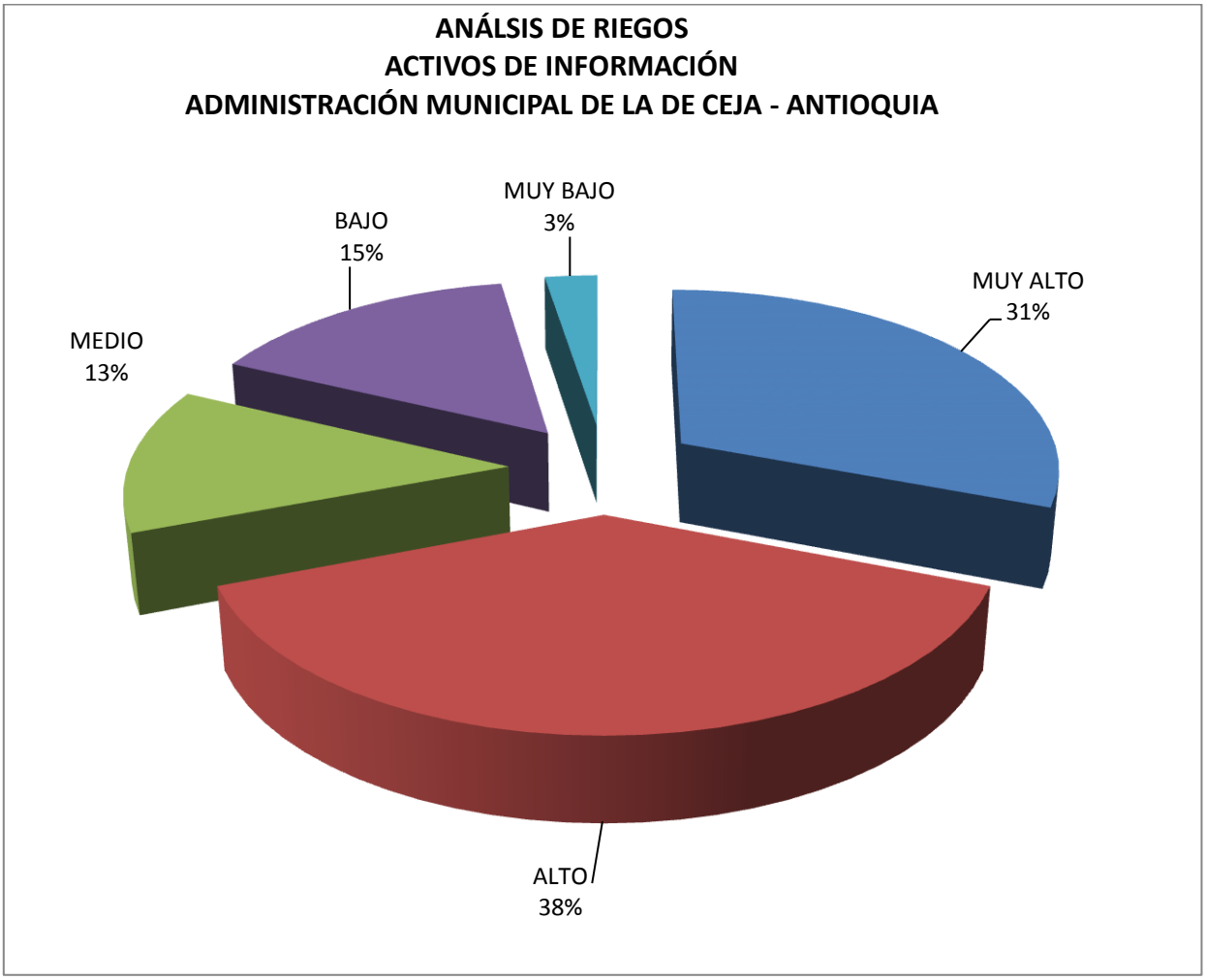
Fuente: Autor

Tabla 32 - Tabla resumen RIEGOS

RIESGO	CANTIDAD DE ACTIVOS x NIVEL DE RIEGOS
MUY ALTO	12
ALTO	16
MEDIO	5
BAJO	6
MUY BAJO	1

Fuente: Autor

Ilustración 27 – Gráfico. Análisis del IMPACTO de los riegos en los activos de la entidad



Fuente: Autor

Análisis

De acuerdo al grafico anterior podemos definir lo siguiente:

- La mayoría de riegos de los activos de información a los cuales se les está realizando el análisis se encuentran ubicados en una zona de ALTO IMPACTO para la entidad, por ello es necesario tomar decisiones y establecer las estrategias que permitan la mitigación de los mismos.
- La evaluación de los riegos nos permite determinar que estos activos en cuanto a sus dimensiones de confiablidad, integridad y disponibilidad tendrán que reducirse, evitarse o transferirse.
- Se identificaron activos críticos como lo son las copia de seguridad, los códigos fuente de la aplicaciones que en la actualidad se tercerizan, las red de datos interna, las instalaciones del centro de cómputo, el registro de actividades, el gestor de bases de datos, la red eléctrica, las UPS entre otros son activos que son sucesibles a una gran cantidad de amenazas y que la materialización de alguna de ellas puede causar grandes impactos a la entidad, es por ello adoptar mecanismo de protección que permitan preservar las características básicas de la información en cuanto a sus dimensiones de confiablidad, integridad y disponibilidad.

7.5 DECLARACIÓN DE APLICABILIDAD (SOA)

SoA se trata de un documento que enlista los controles de seguridad establecidos en el Anexo A del estándar ISO/IEC 27001 (un conjunto de 114 controles agrupados en 35 objetivos de control, en la versión de 2013 de esta norma de seguridad). ("¿Qué es una Declaración de Aplicabilidad (SoA) y para qué sirve?," n.d.)

Tabla 33 - Declaración de aplicabilidad (SOA)

Dominio o descripción	Evidencia o registro de implementación	
Políticas de seguridad	Aplica	
Implementación y revisión periódica de la política de seguridad de la información.	Si	Documento de la política firmado por la alta dirección y actas de revisión periódica de la misma.
Organización de la seguridad de la Información	SI	
Compromiso y asignación de responsabilidades	Si	Documento con la asignación de responsabilidades y actas de comité
Gestión de activos	Si	
Gestión de los activos (inventario, asignación, clasificación, etiquetado.	Si	Documento con el inventario actualizado y gestionado.

Seguridad de los recursos humanos	Si	
Determinación de los roles y responsabilidades	Si	Documento escrito donde se determines los roles y responsabilidades referentes a seguridad de la información de las personas que hacen parte de la entidad.
Seguridad física y ambiental	Si	
Aplicación de la seguridad física y perimetral de la entidad	Si	Implementación de medidas físicas y procedimentales.
Control de acceso	Si	
Aplicación de la Política de control de acceso	Si	Documento de política firmado por la alta dirección
Desarrollo seguro de aplicaciones por partes de la entidad	Si	
Desarrollo seguro de aplicaciones por parte de la entidad bajo estándares de confidencialidad e integridad de los datos.	Si	Documento con las requisitos mínimos para el desarrollo de aplicaciones seguras por parte de la entidad.
Gestión de incidentes de seguridad de la información	Si	
Reporte sobre los eventos de seguridad de la información	Si	Documentos que permitan determinar los incidentes sobre la seguridad de la información y su gestión.
Gestión de la continuidad del negocio	Si	
Determinación de los planes de continuidad del negocio ante una eventualidad.	Si	Documento detallado donde se especifiquen cada uno de los procedimientos que permitan determinar la continuidad del negocio.
Cumplimiento	Si	
Verificación de la legislación aplicable y su nivel de cumplimento en la entidad.	Si	Documento con las normas/leyes que aplican al SGSI

Fuente: Autor

7.6 PLAN DE TRATAMIENTO DE RIESGOS

Existen varias opciones de tratamiento, aunque de manera general se pueden agrupar en las siguientes categorías:

- **Mitigar**. Consiste en implementar algún control que reduzca el riesgo.
- **Transferir**. Ocurre cuando se delega la acción de mitigación a un tercero.
- **Aceptar**. Se presenta cuando el impacto generado por un riesgo es suficientemente bajo para que la organización decida no tomar ninguna acción de mitigación o cuando el costo de la aplicación de un control supera el valor el activo.

Este proceso es fundamental, para lleva a cabo un SGSI, ya que implica llevar lo que está en la teoría a la práctica. El propósito fundamental del plan de tratamiento de riegos de seguridad de la información debe indicar de forma exacta:

- ¿Quién va a implementar cada control?
- ¿Cuándo?
- ¿Con que presupuesto cuenta?

Luego de que se ha escrito este documento es crucial que se obtenga la aprobación de la dirección de la entidad, ya que lleva tiempo y esfuerzo poder implementar todos los controles o salvaguardas a los activos anteriormente descritos.

Con el objetivo de alcanzar los objetivos de seguridad del Sistema de Gestión de la Seguridad de la Información, se establecen los siguientes controles de seguridad basados en la metodología de análisis y evaluación de riesgos MAGERIT y los controles del Anexo A del estándar ISO/IEC 27001:2013.

*CONTROLES TOMADOS DE LA GUÍA Nro. 8 MIN TIC (Controles de Seguridad y Privacidad de la Información)

DATOS/INFORMACIÓN

Tabla 34 – Plan de tratamiento de riegos.

DESCRIPCIÓN	CATEGORÍA DE SALVAGUARDA	TIPO DE SALVAGUARDA	RAZÓN	*CONTROLES	RESPONSABLE
Copias de Seguridad de los Sistemas de Información	Protección de los soportes de información	[PR] Preventivas [CR] Correctivas	• Copias de seguridad de los datos (backup) • Aseguramiento de la disponibilidad	• Se deberían hacer copias de respaldo de la información, del software e imágenes de los sistemas, y ponerlas a prueba regularmente de acuerdo con una política de copias de respaldo aceptada.	• OFICINA DE SISTEMAS
Contratos	Protección de los datos / información	[PR] Preventivas [AD] administrativas	• Protección de la Información • Aseguramiento de la integridad	• Las instalaciones y la información de registro se deberían proteger contra alteración y acceso no autorizado.	• LÍDER DE CONTRATACIÓN • CONTROL INTERNO
Historial Laboral	Protección de los datos / información	[PR] Preventivas [AD] administrativas	• Protección de la Información • Aseguramiento de la integridad	• Las instalaciones y la información de registro se deberían proteger contra alteración y acceso no autorizado.	• GESTIÓN HUMANA
Registros de Actividad	Protección de los datos / información	[PR] Preventivas [AD] administrativas [MN] de monitorización	• Protección de la Información • Aseguramiento de la integridad	• Se deberían elaborar, conservar y revisar regularmente los registros acerca de actividades del usuario, excepciones, fallas y eventos de seguridad de la información	• OFICINA DE SISTEMAS
Códigos Fuentes	Protección de las aplicaciones (software)	[PR] Preventivas	• Protección de la Información • Cambios (actualizaciones y mantenimiento)	• La organización debería supervisar y hacer seguimiento de la actividad de desarrollo	• OFICINA DE SISTEMAS

				de sistemas contratados externamente. • Se deberían 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.	

SERVICIOS

DESCRIPCIÓN	CATEGORÍA DE SALVAGUARDA	TIPO DE SALVAGUARDA	RAZÓN	*CONTROLES	RESPONSABLE
Correo Electrónico	Protección de los soportes de información	[PR] Preventivas [AW] de concienciación [DC] de detección [MN] de monitorización	• Copias de seguridad de los datos (backup) • Aseguramiento de la disponibilidad • Protección del correo electrónico	• Se debería proteger adecuadamente la información incluida en la mensajería electrónica.	• OFICINA DE SISTEMAS • COMUNICACIONES
Gestión de Identidades	Protección de los datos / información	[PR] Preventivas [AD] administrativas [DC] de detección [CR] Correctivas	• Protección de la Información • Aseguramiento de la integridad	• Se debería establecer, documentar y revisar una política de control de acceso con base en los requisitos del negocio y de seguridad de la información. • Se debería implementar un proceso formal de	• OFICINA DE SISTEMAS

				registro y de cancelación de registro de usuarios, para posibilitar la asignación de los derechos de acceso. • Se debería implementar un proceso de suministro de acceso formal de usuarios para asignar o revocar los derechos de acceso a todo tipo de usuarios para todos los sistemas y servicios. • Se debería restringir y controlar la asignación y uso de derechos de acceso privilegiado. • La asignación de la información secreta se debería controlar por medio de un proceso de gestión formal. • Los derechos de acceso de todos los empleados y de usuarios externos a la información y a las instalaciones de procesamiento de información se deberían retirar al terminar su empleo, contrato o acuerdo, o se deberían ajustar cuando se hagan cambios	
Servicios Internos	• Protección de los datos / información • Protección de los servicios	[PR] Preventivas [AD] administrativas [AW] de concienciación [DC] de detección [CR] Correctivas	• Protección de la Información • Aseguramiento de la integridad	• Se debería definir un conjunto de políticas para la seguridad de la información, aprobada por la dirección, publicada y comunicada a los	• OFICINA DE SISTEMAS

				empleados y partes externas pertinentes.	
Páginas web de acceso público	• Protección de los datos / información • Protección de los servicios	[PR] Preventivas [AD] administrativas [AW] de concienciación [MN] de monitorización	• Protección de la Información • Aseguramiento de la integridad	• La información involucrada en los servicios de aplicaciones que pasan sobre redes públicas se debería proteger de actividades fraudulentas, disputas contractuales y divulgación y modificación no autorizadas	• OFICINA DE SISTEMAS • COMUNICACIONES • GOBIERNO EN LÍNEA

SOFTWARE

DESCRIPCIÓN	CATEGORÍA DE SALVAGUARDA	TIPO DE SALVAGUARDA	RAZÓN	*CONTROLES	RESPONSABLE
Software Estándar	Protección de los soportes de información Adquisición y desarrollo	[PR] Preventivas	• Copias de seguridad de los datos (backup) • Aseguramiento de la disponibilidad	• Se deberían establecer e implementar las reglas para la instalación de software por parte de los usuarios. • La información involucrada en las transacciones de los servicios de las aplicaciones se debería proteger para evitar la transmisión incompleta, el enrutamiento errado, la alteración no autorizada de mensajes, la divulgación no autorizada, y la duplicación o reproducción de mensajes no autorizada	• OFICINA DE SISTEMAS
Gestores de Bases de Datos	Protección de los datos / información	[PR] Preventivas [AD] administrativas	• Protección de la Información • Aseguramiento de la	• La información se debería clasificar en función de los requisitos legales, valor,	• OFICINA DE SISTEMAS

			integridad	criticidad y susceptibilidad a divulgación o a modificación no autorizada.	
Ofimática	Protección de los datos / información	[PR] Preventivas [AD] administrativas	• Protección de la Información • Aseguramiento de la integridad	• Evitar el acceso no autorizado a sistemas y aplicaciones. • Se debería restringir y controlar estrictamente el uso de programas utilitarios que pudieran tener capacidad de anular el sistema y los controles de las aplicaciones.	• OFICINA DE SISTEMAS
Software de Antivirus	Protección de los datos / información	[PR] Preventivas [AD] administrativas [DC] de detección [CR] Correctivas [MN] de monitorización	• Protección de la Información • Aseguramiento de la integridad	• Se deberían implementar controles de detección, de prevención y de recuperación, combinados con la toma de conciencia apropiada de los usuarios, para proteger contra códigos maliciosos	• OFICINA DE SISTEMAS
Sistemas Operativos	Protección de los datos / información	[PR] Preventivas	• Protección de la Información	• Se deberían implementar procedimientos para controlar la instalación de software en sistemas operativos.	• OFICINA DE SISTEMAS

HARDWARE

DESCRIPCIÓN	CATEGORÍA DE SALVAGUARDA	TIPO DE SALVAGUARDA	RAZÓN	*CONTROLES	RESPONSABLE
Dispositivos de Respaldo	Protección de los soportes de información Protección de los equipos (hardware)	[PR] Preventivas [CR] Correctivas	• Copias de seguridad de los datos (backup) • Aseguramiento de la disponibilidad	• Se deberían hacer copias de respaldo de la información, del software e imágenes de los sistemas, y ponerlas a prueba regularmente de acuerdo con una política	• OFICINA DE SISTEMAS

				de copias de respaldo aceptada	
Firewall	Protección de los equipos (hardware) Protección en los puntos de interconexión con otros sistemas	[PR] Preventivas [AD] administrativas [DC] de detección [MN] de monitorización	• Protección de la Información • Aseguramiento de la integridad • Aseguramiento de la disponibilidad	• Se debería establecer, documentar y revisar una política de control de acceso con base en los requisitos del negocio y de seguridad de la información. • Solo se debería permitir acceso de los usuarios a la red y a los servicios de red para los que hayan sido autorizados específicamente. • Se debería restringir y controlar la asignación y uso de derechos de acceso privilegiado	•
Antenas	Protección de los equipos (hardware)	[PR] Preventivas [AD] administrativas	• Protección de la Información • Aseguramiento de la integridad • Aseguramiento de la disponibilidad	• Mantener la seguridad de la información transferida dentro de una organización y con cualquier entidad externa.	• OFICINA DE SISTEMAS
Servidores	Protección de los equipos (hardware)	[PR] Preventivas [AD] administrativas [CR] Correctivas [MN] de monitorización	• Protección de la Información • Aseguramiento de la integridad • Aseguramiento de la disponibilidad	• Los equipos se deberían proteger contra fallas de energía y otras interrupciones causadas por fallas en los servicios de suministro. • Se debería establecer, documentar y revisar una política de control de acceso con base en los requisitos del negocio y de seguridad de la información.	• OFICINA DE SISTEMAS

				• Se deberían definir y usar perímetros de seguridad, y usarlos para proteger áreas que contengan información sensible o critica, e instalaciones de manejo de información. • Las áreas seguras se deberían proteger mediante controles de entrada apropiados para asegurar que solamente se permite el acceso a personal autorizado. • Los equipos se deberían mantener correctamente para asegurar su disponibilidad e integridad continuas. • Se debería diseñar y aplicar protección física contra desastres naturales, ataques maliciosos o accidentes.	
Computadoras Portátiles de Uso Institucional	Protección de los equipos (hardware)	[PR] Preventivas	• Se aplican perfiles de seguridad	• Prevenir la perdida, daño, robo o compromiso de activos, y la interrupción de las operaciones de la organización. • Los equipos se deberían mantener correctamente para asegurar su disponibilidad e integridad continuas. • Los equipos, información o software no se deberían retirar de su sitio sin autorización previa. • Se deberían aplicar medidas de seguridad a	• OFICINA DE SISTEMAS • OFICINA DE BIENES

				los activos que se encuentran fuera de las instalaciones de la organización, teniendo en cuenta los diferentes riesgos de trabajar fuera de dichas instalaciones.	
Computadoras de Escritorio de Uso Institucional	Protección de los equipos (hardware)	[PR] Preventivas	• Se aplican perfiles de seguridad	• Prevenir la perdida, daño, robo o compromiso de activos, y la interrupción de las operaciones de la organización. • Los equipos se deberían proteger contra fallas de energía y otras interrupciones causadas por fallas en los servicios de suministro. • Los equipos se deberían mantener correctamente para asegurar su disponibilidad e integridad continuas • Se debería adoptar una política de escritorio limpio para los papeles y medios de almacenamiento removibles, y una política de pantalla limpia en las instalaciones de procesamiento de información	• OFICINA DE SISTEMAS • OFICINA DE BIENES
Impresoras	Protección de los equipos (hardware)	[PR] Preventivas	• Aseguramiento de la disponibilidad	• Los equipos se deberían mantener correctamente para asegurar su disponibilidad e integridad continuas	• OFICINA DE SISTEMAS • OFICINA DE BIENES

Router	Protección de los equipos (hardware)	[PR] Preventivas	• Se aplican perfiles de seguridad. • Aseguramiento de la disponibilidad	• Los equipos deberían estar ubicados y protegidos para • reducir los riesgos de amenazas y peligros del entorno, y las • oportunidades para acceso no autorizado.	• OFICINA DE SISTEMAS • OFICINA DE BIENES
Escáner	Protección de los equipos (hardware)	[PR] Preventivas	• Aseguramiento de la disponibilidad	• Los equipos se deberían mantener correctamente para asegurar su disponibilidad e integridad continuas	• OFICINA DE SISTEMAS • OFICINA DE BIENES
Switch	Protección de los equipos (hardware)	[PR] Preventivas	• Aseguramiento de la disponibilidad	• Los equipos se deberían mantener correctamente para asegurar su disponibilidad e integridad continuas. • Los equipos se deberían proteger contra fallas de energía y otras interrupciones causadas por fallas en los servicios de suministro	• OFICINA DE SISTEMAS • OFICINA DE BIENES
Puntos de Acceso Inalámbricos	Protección de los equipos (hardware) Protección de las comunicaciones	[PR] Preventivas	• Se aplican perfiles de seguridad	• Los equipos deberían estar ubicados y protegidos para reducir los riesgos de amenazas y peligros del entorno, y las oportunidades para acceso no autorizado.	• OFICINA DE SISTEMAS

COMUNICACIONES

DESCRIPCIÓN	CATEGORÍA DE SALVAGUARDA	TIPO DE SALVAGUARDA	RAZÓN	*CONTROLES	RESPONSABLE
Internet	Protección de los datos / información	[PR] Preventivas	• Copias de seguridad de los datos (backup) • Aseguramiento de la disponibilidad	• Se debería implementar un proceso de suministro de acceso formal de usuarios para asignar o revocar los derechos de acceso a todo tipo de usuarios para todos los sistemas y servicios.	• OFICINA DE SISTEMA
Red de Área Local	Protección de los datos / información Protección de los equipos (hardware)	[PR] Preventivas [DC] de detección [CR] Correctivas	• Protección de la Información • Aseguramiento de la disponibilidad	• Las redes se deberían gestionar y controlar para proteger la información en sistemas y aplicaciones. • Se deberían 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 servicios de red, ya sea que los servicios se presten internamente o se contraten externamente	• OFICINA DE SISTEMA
Conectividad Inalámbrica	Protección de los datos / información	[PR] Preventivas	• Protección de la Información • Aseguramiento de la disponibilidad	• Los equipos deberían estar ubicados y protegidos para • reducir los riesgos de amenazas y peligros del entorno, y las • oportunidades para acceso no autorizado. • Se debería contar con políticas, procedimientos y controles de transferencia formales	• OFICINA DE SISTEMA

				para proteger la transferencia de información mediante el uso de todo tipo de instalaciones de comunicación	

EQUIPO AUXILIAR

DESCRIPCIÓN	CATEGORÍA DE SALVAGUARDA	TIPO DE SALVAGUARDA	RAZÓN	*CONTROLES	RESPONSABLE
Fibra Óptica	Protección de los soportes de información Protección de las comunicaciones	[PR] Preventivas	• Copias de seguridad de los datos (backup) • Aseguramiento de la disponibilidad	• Las redes se deberían gestionar y controlar para proteger la información en sistemas y aplicaciones. • Los equipos se deberían proteger contra fallas de energía y otras interrupciones causadas por fallas en los servicios de suministro	• OFICINA DE SISTEMA • PROVEEDOR DE SERVICIOS DE INTERNET
Rack	Protección de los equipos (hardware)	[PR] Preventivas [AD] administrativas	• Protección de la Información	• Se debería establecer, documentar y revisar una política de control de acceso con base en los requisitos del negocio y de seguridad de la información. • Se debería diseñar y aplicar protección física contra desastres naturales, ataques maliciosos o accidentes. • Los equipos se deberían proteger contra fallas de energía y otras	• OFICINA DE SISTEMA

				interrupciones causadas por fallas en los servicios de suministro	
Fuente de Alimentación (RED eléctrica)	Protección de los equipos (hardware)	[PR] Preventivas	• Protección de la Información • Aseguramiento de la integridad • Aseguramiento de la disponibilidad	• Los equipos se deberían mantener correctamente para asegurar su disponibilidad e integridad continuas. • Los equipos se deberían proteger contra fallas de energía y otras interrupciones causadas por fallas en los servicios de suministro	• OFICINA DE SISTEMA
Sistema de Alimentación Ininterrumpida	Protección de los equipos (hardware)	[PR] Preventivas [AD] administrativas	• Protección de la Información • Aseguramiento de la integridad • Aseguramiento de la disponibilidad	• Los equipos se deberían mantener correctamente para asegurar su disponibilidad e integridad continuas. • Los equipos se deberían proteger contra fallas de energía y otras interrupciones causadas por fallas en los servicios de suministro	• OFICINA DE SISTEMA
Cableado Eléctrico	Protección de los equipos (hardware)	[PR] Preventivas	• Aseguramiento de la disponibilidad	• • Los equipos se deberían mantener correctamente para asegurar su disponibilidad e integridad continuas. • El cableado de potencia y de telecomunicaciones que porta datos o soporta servicios de información debería estar protegido contra interceptación, interferencia o daño.	• OFICINA DE SISTEMA

Cableado Estructurado	Protección de los equipos (hardware)	[PR] Preventivas	• Segregación de las redes en dominios	• El cableado de potencia y de telecomunicaciones que porta datos o soporta servicios de información debería estar protegido contra interceptación, interferencia o daño.	• OFICINA DE SISTEMA

INSTALACIONES

DESCRIPCIÓN	CATEGORÍA DE SALVAGUARDA	TIPO DE SALVAGUARDA	RAZÓN	*CONTROLES	RESPONSABLE
Oficina de Sistemas de Información y Telemática	Seguridad física – Protección de las instalaciones	[PR] Preventivas [DC] de detección [CR] Correctivas	• Copias de seguridad de los datos (backup) • Aseguramiento de la disponibilidad • Se aplican perfiles de seguridad •	• Se deberían definir y usar perímetros de seguridad, y usarlos • para proteger áreas que contengan información sensible o critica, e • instalaciones de manejo de información. • Se debería diseñar y aplicar seguridad física a oficinas, • recintos e instalaciones.	• OFICINA DE SISTEMA

PERSONAL

DESCRIPCIÓN	CATEGORÍA DE SALVAGUARDA	TIPO DE SALVAGUARDA	RAZÓN		
Administrador de Sistema	Salvaguardas relativas al personal	[PR] Preventivas [AD] administrativas	• Copias de seguridad de los datos (backup) • Aseguramiento de la disponibilidad	• Se deberían controlar los cambios en la organización, en los procesos de negocio, en las instalaciones y en los sistemas de procesamiento de información que afectan la	• OFICINA DE SISTEMA

				seguridad de la información.	
Administrador de red de datos	Salvaguardas relativas al personal	[PR] Preventivas [AD] administrativas	• Protección de la Información • Aseguramiento de la integridad	• Se debería obtener oportunamente información acerca de las vulnerabilidades técnicas de los sistemas de información que se usen; evaluar la exposición de la organización a estas vulnerabilidades, y tomar las medidas apropiadas para tratar el riesgo asociado. • Los grupos de servicios de información, usuarios y sistemas de información se deberían separar en las redes	• OFICINA DE SISTEMA
Administrador de Bases de Datos	Salvaguardas relativas al personal	[PR] Preventivas [AD] administrativas	• Protección de la Información • Aseguramiento de la integridad	• Se debería exigir a los usuarios que cumplan las prácticas de la organización para el uso de información de autenticación secreta. • Se deberían hacer copias de respaldo de la información, del software e imágenes de los sistemas, y ponerlas a prueba regularmente de acuerdo con una política de copias de respaldo aceptada.	• OFICINA DE SISTEMA
Desarrolladores de Software	Protección de las aplicaciones (software) Adquisición y desarrollo	[PR] Preventivas [AD] administrativas	• Protección de la Información • Aseguramiento de la integridad	• Se deberían establecer y aplicar reglas para el desarrollo de software y de sistemas, a los desarrollos que se dan	• OFICINA DE SISTEMA

			• Cambios (actualizaciones y mantenimiento)	dentro de la organización. • Los cambios a los sistemas dentro del ciclo de vida de desarrollo se deberían controlar mediante el uso de procedimientos formales de control de cambios. • La organización debería supervisar y hacer seguimiento de la actividad de desarrollo de sistemas contratados externamente. • Se deberían 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.	

Fuente: Autor – NTC 27001:2013

7.7 PLAN DE CONTINUIDAD DEL NEGOCIO

Ilustración 28 -Plan de continuidad del negocio.

Fuente: http://www.banrep.gov.co/sites/default/files/paginas/gestion_continuidad.JPG

La norma ISO 27001 ofrece herramientas que tienen el objetivo de facilitar la implementación de los planes de contingencia y de continuidad en las empresas, existen diferentes pasos a seguir si se produce un incidente de seguridad:

El objetivo del Plan de continuidad del negocio es definir de forma precisa cómo la organización gestionará los incidentes en caso de un desastre o de otra interrupción del negocio y cómo recuperará sus actividades críticas dentro de plazos establecidos.

El plan para la aplicación del plan de continuidad del negocio tendrá las siguientes fases:

- Plan de recuperación ante desastres
- Plan de respuesta a los incidentes
- Registro de incidentes
- Lista de ubicaciones para continuidad del negocio
- Plan de transporte
- Contactos clave
- Plan de recuperación de actividad
- Plan de prueba y verificación
- Formulario – Informe de prueba y verificación

El plan de continuidad del negocio requiere de una estructura organizacional, encargada de promover el desarrollo de los lineamientos definidos en cuanto al plan, es por ello que se definirá los integrantes del comité, sus roles y responsabilidades

Tabla 35 - Roles integrantes del comité de continuidad del negocio

INTEGRANTES	ROLES	RESPONSABILIDADES
• Jefe de oficia de sistemas	• Director de continuidad • Jefe de riesgos • Líder de administración y recuperación de infraestructura física • Líder de Recuperación tecnológica	• Delegar responsabilidades dentro del comité para actualizar, mantener y probar el plan de continuidad. • Evaluar y probar los recursos requeridos para establecer y mantener la estrategia de recuperación y contingencia de la entidad. • Liderar las reuniones del comité. • Advertir sobre nuevos riesgos que afecten la continuidad de la operación normal de la entidad y que ponen al descubierto debilidades del plan de continuidad. • Monitorear los reportes sobre el estado de recuperación o evaluación durante una contingencia. • Velar por la seguridad del apersonas que actúan en la solución de una eventualidad. • Realizar las investigaciones necesarias y tomar medidas preventivas ante la materialización de una amenaza. • Liderar la recuperación tecnológica ante una eventualidad. • Identificar los posibles riesgos de aspectos tecnológicos que afectan la continuidad de la operación normal de la Entidad y que ponen al descubierto debilidades del plan de continuidad.

• Técnicos de apoyo Oficina de sistemas	• Tares de apoyo (Mantenimiento preventivo y correctivo	• Ejecutar los planes de contingencia ante el incidente presentado. • Identificar los posibles riesgos que afectan la continuidad de la operación normal de la Entidad y que ponen al descubierto debilidades del plan de continuidad. • Mantener comunicación constante durante el estado de contingencia. • Realizar las actividades que le sean asignadas durante la declaración de contingencia.
• Jefe de control interno • Jefe de Gestión humana	• Tareas de apoyo y cumplimento	• Mantener comunicación constante durante el estado de contingencia. • Realizar las actividades que le sean asignadas durante la declaración de contingencia. • Advertir sobre riesgos que puedan afectar la continuidad en la prestación del servicio o la funcionalidad del plan. • Verificar que la eventualidad que se presente no tenga efectos en la normatividad vigente.
• Jefe de comunicaciones	• Tareas de comunicaciones	• Asesora en la comunicación tanto interna como externa del evento de interrupción.

7.7.1 Análisis del impacto al negocio (BIA)

En el BIA se identifican los componentes claves requeridos para continuar con las operaciones de negocio luego de un incidente. A continuación relacionamos algunos de ellos.[13]

- Personal requerido
- Área de trabajo
- Registros vitales- Backus de información
- Aplicativos críticos
- Dependencias de otras áreas.
- Criticidad de los recursos de información.
- Participación del personal de seguridad informática y los usuarios finales
- Análisis de todos los tipos de recursos de información.

[13] https://es.wikipedia.org/wiki/Plan_de_continuidad_del_negocio

Una estrategia de recuperación en una combinación de medidas preventivas, defectivas y correctivas para:

- Eliminar la amenazas completamente
- Minimizar la probabilidad de que ocurra
- Minimizar el efecto

8 CRONOGRAMA

Tabla 36 - Cronograma del proyecto

Nro.	ACTIVIDAD	DESCRIPCIÓN		FECHA INICIO	FECHA FINALIZACIÓN
1	Inicio	Se solicita autorización para la realización del proyecto y se expone su importancia y sus efectos para entidad		01-08-17	01-08-17
2	Aprobación	Se presenta la propuesta en la asignatura OPCIÓN DE GRADO I para su respectiva aprobación		15-08-17	24-08-17
3	Introducción	Se da una idea somera, pero exacta de los diversos aspectos que componen el trabajo, se hace un planteamiento claro y ordenado del proyecto.		01-02-18	01-02-18
4	Planteamiento del problema	Se establece una situación clara para analizarla, delimitarla, describirla y darle una posible situación o respuesta al porqué de sus causas o consecuencias. Se hace una descripción general del proyecto, en esta tarea se desarrollan los siguientes puntos. • Antecedentes del problema • Formulación del problema • Descripción o resumen del problema		02-02-18	10-02-17
5	Objetivos	Se redactan los objetivos del proyecto indicando las tereas a realizar. • El objetivo general es la finalidad del por qué empezamos a desarrollar un proyecto. • Los objetivos específicos corresponden a los pasos que se deben seguir para alcanzar el objetivo general.		11-02-18	11-02-18
6	Justificación	Se realiza la exposición de las razones por las cuales se realiza el proyecto.		12-02-18	12-02-18
7	Alcance	DEFINICIÓN DEL ALCANCE DEL PROYECTO	Se definen las características y funciones del proyecto que se van a entregar o que va ser objeto de estudio.	13-02-18	20-02-18
		MAPA DE PROCESOS	Se especifica el mapa de proceso de la entidad.		
		LIMITACIONES DEL PROYECTO	Se establecen las limitaciones del proyecto.		

8	Marco de referencia	ESTADO DEL ARTE	El desarrollo del estado del arte permite conocer otras investigaciones que nos permiten clarificar ideas respecto al tema de interés, y así podremos definirlo mejor, afinarlo, delimitarlo, y enfocarlo desde la perspectiva nos interesa.	21-02-18	28-02-18
		MARCO TEÓRICO	Se lleva a cabo la consulta de ideas, procedimientos y teorías que sirven para llevar a cabo el proceso de investigación	01-03-18	10-03-18
		MARCO CONCEPTUAL	Se lleva a cabo en esta actividad la consulta de toda la información detallada de los modelos teóricos, conceptos, argumentos e ideas que se han desarrollo en relación con el tema de investigación	11-03-18	15-03-18
		MARCO LEGAL	Se lleva a cabo las referencias de todas las leyes o reglamentos legales sobre los cuales se fundamente el proyecto.	16-03-18	16-03-18
		MARCO CONTEXTUAL	Se realiza una descripción donde (lugar o ambiente) se va a desarrollar el proyecto de investigación.	17-03-18	20-03-18
9	Metodología	METODOLOGÍA ISO/IEC27001:2013	Se realiza una descripción de la norma técnica ISO27001:2013 la cual describe cómo gestionar la seguridad de la información en una organización.	21-03-18	21-03-18
10	Desarrollo del proyecto	ANÁLISIS DIFERENCIAL	Este análisis permite comparar las condiciones actuales con el fin de encontrar las deficiencias existentes y el nivel de cumplimiento en base al estándar.	22-03-18	31-03-18
11		POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN	La política de alto nivel o política general, aborda la necesidad de la implementación de un sistema de gestión de seguridad de la información (SGSI) planteado desde la descripción del quién, qué, por qué, cuándo y cómo, en torno al desarrollo de la implementación del SGSI.	02-04-18	05-04-18

12		METODOLOGÍA DE ANÁLISIS y EVALUACIÓN DE RIESGOS	Definición de los conceptos fundamentales de la metodología MAGERIT. Esta metodología de análisis y gestión de riesgos elaborada por el Consejo Superior de Administración Electrónica de España, que ofrece un método sistemático para analizar los riesgos derivados del uso de tecnologías de la información y comunicaciones.	06-04-18	08-04-18
13		FORMALIZACIÓN DE ACTIVIDADES DEL PROYECTO MÉTODO DE ANÁLISIS DE RIESGOS	Caracterización de los activos	09-04-18	15-04-18
			Caracterización de las amenazas	16-04-18	18-04-18
			Estimación del riesgo potencial	19-04-18	20-04-18
14		DECLARACIÓN DE APLICABILIDAD (SOA)	Este documento permite definir qué controles son adecuados para implementar en la organización, cuáles son los objetivos de esos controles y cómo se implementan.	21-04-18	30-04-18
15		PLAN DE TRATAMIENTO DE RIESGOS	El objetivo de este documento es determinar, de forma precisa, quién es responsable de la implementación de los controles, en qué período de tiempo, con qué presupuesto, etc.	01-05-18	03-05-18
16		PLAN DE CONTINUIDAD DEL NEGOCIO	Permite definir de forma precisa cómo la organización gestionará los incidentes en caso de un desastre o de otra interrupción del negocio y cómo recuperará sus actividades críticas dentro de plazos establecidos	04-05-18	05-05-18
17	Conclusiones	Se redactan las conclusiones del proyecto		06-05-18	06-05-18
18	Recomendaciones	Se redactan las recomendaciones del proyecto		06-05-18	06-05-18
19	Bibliografía	Se establece la bibliógrafa empleada para la realización del proyecto		06-05-18	06-05-18

9 CONCLUSIONES

Un Sistema de Gestión de la Seguridad de la Información (SGSI), preserva la confidencialidad, integridad, disponibilidad y privacidad de la información, mediante la aplicación de un proceso de gestión del riesgo, brindando confianza entre los funcionarios de la administración municipal y los ciudadanos que demandan sus servicios.

Con el diseño del SGSI se garantiza que los riesgos de la seguridad de la información sean conocidos, asumidos, gestionados y minimizados por la entidad de una forma documentada, sistemática, estructurada, repetible, eficiente y adaptada a los cambios que se produzcan en los riesgos, el entorno y las tecnologías.

Posteriormente con su implementación se tendrá un municipio: Más Eficiente, Más transparente y Más participativo ya que se tendrá un mejor aprovechamiento de las TIC y un fortalecimiento de la seguridad de la información en la entidad, con el fin de garantizar la protección de la misma y la privacidad de los datos de los ciudadanos y funcionarios de la entidad, todo esto acorde con lo expresado en la legislación Colombiana.

El diseño del SGSI para la administración municipal de la Ceja-Antioquia está alineado con las mejores prácticas del estándar ISO27001:2013 y la metodología para el análisis de riegos Magerit, estas metodologías permitieron establecer los objetivos de seguridad de la información y un tratamiento de ellos.

Se actualizo la actual política de seguridad y privacidad de la información de la entidad, la cual fue aprobada en el comité del sistema integrado de gestión organizacional SIGO en el año 2015, Esta política se articulará a través del propio Sistema de Gestión de Seguridad de la Información basado en la norma internacional ISO 27001:2013 tratando de forma más detallada todos los aspectos necesarios para la correcta gestión de la seguridad de la información de la entidad alineada de forma efectiva con los demás sistemas de gestión.

La nueva política de información de seguridad de la entidad se constituirá en el derrotero a seguir en el uso, protección y manejo de la información y los recursos tecnológicos por parte de funcionarios, contratistas y particulares que ejercen funciones públicas y su cumplimiento será de carácter obligatorio

El SGSI permitirá que se gestionen los riesgos, se minimicen las amenazas y se traten las vulnerabilidades a las que se enfrentan los activos de información de la entidad y se establezcan medidas permitan mitigar los riesgos relacionados con los

activos involucrados en el procesamiento, tratamiento y almacenamiento de la información, además del cumplimento del 100% en lo referente a información, iteración, transacción , transformación, democracia y otras actividades trasversales que se realizan en línea y que hacer parte del quehacer de las entidades públicas.

10 RECOMENDACIONES

Es importante la revisión del proyecto por parte de las dependencias de control interno, planeación, presupuesto, el departamento administrativo general y por los integrantes del comité SIGO, antes de su implementación, para evaluar la asignación de recursos económicos y su nivel de compromiso con el Sistema General de Seguridad de la información SGSI.

El cumplimento de la Política de Seguridad y privacidad de la Información es de carácter obligatorio para todo el personal de la entidad, cualquiera sea su situación laboral, el proceso al que pertenece y cualquiera que sea el nivel organizacional en el que se encuentre.

Es imprescindible que la Alta Dirección apruebe, dé a conocer y entender la actualización que se la hace a la política de seguridad y privacidad de la información a toda la entidad.

Los usuarios de la Información y de los Sistemas utilizados para su procesamiento son responsables de conocer, dar a conocer, cumplir y hacer cumplir la Política de Seguridad y privacidad actualizada.

Es fundamental dar capacitaciones y sensibilizaciones a todos los funcionarios, de la entidad en todos los temas relacionados a la seguridad y privacidad de la Información para mitigar riesgos de ataques de cualquier tipo.

Crear el comité de seguridad y privacidad de la información, como ente fundamental en la aplicación y revisión del SGSI.

De acuerdo a la guía Nro. 4 Roles y responsabilidades que emitió MINTiC acerca de la seguridad y privacidad de información expresa lo siguiente: “Es necesarios que se vincule de manera más efectiva a las directivas de la entidad para logra el éxito en la implementación de un SGSI en las entidades territoriales” (“Roles y Responsabilidades,” 2016)

11 BIBLIOGRAFÍA

¿Qué es una Declaración de Aplicabilidad (SoA) y para qué sirve? (n.d.). Retrieved May 4, 2018, from https://www.welivesecurity.com/la-es/2015/04/01/que-es-declaracion-de-aplicabilidad-soa/

Amutio Gómez, M. A. (2012). Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información, 75. Retrieved from https://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_Magerit.html#.Wuo5kO8vzcc

Análisis de riesgos con MAGERIT en el ENS (II) - Security Art Work. (n.d.). Retrieved May 2, 2018, from https://www.securityartwork.es/2012/04/26/analisis-de-riesgos-con-magerit-en-el-ens-ii/

Generales, A. (n.d.). AMENAZAS INFORMÁTICAS Y, 137–146.

ICONTEC. (2013). Norma Técnica Ntc-Iso/Iec Colombiana 27001. *Icontec*, (571), 37.

iso27000 @ www.iso27000.es. (n.d.). Retrieved from http://www.iso27000.es/iso27000.html

ISO 27001: El método MAGERIT. (n.d.). Retrieved May 2, 2018, from https://www.pmg-ssi.com/2015/03/iso-27001-el-metodo-magerit/

la-importancia-de-la-seguridad-en-las-tic @ www.euroinnova.co. (n.d.). Retrieved from https://www.euroinnova.co/11-7-26/la-importancia-de-la-seguridad-en-las-tic

manual-del-sistema-integrado-de-gestin-organizacional-sigo-1-.pdf. (n.d.).

Ministerio de Tecnologías de la Información y las Comunicaciones. (n.d.). Implementa - Estrategia GEL. Retrieved March 26, 2018, from http://estrategia.gobiernoenlinea.gov.co/623/w3-propertyvalue-7652.html

MINTIC. (2016). Política general de seguridad y privacidad de la información, (2). Retrieved from http://estrategia.gobiernoenlinea.gov.co/623/articles-8258_recurso_1.pdf

Neira, A. L., & Spohr, J. R. (2010). Sistema de Gestión de la Seguridad de la Información. *Article*, *1*, 14.

pae_Magerit @ administracionelectronica.gob.es. (n.d.). Retrieved from https://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_Magerit.html#.Wt_OQ9Twbcc

polseginf @ www.segu-info.com.ar. (n.d.). Retrieved from https://www.segu-info.com.ar/politicas/polseginf.htm

Principios de Seguridad Informatica | Seguridad Informatica. (n.d.). Retrieved May 2, 2018, from http://antisec-sys.blogspot.com.co/2016/06/objetivos-de-la-seguridad.html

Roles y Responsabilidades. (2016). Retrieved from https://www.mintic.gov.co/gestionti/615/articles-5482_G4_Roles_responsabilidades.pdf

Secretaría General de la Alcaldía Mayor de Bogotá D.C. (2011). Norma1 @ www.alcaldiabogota.gov.co. *Diario Oficial 48242 Del 3 de Noviembre de 2011*. Retrieved from http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=17985#2

ti-organizaciones @ sistemas.uniandes.edu.co. (n.d.). Retrieved from https://sistemas.uniandes.edu.co/es/isis-opciones/ti-organizaciones

Valencia Duque, F. J., & Orozco-alzate, M. (2017). Metodología para la implementación de un Sistema de Gestión de Seguridad de la Información basado en la familia de normas ISO / IEC 27000. *Revista Ibérica de Sistemas Y Tecnologías de Información*, (22), 73–88. https://doi.org/10.17013/risti.22.73

W3-Article-5414 @ Www.Mintic.Gov.Co. (n.d.). Retrieved from http://www.mintic.gov.co/portal/604/w3-article-5414.html