DISEÑO DE UN SISTEMA DE GESTION DE LA SEGURIDAD DE LA INFORMACION ISO 27001 PARA LA ALCALDIA DE FLORIDABLANCA Y PLAN DE ACCION PARA SU IMPLEMENTACION SEGÚN LA GUIA PMBOK

JULIO ANDRÉS ANGARITA LEIVA

CINDY LORENA BAUTISTA BOHORQUEZ

UNIVERSIDAD INDUSTRIAL DE SANTANDER
FACULTAD DE INGENIERIAS FISICOMECÁNICAS
ESCUELA DE ESTUDIOS INDUSTRIALES Y EMPRESARIALES
BUCARAMANGA
2014

DISEÑO DE UN SISTEMA DE GESTION DE LA SEGURIDAD DE LA INFORMACION ISO 27001 PARA LA ALCALDIA DE FLORIDABLANCA Y PLAN DE ACCION PARA SU IMPLEMENTACION SEGÚN LA GUIA PMBOK

JULIO ANDRÉS ANGARITA LEIVA
CINDY LORENA BAUTISTA BOHORQUEZ

Monografía para Optar por al título de

Especialista en Evaluación y Gerencia de Proyectos

Director:

Manuel José Álvarez Arango

Administrador de Empresas

UNIVERSIDAD INDUSTRIAL DE SANTANDER
FACULTAD DE INGENIERIAS FISICOMECÁNICAS
ESCUELA DE ESTUDIOS INDUSTRIALES Y EMPRESARIALES
BUCARAMANGA
2014

CONTENIDO

LISTA DE TABLAS

LISTA DE FIGURAS

LISTA DE ANEXOS

RESUMEN

TITULO: DISEÑO DE UN SISTEMA DE GESTION DE LA SEGURIDAD DE LA INFORMACION ISO 27001 PARA LA ALCALDIA DE FLORIDABLANCA Y PLAN DE ACCION PARA SU IMPLEMENTACION SEGÚN LA GUIA PMBOK.*

AUTORES: ANGARITA LEIVA, Julio Andrés **
BAUTISTA BOHÓRQUEZ, Cindy Lorena**

PALABRAS CLAVE: Sistema de gestión de seguridad de la información. Activo de información. Gestión de riesgos. Objetivos de control. Gestión del proyecto. Interesados. Recursos.

CONTENIDO: Hoy en día muchas empresas consideran la información como el activo más importante, es por esto que se buscan medios para su protección, la norma ISO 27001 da soporta para el proceso de gestión de la información. Debido a los grandes volúmenes de información que maneja una empresa, esta se encuentra expuesta a riesgos que pueden afectar la integridad, disponibilidad y confidencialidad de la información.

La norma ISO 27001 presenta un modelo estándar para establecer, implementar, realizar seguimiento y revisión, mantenimiento y mejora de un sistema de gestión de seguridad de la información documentado en el contexto de los riesgos globales de cualquier organización, especificando la implementación de controles de seguridad de acuerdo a las características de la organización.

La alcaldía de Floridablanca con base en los requisitos legales establecidos en la ley 1581 de 2012, donde se dictan disposiciones generales para la protección de datos personales y teniendo en cuenta su plan estratégico requiere el diseño de un sistema de gestión de la seguridad de la información ISO 27001 que se adapte a los procesos de la entidad.

En el desarrollo de este proyecto se realizo el diseño de un SGSI para la Alcaldía de Floridablanca fundamentado en los principales procesos de la entidad, posteriormente se realiza el proceso de gestión del proyecto basado en la guía PMBOK.

---

* Proyecto de grado

** Facultad de Ingenierías Físico-Mecánicas. Escuela de Estudios Industriales y Empresariales. Director: Manuel José Álvarez Arango.

ABSTRACT

TITLE: DESIGN OF AN INFORMATION SECURITY MANAGEMENT SYSTEM ISO 27001 FOR FLORIDABLANCA TOWN HALL AND MANAGEMENT PLAN FOR ITS IMPLEMENTATION BY THE PMBOK GUIDE.*

AUTHORS: ANGARITA LEIVA, Julio Andrés **
BAUTISTABOHÓRQUEZ, Cindy Lorena**

KEY WORDS: Information security management system, information asset, risk management, control objectives, project management, stakeholders, resources.

CONTENT: Today, lots of companies are considering the information asset like the most important for them, therefore there are ways to ensure the information, ISO 27001 standard provides supporting to the information process management. Due to large information volumes that are managed by companies, there are a lot of risks that could affect the integrity, availability and confidentiality of information.

ISO 27001 standard shows a model to establish, implement, check and improve an Information security management system which take part within global risk context of any company, specifying security controls according the organizational features

The town hall of Floridablanca in order to legal requirements established by the law of data protection since 2012, which there are general provisions for the protection of personal data and considering its strategic plan requires and design of an information security management system ISO 27001 which could be applied inside their management process.

The project has been developed with the Information security management system for the town hall of Floridablanca which were made whit the main company process management, hence the management process based on PMBOK guide.

---

* Minor Degree Project

** Faculty of Physic and Mechanic Engineering. School of Industrial and Business Studies. Director: Manuel José Álvarez Arango.

INTRODUCCIÓN

La información en una organización es un bien de pertenencia exclusiva, no puede estar al alcance de agentes externos, procesos o personas no interesadas, por eso un objetivo claro es lograr alcanzar los niveles más altos posibles de confidencialidad, disponibilidad e integridad.

Dado que la información se considera el principal activo de toda organización constantemente se encuentra amenazada desde muchas fuentes, que pueden ser internas o externas, accidentales o maliciosas, que podrían traer daños a la integridad de la organización. La ISO 27001:2005 se plantea como el estándar internacional que establece las pautas para implementar un Sistema de Gestión de Seguridad de la Información.

Debido a que la Alcaldía de Floridablanca es una organización que maneja grandes volúmenes de información en cada uno de sus procesos, la gestión de la seguridad de la información le permitirá manejar adecuadamente los flujos internos de información, protegiendo todo aquello que se considere confidencial.

La oficina de sistemas, es la principal responsable del procesamiento y almacenamiento de la información dentro de la entidad, y tiene como objetivo la implantación de un sistema de gestión de seguridad de la información ISO 27001 para dar cumplimiento a la ley 1581 del año 2012, y así lograr dar un manejo eficiente a la información.

En el presente trabajo de grado, se describe el diseño de un sistema de gestión de la seguridad de la información ISO-27001 acorde a las necesidades de la Alcaldía de Floridablanca (Santander), basados en el estándar para la gerencia de proyectos consignado en la guía PMBOK v5 del Project Management Institute para su implementación en la entidad.

1. OBJETIVO GENERAL

Diseñar un sistema de gestión de la seguridad de la información ISO 27001 con el propósito de preservar la confidencialidad, integridad y disponibilidad de la información en la Alcaldía de Floridablanca usando como base para el proceso de gestión la guía PMBOK.

1.1. OBJETIVOS ESPECIFICOS

- Analizar la situación actual de la Alcaldía de Floridablanca.
- Establecer el sistema de gestión de la seguridad de la información.
- Definir los procedimientos involucrados en el proceso de seguimiento y revisión del SGSI.
- Definir los procedimientos involucrados en el proceso de mantenimiento y mejora del SGSI.
- Elaborar el plan de gestión del proyecto con base en la guía PMBOK.

1.2. METODOLOGÍA SEGUIDA DURANTE EL PROYECTO

Durante el presente proyecto fue necesario el uso de técnicas de diagnóstico como la realización de entrevistas, reuniones de grupo, análisis de documentos de la organización y observación directa.

Inicialmente fue necesaria la realización de mapas mentales para estudiar la norma ISO 27001 y extraer los aspectos que se contemplarían en el proyecto, esta técnica fue bastante útil ya que permitió tener claridad en la totalidad de los procesos que se llevarían a cabo y las herramientas que se utilizarían.

Se realizó el análisis de los documentos suministrados por la organización para extraer información sobre sus características, inferir aspectos importantes sobre la cultura organizacional y conocer a profundidad los procesos que se manejan internamente.

Posteriormente fue necesario la realización de entrevistas y reuniones de grupo con el personal encargado de la oficina de sistemas para conocer a fondo la situación actual de la organización en cuanto al manejo de la información, y la forma real como se llevan a cabo los procesos.

El conocimiento de los procesos de la organización nos permitió definir el alcance, establecer la política de seguridad de la información e identificar los principales activos de información de la Alcaldía con relación al alcance.

Fue clave contar con la ayuda de los encargados del manejo de la información clave de la entidad para identificar los controles actualmente implementados en cuanto a la seguridad de la información. Además la observación directa nos permitió establecer los principales riesgos que afectan la seguridad de la información.

Fue necesario definir una metodología propia que se ajustara a los requerimientos de la norma para realizar la valoración de los riesgos, donde se tuviera en cuenta

la valoración del impacto en la confidencialidad, disponibilidad e integridad de la información.

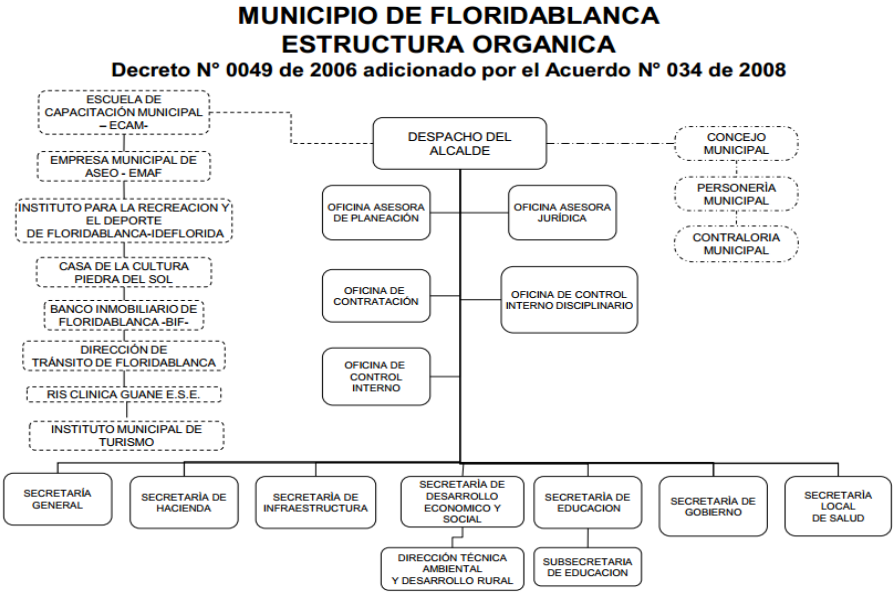
Los procesos de seguimiento y revisión así como el de mantenimiento y mejora fueron contemplados en la última etapa, cuando ya se tenía un conocimiento más amplio de las características de la organización y de la forma como se llevaban a cabo los procesos internos, fue necesario realizar consultas de diferentes fuentes secundarias para tener un conocimiento más amplio de las fases que era necesario tener en cuenta.

2. ALCALDIA DE FLORIDABLANCA

2.1. ESTRUCTURA ORGANIZACIONAL

La Entidad cuenta con una estructura organizacional que le permite definir los diferentes niveles de responsabilidad y autoridad, es función de la alta dirección asegurar que las responsabilidades y autoridades estén definidas y comunicadas dentro de la Entidad. La siguiente estructura organizacional se representa en la siguiente figura:

Figura 1. Estructura Organizacional de la Alcaldía de Floridablanca.

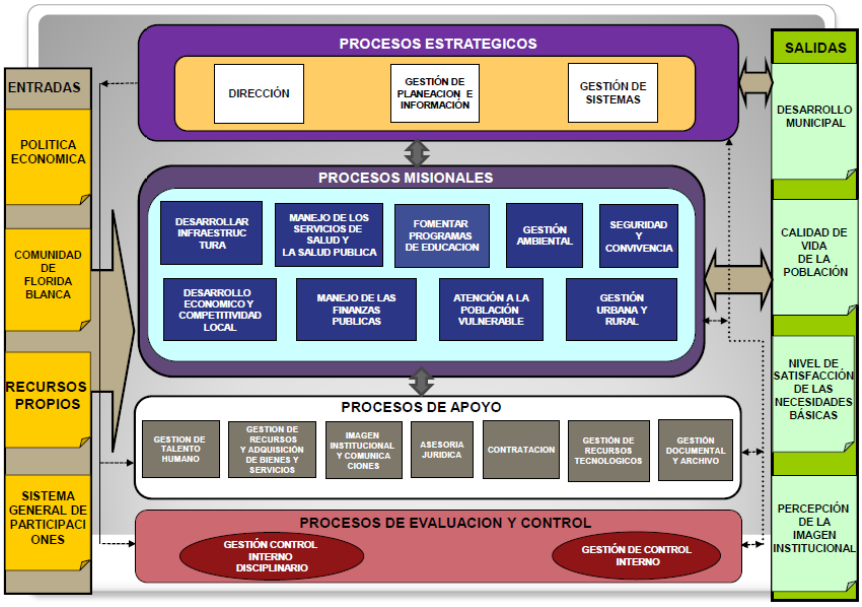


Fuente: Estructura Orgánica, Estructura administrativa del Municipio de Floridablanca Santander, Decreto 0066 de 2013, pág. 29.

El mapa de procesos de la alcaldía está definido en función de cumplir los objetivos organizacionales como entidad pública, los cuales están definidos en su plan estratégico. Se define proceso como *cualquier actividad que use recursos y*

cuya gestión permita la transformación de entradas en salidas[2] En la siguiente figura, se describe el mapa de procesos de la Alcaldía de Floridablanca:

Figura 2. Mapa de procesos de la Alcaldía de Floridablanca.



Fuente: Mapa de procesos, Modelo Estándar de Control Interno (MECI)/Calidad http://floridablanca.gov.co/download/meci/GS-G-200-27.001%20MAPA%20DE%20PROCESOS.pdf.

2.2. PLAN ESTRATÉGICO

2.2.1. Misión

El Municipio de Floridablanca como entidad se desarrolla conforme a los principios de dignidad, responsabilidad, transparencia, eficiencia, equidad y solidaridad, con el fin de promover la participación comunitaria, el mejoramiento social y cultural de sus habitantes y atender las competencias legales inherentes al Municipio y particularmente para:

[2]INSTITUTO COLOMBIANO DE NORMALIZACIÓN Y CERTIFICACIÓN. Sistemas de gestión de la seguridad de la información (SGSI). NTC-ISO/IEC 27001. Bogotá D.C.: El instituto, 2006. 46 p.

- ✓ Administrar los asuntos municipales y prestar los servicios públicos que determine la ley.
- ✓ Ordenar el desarrollo de su territorio y construir las obras que demande el Progreso municipal.
- ✓ Promover la participación comunitaria y el mejoramiento social y cultural de sus habitantes.
- ✓ Planificar el desarrollo económico, social y ambiental de su territorio, de conformidad con la ley y en coordinación con otras entidades.
- ✓ 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.
- ✓ Velar por el adecuado manejo de los recursos naturales y del medio ambiente, de conformidad con la ley.
- ✓ Promover el mejoramiento económico y social de los habitantes del respectivo municipio.
- ✓ Hacer cuanto pueda adelantar por sí mismo, en subsidio de otras entidades territoriales, mientras éstas proveen lo necesario.

2.2.2. Visión

Floridablanca, en el año 2015, será reconocida como un Municipio de gestión pública transparente, eficaz, eficiente y participativa, con una identidad propia y reconocimiento como el corazón del Área Metropolitana por sus niveles de crecimiento y competitividad que propician la igualdad de oportunidades enmarcadas en sistemas de inversión social, con óptimos resultados en seguridad, educación, salud e innovación, destacándose como líder en la gestión y ejecución de proyectos ambientalmente amigables que favorezcan el fortalecimiento institucional y la generación de mejores niveles de vida para sus habitantes.

2.2.3. Política de calidad

La Alcaldía del Municipio de Floridablanca, se compromete a ofrecer una atención al ciudadano como lo establece la Ley, orientados a un desarrollo y mejoramiento territorial, económico, ambiental, social y cultural, promoviendo la participación y progreso del Municipio, logrando la Satisfacción de los Comunidad de Floridablanca, ejerciendo sus labores con responsabilidad y transparencia, para lo cual contará con Servidores Públicos competentes que contribuyen a la mejora continua de los Procesos permitiendo demostrar una Administración Municipal eficiente, eficaz y efectiva que cumpla con las Políticas de Operación.

2.2.4. Objetivos de calidad

Garantizar la Satisfacción del ciudadano, brindando un Servicios con responsabilidad, transparencia, equidad y solidaridad, que permita lograr una Administración Municipal Eficiente.

Contribuir al Desarrollo del Municipio, mediante el mejoramiento territorial, económico, ambiental, social y cultural, asegurando el funcionamiento adecuado de los procesos de la Entidad.

Fortalecer continuamente a los Servidores Públicos, desarrollando un equipo humano competentes, en constante capacitación, comprometidos y con sentido de pertenencia en la prestación de servicios a la comunidad.

Implementar mecanismos para la mejora continua en los procesos de la Entidad.

2.3. SITUACIÓN ACTUAL DE LA ALCALDÍA DE FLORIDABLANCA

Con base en la información recopilada podremos hacer un análisis del manejo que se le da actualmente a la información en la Alcaldía de Floridablanca, para la entidad la información es un activo fundamental para la prestación de sus servicios y la toma de decisiones eficientes, razón por la cual existe un compromiso expreso de protección de la información, el cual es plasmado en la política de seguridad de la información de la entidad.

La Alcaldía maneja grandes volúmenes de información, lo que cada vez hace más difícil implantar controles eficientes; los actuales controles llegan a ser insuficientes y poco eficientes, por lo tanto es necesario realizar mejoras que están alineadas a una normativa.

La información está expuesta a gran cantidad de riesgos, no existe una cultura de seguridad ni mucho menos una garantía en el cumplimiento de los requerimientos legales vigentes.

Existe gran cantidad de problemas relacionados con el uso que se le da a la información, entre los más importantes están:

1. Los controles de los servicios que presta la entidad relacionados con el manejo de información de los predios del municipio, los contribuyentes e industria y comercio son mínimos, lo que podría causar uso indebido o pérdida de información.

2. No existe un plan de contingencia documentado y difundido que permita la continuidad de las operaciones de la entidad en caso de hechos que expongan la integridad de los equipos de cómputo y la información contenida en los diferentes medios de almacenamiento.

3. La política de seguridad de la información con la que cuenta la entidad no especifica los procedimientos del manejo adecuado de la información en la organización.

4. No hay un procedimiento formal para la realización de las copias de seguridad de la información contenida en servidores y equipos, estas son hechas sin tener en cuenta la periodicidad en que se deberían realizar ni las condiciones de almacenamiento posterior.

5. Cuando se realizan cambios sobre el servidor estos no son documentados, lo que genera grandes desventajas en caso de presentarse algún problema posterior a la modificación de alguna de sus características.

6. No hay claridad de los controles que se deben tener para garantizar la protección de la información y los mecanismos que aseguren que esta solo llegue al personal de interés.

7. No existe un procedimiento formal de registro de usuarios para otorgar y revocar el acceso a todos los sistemas y bases de datos, adicionalmente no se controla la asignación de privilegios de lo usuario en el sistema.

8. La importancia que le da la organización a la capacitación del personal en todo lo relacionado a la seguridad de la información es aceptable.

9. En la alcaldía se realizan copias de seguridad de la información contenida en los servidores.

10. Los equipos están ubicados en sitios designados como seguros.

11. Los equipos de la entidad reciben mantenimiento en periodos no programados.

12. La Alcaldía restringe el acceso al código fuente de los programas de la organización.

2.4. MARCO LEGAL:

Todas las personas tienen derecho a su intimidad personal y familiar y a su buen nombre, y el Estado debe respetarlos y hacerlos respetar. De igual modo, tienen

derecho a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bancos de datos y en archivos de entidades públicas y privadas.[3]

Por medio del anterior Artículo, la Constitución Política estipula como derecho la intimidad personal, a conocer, actualizar y rectificar las informaciones que se hayan recogido por entidades u organizaciones de carácter público o privado en el Estado Colombiano, así mismo la recolección, tratamiento y circulación de datos deberá cumplir con las garantías consagradas en la constitución. Garantizar la libertad de expresión y la difusión del pensamiento y opiniones así como la acción de informar y recibir información veraz e imparcial están consignados en el Artículo 20 de la misma.

El marco legal Colombiano exige un tratamiento veraz de la información haciendo énfasis en la difusión, corrección y publicación de los datos procesados. El desarrollo de este derecho constitucional que tienen los colombianos, las libertades y garantías constitucionales referidas en los artículos 15 y 20 se desarrollan mediante la ley 1581 de 2012 "*Por el cual se dictan disposiciones generales para la protección de datos personales*[4]" decretada por el congreso de la República.

La presente ley tiene por objeto desarrollar el derecho constitucional que tienen todas las personas a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bases de datos o archivos, y los demás derechos, libertades y garantías constitucionales a que se refiere el artículo 15 de la Constitución Política; así como el derecho a la información consignado en el artículo 20 de la misma.

La ley 1581 del 2012 aplicada en todo el territorio Colombiano, establece los principios y disposiciones para el tratamiento de los datos personales que son almacenados en bases de datos por entidades de naturaleza pública o privada.

[3] COLOMBIA. CONGRESO DE LA REPÚBLICA. Artículo 15 (Constitución política de Colombia, 1991)
[4] COLOMBIA. CONGRESO DE LA REPÚBLICA. Ley 1581 (17, Octubre, 2012). Por la cual se dictan disposiciones generales para la protección de datos personales. Diario Oficial. Bogotá, D.C., 2012. No 48587.

La norma establece principios rectores para el tratamiento de los datos con el fin de dar una aplicación y cumplimiento integral correspondiente a los principios establecidos en la constitución política. El sistema de gestión de la seguridad de la información abarca las exigencias legales expuestas en la ley 1581 de 2012 para la gestión de la información.

2.5. JUSTIFICACIÓN

Cada vez hay más consenso sobre la importancia de la Seguridad de la Información en las organizaciones, todas ellas sin importar su tamaño, sector de la economía o rol que desempeña dentro de la sociedad deben contar con un sistema de gestión de seguridad de la información, ya que este proporciona grandes herramientas para la correcta administración de la información, garantizando los aspectos de confidencialidad, integridad y disponibilidad que debe cumplir.

Según el estándar Internacional ISO/IEC 17799 "*la información es un activo que, como otros activos comerciales importantes, es esencial para el negocio de una organización y en consecuencia necesita ser protegido adecuadamente."* Por ende se justifica la realización de un sistema de gestión de seguridad de la información con el fin de salvaguardar los intereses de la población del municipio de Floridablanca y de la Entidad Pública dado que la entidad cuenta con suficiente información almacenada en diversos medios los cuales se deberán realizar un adecuado plan de gestión para su tratamiento.

Con la implantación de un SGSI la Alcaldía de Floridablanca minimizará considerablemente el riesgo de que sus procesos se vean afectados por la ocurrencia de eventos que comprometan la integridad de la información.

Adicionalmente, la implantación del sistema de gestión de seguridad de la información permite dar cumplimiento a lo dispuesto en la ley 1581 del año 2012, donde se contemplan los principios y disposiciones generales para el tratamiento de la información que ha sido registrada en las bases de datos de entidades públicas y privadas.

3. SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN EN LA ALCALDIA DE FLORIDABLANCA

3.1. ESTABLECIMIENTO DEL SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

3.1.1. Definición del Alcance:

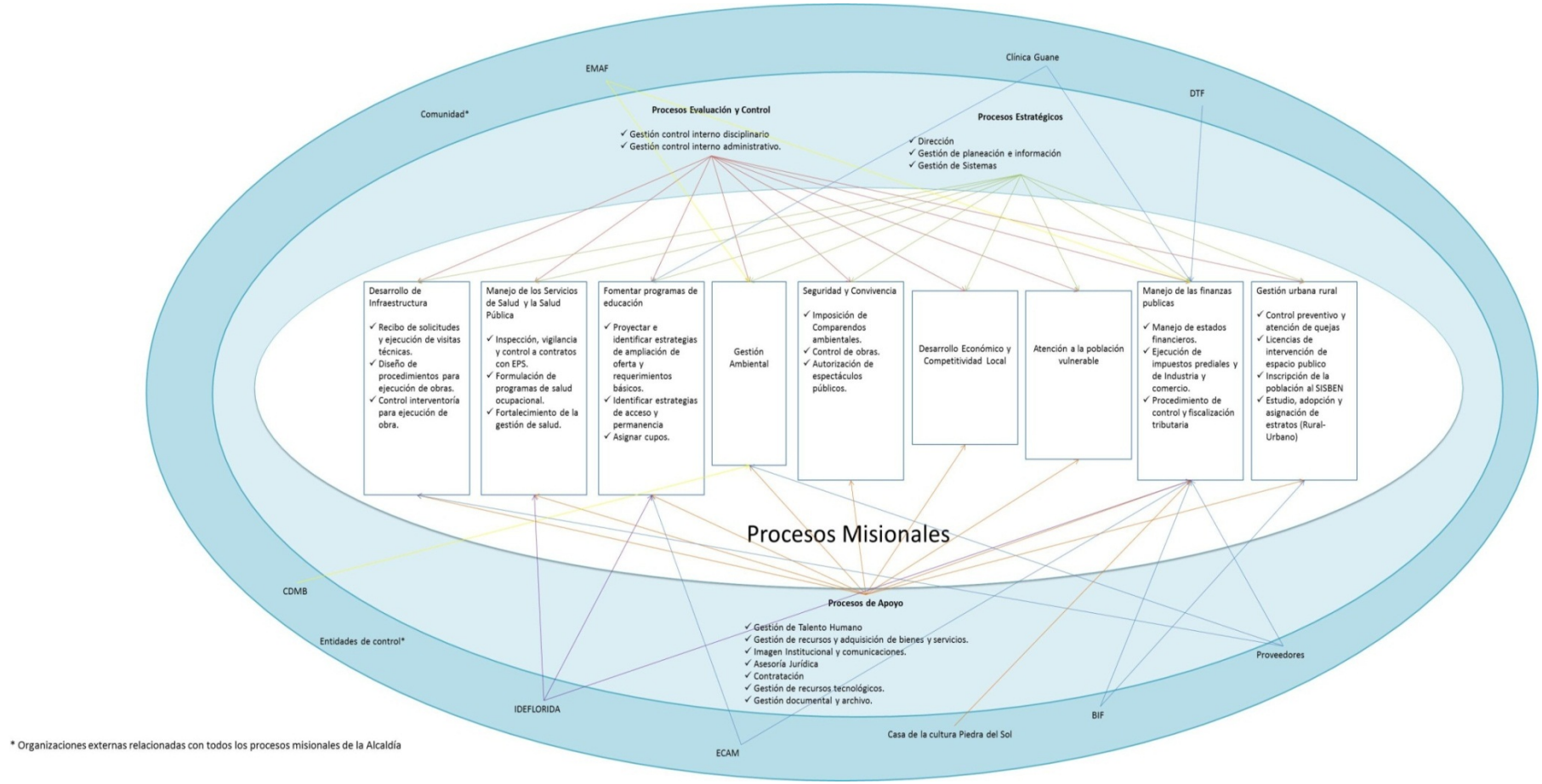
Entre las posibles opciones para definir el alcance estaba incluir toda la Alcaldía de Floridablanca o incluir solamente los procesos más importantes dentro de la entidad. Para tomar la decisión se tuvieron en cuenta aspectos como la poca experiencia con la que contaba la entidad en la implantación de SGSI lo que podría disminuir las posibilidades de éxito y el hecho de tener un alcance tan limitado también podría traer inconvenientes en el momento de ser auditado.

Se adopto el método de la elipse para identificar los procesos de la entidad y sus relaciones, inicialmente se tomó la totalidad de los procesos y se evidencio gran cantidad de relaciones entre ellos lo que implicaría trabajar sobre un alcance demasiado amplio, donde podría ser difícil controlar las diferentes variables.

Posteriormente se tomaron los procesos estratégicos como el centro de estudio pero al realizar el análisis se evidencio que la mayoría de los procesos giraban en torno a los procesos misionales de la entidad donde están concentrados la mayor cantidad de activos de información por lo que se determinó definir el alcance en torno a estos procesos.

Por medio del método de la elipse se identificó las relaciones entre los diferentes subprocesos que hacen parte de los procesos misionales, la relación con otros procesos de la entidad y las relaciones de los subprocesos con las entidades externas a la Alcaldía.

Figura 3. Método de la Elipse para la Alcaldía de Floridablanca



FUENTE: Los Autores

3.1.1.1. Procesos incluidos en el alcance

El sistema de gestión contemplará los procesos misionales de la entidad, los subprocesos que hacen parte de este proceso junto con algunas de las actividades que implica se describen a continuación:

Desarrollar infraestructura

- ✓ Recibo de solicitudes y ejecución de visita técnica
- ✓ Definición de procedimientos para la ejecución de obra
- ✓ Control e interventoría para la ejecución de obra publica

Manejo de los servicios de salud y salud publica

- ✓ Inspección, vigilancia y control a contratos con EPSS
- ✓ Fortalecimiento de la gestión de salud ante situaciones de emergencia y desastres
- ✓ Manejo de programas epidemiológicos
- ✓ Formulación del programa de salud ocupacional

Fomentar programas de educación

- ✓ Manejo de programas de capacitación y bienestar
- ✓ Vigilancia sobre los tramites de prestaciones sociales y económicas
- ✓ Proyectar e identificar estrategias de ampliación de oferta y requerimientos básicos
- ✓ Identificar estrategias de acceso y permanencia
- ✓ Solicitar reserva (prematricula) y reserva de cupos para alumnos antiguos
- ✓ Asignar cupos a niños procedentes de bienestar social
- ✓ Liquidación de prenomina y nomina

- ✓ Inducción del personal
- ✓ Nombramiento de personal
- ✓ Realización de evaluaciones de desempeño
- ✓ Atender, direccionar y hacer seguimiento a solicitudes

Gestión ambiental

Seguridad y convivencia

- ✓ Diseño de rutas de protección
- ✓ Recepción y protección al usuario
- ✓ Comparendo ambientales
- ✓ Control de obras
- ✓ Autorización de espectáculos públicos
- ✓ Propiedad horizontal
- ✓ Consultas Jurídicas

Desarrollo económico y competitividad local

Manejo de las finanzas publicas

- ✓ Estados financieros
- ✓ Conciliaciones bancarias
- ✓ Control y fiscalización
- ✓ Visita- Control establecimientos de comercio
- ✓ Ejecución de impuestos correspondientes a industria y comercio
- ✓ Ejecución de impuesto predial

- ✓ Ejecución de multas y sanciones
- ✓ Liquidaciones oficiales
- ✓ Cobro persuasivo
- ✓ Recaudo de Cartera
- ✓ Procedimiento de control y fiscalización tributaria
- ✓ Procedimiento de recaudo
- ✓ Certificados de disponibilidad presupuestal
- ✓ Registro presupuestal
- ✓ Manejo del estado de la deuda publica
- ✓ Contabilización de embargos
- ✓ Contabilización de fiducias
- ✓ Custodia de títulos valores

Atención a la población vulnerable

Gestión urbana y rural

- ✓ Control preventivo y atención de quejas
- ✓ Licencias de intervención de espacio publico
- ✓ Seguimiento de licencias urbanísticas expedidas
- ✓ Inscripción de la población al SISBEN
- ✓ Estudio, adopción y asignación de estratos (Rural- Urbano)

3.1.1.2. Procesos excluidos en el alcance

A continuación de mencionan los procesos que fueron excluidos del alcance pero se relacionan de forma directa con los procesos misionales:

PROCESOS ESTRATEGICOS

Dirección

- ✓ Definición de lineamientos estratégicos dentro de la organización.
- ✓ Establecer procedimientos de atención PQRS

Gestión de planeación e información

- ✓ Procesamiento de información geográfica para planes y proyecto de ordenamiento territorial.
- ✓ Atención y conceptualización para las consultas técnicas que involucren información georeferenciada.
- ✓ Coordinación de proyectos para el fortalecimiento de los recursos e insumos informáticos y operativos del área del SIG.
- ✓ Gestión del plan de ordenamiento territorial
- ✓ Seguimiento y evaluación de plan de ordenamiento territorial
- ✓ Revisión total o parcial del plan de ordenamiento territorial ejecución y seguimiento del plan de desarrollo

Gestión de sistemas

- ✓ Capacitación para directivos
- ✓ Capacitación para dependencias
- ✓ Diseño de manuales de procesos y procedimientos
- ✓ Diseño de manuales de operaciones y de calidad
- ✓ Establecimiento de políticas de operación

- ✓ Control de documentos
- ✓ Solicitudes de cambio a documentos
- ✓ Definición de políticas y objetivos de calidad
- ✓ Política de talento humano

PROCESOS DE APOYO

Gestión de talento humano

- ✓ Control de horarios
- ✓ Manejo de permisos
- ✓ Programación de actividades de campo
- ✓ Adquisiciones de recursos y bienes
- ✓ Realización de informes de bienestar
- ✓ Consolidación de proyectos
- ✓ Planes de capacitación
- ✓ Realización de Inducciones y reinducciones
- ✓ Evaluaciones de desempeño
- ✓ Manejo de historias laborales
- ✓ Liquidación de pensiones
- ✓ Liquidación de nomina

Gestión de recursos y adquisición de bienes y servicios

- ✓ Baja de bienes
- ✓ Ingreso de bienes

- ✓ Levantamiento físico de inventarios
- ✓ Control de activos fijos

Imagen institucional y comunicaciones

- ✓ Diseño del plan de comunicaciones
- ✓ Establecimiento de la Matriz de medios

Asesoría jurídica

- ✓ Consultas jurídicas
- ✓ Contestación de demandas

Contratación

- ✓ Establecimiento de procedimientos de contratación
- ✓ Realización de minutas de los contratos
- ✓ Realización de estudios de oportunidad y conveniencia

Gestión de recursos tecnológicos

Gestión documental y archivo

- ✓ Conservación de documentos
- ✓ Producción documental
- ✓ Recepción de documentos
- ✓ Trasferencia de documentos

PROCESOS DE EVALUACION Y CONTROL

Gestión control interno disciplinario

- ✓ Realización de investigaciones disciplinarias

- ✓ Pliegos de cargos
- ✓ Indagaciones preliminares

Gestión de control interno

- ✓ Programación de visitas especiales
- ✓ Programación de auditorias
- ✓ Seguimiento a acciones de mejora
- ✓ Elaboración de informes a los entes de control
- ✓ Administración del riesgo

3.1.1.3. Entidades externas

Entre las organizaciones o personas externas a la alcaldía que tienen algún tipo de relación con los procesos misionales se encuentran DTF, BIF, casa de la cultura piedra del sol, EMAB, CDMB, entidades de control, IDEFLORIDA, ECAM, proveedores, clínica Guane, EMAF y la comunidad en general.

3.1.2. Definición de la política SGSI

3.1.2.1. Aspectos generales

En la Alcaldía de Floridablanca la información es un activo fundamental para la prestación de sus servicios y la toma de decisiones eficientes, razón por la cual existe un compromiso expreso de protección de sus propiedades más significativas como parte de una estrategia orientada a la administración de riesgos y la consolidación de una cultura de seguridad.

Consciente de sus necesidades actuales, la Alcaldía de Floridablanca Implementa un modelo de gestión de seguridad de la información como la herramienta que permite identificar y minimizar los riesgos a los cuales se expone la información, ayuda a la reducción de costos operativos y financieros, establece una cultura de seguridad y garantiza el cumplimiento de los requerimientos legales, contractuales y regulatorios vigentes como los planteados en la Ley 1581 del 17 de octubre del 2012.

La ley 1581 dicta disposiciones generales para la protección de datos personales y contempla los principios generales para el tratamiento de la información que ha sido almacenada en las bases de datos de las entidades públicas y privadas.[5]

El proceso de análisis de riesgos de los activos de información es el soporte para el desarrollo de las Políticas de Seguridad de la Información, los controles y objetivos de vigilancia seleccionados para obtener los niveles de protección esperados en la Alcaldía de Floridablanca; este proceso será liderado de manera permanente por el comité designado para tal fin.

Esta política será revisada con regularidad como parte del proceso de revisión estratégica, o cuando se identifiquen cambios en la Entidad, su estructura, sus objetivos o alguna condición que afecte la política, para asegurar que sigue siendo adecuada y ajustada a los requerimientos identificados.[6]

3.1.2.2. Objetivos de seguridad

- ✓ Minimizar el riesgo en los procesos más importantes de la entidad.
- ✓ Cumplir con los principios de seguridad de la información.

[5] CONGRESO DE COLOMBIA. Ley estatutaria No. 1581 del 17 de Octubre de 2012. [En línea]. Disponible en <http://www.redipd.org/legislacion/common/legislacion/Colombia/Ley_1581_2012_COLOMBIA.pdf>

[6] ALCALDIA DE FLORIDABLANCA. Politica de seguridad de la información Alcaldía Municipal de Floridablanca. [En línea]. Disponible en <http://floridablanca.gov.co/wp-content/uploads/2013/06/POLITICA-DE-LA-SEGURIDAD-DE-LA-INFORMACION-1.pdf>

- ✓ Cumplir con los principios de la función administrativa.
- ✓ Mantener la confianza de sus clientes, socios y empleados.
- ✓ Apoyar la innovación tecnológica.
- ✓ Implementar el sistema de gestión de seguridad de la información.
- ✓ Proteger los activos tecnológicos.
- ✓ Establecer las políticas, procedimientos e instructivos en materia de seguridad de la información.
- ✓ Fortalecer la cultura de seguridad de la información en los funcionarios, terceros, aprendices, practicantes y clientes.
- ✓ Garantizar la continuidad del negocio frente a incidentes.
- ✓ Proteger la información de accesos no autorizados.
- ✓ Garantizar la privacidad de la información personal de los clientes.
- ✓ Evitar la modificación de la información de los clientes.

3.1.2.3. Políticas generales de seguridad de la información

La Alcaldía de Floridablanca ha decidido definir, implementar, operar y mejorar de forma continua un Sistema de Gestión de Seguridad de la Información, soportado en lineamientos claros acordes a las necesidades de la Entidad, y a los requerimientos regulatorios. Las responsabilidades frente a la seguridad de la información serán definidas, compartidas, publicadas y aceptadas por cada uno de los empleados, proveedores o terceros.

La entidad protegerá la información generada, procesada o resguardada por los procesos estratégicos, misionales y de apoyo de la Entidad, su infraestructura tecnológica y activos del riesgo que se genera de los accesos otorgados a terceros (ej.: proveedores o clientes), o como resultado de un servicio interno en outsourcing.

Debido a que la Alcaldía de Floridablanca maneja grandes flujos de información es necesario establecer controles que permitan minimizar impactos financieros, operativos o legales debido a un uso incorrecto de ésta.

La Alcaldía de Floridablanca protegerá su información de las amenazas originadas por el uso que realice el personal perteneciente a la entidad, así como implementara los controles de acceso a la información, sistemas y recursos de red.

Existirá un grupo de trabajo a cargo del manejo de la seguridad de la información de la entidad, el cual tendrá la responsabilidad del mantenimiento, revisión y mejora del sistema de gestión de la seguridad de la información.

Se identificaran en una etapa inicial los activos de información de la Alcaldía de Floridablanca, los cuales deberán ser clasificados y estudiados para posteriormente establecer los mecanismos de protección adecuados.

Es responsabilidad de todos los funcionarios y contratistas de la entidad reportar incidentes de seguridad, eventos sospechosos y mal uso de los recursos cuando estos eventos sean identificados.

La Alcaldía de Floridablanca contará con un plan de contingencias que garantice la continuidad de las operaciones ante la ocurrencia de eventos no previstos o desastres naturales.

3.1.2.4. Política de control de acceso

1. Cada empleado que haga uso de los sistemas de información de la entidad debe contar con un usuario y una contraseña única que sirva como mecanismo de autenticación.
2. El acceso a los recursos de información institucional debe ser restringido según los perfiles de usuario definidos.
3. Para aquellos accesos que se dan en casos especiales, es necesario contar con la autorización del propietario de dicha información.
4. El acceso remoto a servicios de red ofrecidos por la Alcaldía debe estar sujeto a medidas de control definidas internamente.

3.1.2.5. Política de correo electrónico

1. El uso del correo electrónico institucional debe ser para el desempeño de las funciones asignadas dentro de la Alcaldía de Floridablanca, debe usarse de forma responsable y ética.

2. El envío de información institucional debe ser realizado exclusivamente desde la cuenta de correo de la Alcaldía.

3. Toda información de la entidad que hubiese sido generada en los diferentes programas computacionales, que requiera ser enviada fuera de la institución garantizando su confidencialidad e integridad deberá ser protegida presentándose en formatos no editables.

4. Deberán existir normas mediante las cuales se asignan cuentas de correo electrónico incluyendo medidas de seguridad, nombres de usuario, contraseñas y demás mecanismos de autenticación.

3.1.2.6. Política del uso de internet

1. Los usuarios que tengan acceso a Internet a través de la entidad no deberán tener expectativas de privacidad alguna con relación al uso y los accesos realizados a través del internet. La alcaldía de Floridablanca se reserva el derecho a intervenir y auditar los accesos realizados por los usuarios a través de su sistema de información, el acceso a Internet y el contenido de lo accedido.

2. La Alcaldía de Floridablanca será responsable por velar que la conexión a internet se lleve dando cumplimiento a lo estipulado en la política de seguridad de la información, donde está incluido el monitoreo del funcionamiento correcto de las conexiones.

3. Cualquier información o servicio publicado en internet deberá ser autorizado por las autoridades de la entidad y bajo el conocimiento de la

persona que lidera el manejo de la seguridad de la información de la Alcaldía.

4. El intercambio no autorizado de información de propiedad de la Alcaldía de Floridablanca, de sus clientes y/o funcionarios, con terceros está prohibido y serán tomadas las medidas correctivas necesarias en caso de presentarse esta situación.

3.1.2.7. Política de uso de los sistemas de información

1. Toda información almacenada, creada o trasmitida desde o hacia los sistemas de información es propiedad de la Alcaldía de Floridablanca, por lo que le serán aplicadas todas las disposiciones establecidas en la política de seguridad de la información. La divulgación de tal información sin autorización está estrictamente prohibida. La alteración fraudulenta de cualquier documento en formato electrónico redundara en las sanciones que se consideren aplicables.

2. La entidad deberá tomar las medidas aplicables a fin de garantizar la confidencialidad de la información privada de los usuarios.

3. Está prohibido reproducir los medios de instalación de las aplicaciones, manuales y sistemas de información utilizados por la institución, además queda prohibido el uso de los mismos para fines diferentes a los institucionales.

4. La Alcaldía de Floridablanca se reserva el derecho de emprender los procesos administrativos pertinentes con relación a los actos cometidos, si dichos actos directa o indirectamente ponen en riesgo la integridad, confidencialidad o disponibilidad de la información, los equipos y los sistemas de información.

5. Los derechos de propiedad intelectual del software de la entidad deben estar claramente documentados.[7]

3.1.2.8. Política para la realización de copias de respaldo

1. El área de sistemas establecerá procedimientos explícitos de resguardo y recuperación de la información que incluyan especificaciones acerca del traslado, frecuencia e identificación de dicha información.

2. La entidad realizara pruebas controladas para asegurar que las copias de seguridad puedan ser correctamente leídas y restauradas.

3. Los registros de copias de seguridad deben ser guardados en una base de datos creada para tal fin.

4. La oficina de control interno deberá efectuar auditorias que permitan determinar el correcto funcionamiento de los procesos de copias de seguridad.

3.1.3. Enfoque organizacional para la valoración del riesgo.

La metodología seleccionada para la valoración del riesgo fue definida por los autores, de acuerdo a los requerimientos del sistema de gestión de seguridad de la información, en cada etapa se describe con claridad que pasos se siguieron para llegar al resultado obtenido.

3.1.4. Identificar los riesgos

3.1.4.1. Identificación de los activos:

Se identifica los activos involucrados dentro del alcance del SGSI y sus propietarios según la siguiente clasificación:

[7] Requisito de la Contralia Municipal de Floridablanca 2013

Activos primarios:

Están divididos en:

Tabla 1. Procesos y actividades del negocio

Subprocesos	Actividades	Propietario
Desarrollar infraestructura	Recibo de solicitudes y ejecución de visita técnica Definición de procedimientos para la ejecución de obra Control e interventoría para la ejecución de obra publica	Secretaría de Infraestructura
Manejo de los servicios de salud y salud publica	Inspección, vigilancia y control a contratos con EPSS Fortalecimiento de la gestión de salud ante situaciones de emergencia y desastres Manejo de programas epidemiológicos Formulación del programa de salud ocupacional	Secretaría de salud
Fomentar programas de educación	Manejo de programas de capacitación y bienestar Vigilancia sobre los tramites de prestaciones sociales y económicas Proyectar e identificar estrategias de ampliación de oferta y requerimientos básicos Identificar estrategias de acceso y permanencia Solicitar reserva (pre matricula) y reserva de cupos para alumnos antiguos Asignar cupos a niños procedentes de bienestar social Liquidación de pre nómina y nomina Inducción del personal Nombramiento de personal Realización de evaluaciones de desempeño Atender, direccionar y hacer seguimiento a solicitudes	Secretaría de educación
Gestión ambiental		Secretaría de gobierno
Seguridad y convivencia	Diseño de rutas de protección Recepción y protección al usuario Comparendo ambientales Control de obras Autorización de espectáculos públicos Propiedad horizontal Consultas Jurídicas	Secretaría de gobierno
Desarrollo económico y competitividad local		Secretaría de desarrollo económico y social
Manejo de las finanzas publicas	Estados financieros	Secretaría de Hacienda

	Conciliaciones bancarias Control y fiscalización Visita- Control establecimientos de comercio Ejecución de impuestos correspondientes a industria y comercio Ejecución de impuesto predial Ejecución de multas y sanciones Liquidaciones oficiales Cobro persuasivo Recaudo de Cartera Procedimiento de control y fiscalización tributaria Procedimiento de recaudo Certificados de disponibilidad presupuestal Registro presupuestal Manejo del estado de la deuda publica Contabilización de embargos Contabilización de fiducias Custodia de títulos valores	
Atención a la población vulnerable		Secretaría de gobierno
Gestión urbana y rural	Control preventivo y atención de quejas Licencias de intervención de espacio publico Seguimiento de licencias urbanísticas expedidas Inscripción de la población al SISBEN Estudio, adopción y asignación de estratos (Rural- Urbano)	Secretaría de gobierno

Fuente: Los Autores.

Tabla 2. Información

Tipo de Información	Característica	Propietarios
Vital	Licencias	oficina asesora de planeación
	Información Financiera	secretaria de Hacienda
	Estudios	Secretarías
	Información legal	oficina asesora jurídica
	Solicitudes	Secretarías
	Manuales de operación	Secretaria general
Personal	Información de los propietarios de los predios que hacen parte del municipio de Floridablanca	Impuesto Predial
	Personas Jurídicas	Industria y Comercio
	Funcionarios Públicos	Secretario General
	Proveedores	Secretarías
	Personas naturales	Secretarías
Estratégica	Información de desempeño	Asesores y Alcalde
	Lineamientos Estratégicos	Asesores y Alcalde
	Procedimientos	Secretarías

	Planes y Proyectos	Secretarías
Alto Costo	Estudios adopción y asignación de estratos Información geográfica Planes de ordenamiento Territorial	Planeación

Fuente: Los Autores.

Activos de soporte:

Tabla 3. Hardware

Activo de Soporte	Tipo de Activo	Activo	Propietarios	Descripción
Hardware	Equipo móvil	Computadores portátiles	Secretarías	Maquinas electrónicas utilizadas para procesar todo tipo de información
	Equipo Fijo	Computadores de escritorio		
		Servidor de software GD	Oficina de Sistemas	
		Servidor de software Distrito		
		Servidor de telefonía IP		
		Servidor de Correo institucional		
	Periféricos para procesamiento	Impresoras	Secretarías	Equipos conectados a un computador a través de un puerto de comunicaciones.
		Scanner		
		Discos removibles		
	Medios Electrónicos	CD-Rom	Secretarías	*Medio de información que se puede conectar a un computador o red de computadores para el almacenamiento de datos*
		Discos duros removibles		
		Memorias removibles		
		DVDs		
	Otros medios	Papeles	Secretarías	Otros medios para la recepción, transmisión de datos.
		Fax		
		Transparencias		
		Teléfonos IP		
		Teléfonos convencionales		
		Fotocopiadoras		
		Contratos		
		Acuerdos		
		Comunicados		
		Actas		
		Documentos de procesos		
		Facturas		
		Recibos		
		Memorandos		
		Oficios		
		Reglamentos		
		Manuales de usuarios		
		Documentación del sistema		
		Evidencias de auditorias		
		Documentación		

		almacenada en archivos		
		Planes de mejoramiento		
		Correspondencia		

Fuente: Los Autores.

Tabla 4. Software

Activo de Soporte	Tipo de Activo	Activo	Propietarios	Descripción
Software	Sistema Operativo	windows server 2008	Oficina de Sistemas	En esta clasificación se ubican los sistemas operativos, el software que sirve para controlar e interactuar con el sistema operativo, proporcionando control sobre el hardware y dando soporte a otrosprogramas.
		windows XP Profesional SP 3		
		windows 7 Ultimate		
		Windows 8		
	Software de servicio, mantenimiento o administración	Antivirus ESET NOD 32		Complementa los servicios del sistema operativo y no está directamente al servicio de los usuarios y las aplicaciones.
		Ccleaner		
	Paquete de software o software estándar	Microsoft Project		Son productos completos comercializados y suministran servicios a los usuarios y las aplicaciones.
		Nero		
		Adobe Reader		
		Microsoft Office		
		Microsoft Visio		
		WinRar		
		Autocad		
		TeamViewer		
		Mozilla Thunderbird		
		PosgreSQL		
		Skype		
		NetBeans		
		Microsoft Visual basic 6.0		
		MySql		
		Eclipse		
	Aplicaciones estándar del negocio	Delfin Gd		Software comercial que permite a los usuarios acceder a servicios y funciones específicas
		Chip (Hacienda)		
		MGA		
	Aplicaciones específicas de negocio	Distrito		Software desarrollado específicamente para atender requerimientos de la Entidad.
		Pagina web de la Entidad		
		Aplicación Web de cuentas		
		Aplicación Web de ventanilla única		
		Aplicación web de Manejo de Cartera		
		Aplicación Web de Alumbrado Publico		
		Intranet Institucional		
		Correo institucional		
		Aplicación web DIAN		

Fuente: Los Autores.

Tabla 5. Redes

Activo de Soporte	Tipo de Activo	Activo	Propietarios	Descripción
Red	Medios y Soportes	Red pública de conmutación telefónica	Oficina de Sistemas	Medios y equipos de telecomunicaciones caracterizados por sus rasgos técnicos y físicos.
		Ethernet		
		GigabitEthernet		
		Línea de suscriptor digital asimétrica (ASDL)		
		WiFi 802.11		
	Transmisión pasiva o activa	Modems		Incluye todos los dispositivos intermedios o de transmisión.
		Switch		
		Routers		
		PBX		

Fuente: Los Autores.

Tabla 6. Personal

Activo de Soporte	Tipo de Activo	Activo	Descripción
Personal	Persona a cargo de la toma de decisiones	Alcalde	Son los encargados de la toma de decisiones y dueño de los activos primarios.
	Usuarios	Secretaría general	Personas que manejan los elementos sensibles de la actividad y tienen responsabilidad especial.
		Secretaría de Hacienda	
		Secretaría de infraestructura	
		Secretaría de desarrollo económico y social	
		Secretaría de educación	
		Secretaría de gobierno	
		Secretaría de salud	
		Oficina de control interno	
		Oficina de contratación	
		Oficina de control interno disciplinario	
		Oficina asesora jurídica	
		Oficina asesora de planeación	
	Personal de operación y mantenimiento	Administrador del sistema	Personas a cargo de la operación y el mantenimiento del sistema de información
		Funcionarios a cargo de copias de seguridad	
		Jefe de Oficina	
	Desarrolladores	Desarrolladores de aplicación	Están a cargo del desarrollo de las aplicaciones de la organización.

Fuente: Los Autores.

Tabla 7. Ubicación

Activo de Soporte	Tipo de Activo	Activo	Descripción
Sitio	Ambiente externo	Domicilios del personal	Lugares en los que no se aplica los medios de seguridad de la organización
		Instalaciones de otras organizaciones	
		Ambiente Fuera de la Alcaldía	
	Instalaciones	Establecimiento	Límites de la Alcaldía que están en

		Edificaciones	contacto directo con el exterior
	Zonas	Oficina	Frontera física que forma divisiones dentro de las instalaciones de la Alcaldía
		Zonas de acceso reservado	
	Servicios de comunicación	Líneas telefónicas	Servicios y equipos de telecomunicaciones suministrados por un proveedor
		Internet	
		Redes telefónicas internas	
	Servicios públicos	Suministro de energía	Destinados a satisfacer una necesidad colectiva
		Suministro de agua	
		Disposición de residuos	

Fuente: Los Autores.

Tabla 8. Estructura de la organización

Activo de Soporte	Tipo de Activo	Activo	Descripción
Organización	Autoridades	Despacho	Organizaciones de las cuales la Alcaldía deriva su autoridad
	Estructura de la organización	Secretarías	Diversas ramas de la organización bajo el control de la gerencia
	Subcontratistas/proveedores	Contratistas	Suministran a la organización un servicio o recurso

Fuente: Los Autores.

3.1.4.2. Amenazas de los activos

Como parte de la metodología realizada por los autores y la recomendación de la norma estudiada, se realiza la identificación de las amenazas a los activos antes mencionados.

En la siguiente tabla se clasifican las amenazas identificadas según su origen bajo la siguiente denominación:

- ✓ A: Accidentales
- ✓ D: Deliberadas
- ✓ E: Ambientales

Tabla 9. Identificación de las Amenazas

Tipo de Amenaza	Amenaza	Origen
Daño Físico	Fuego	A,D,E
	Daño por agua	A,D,E
	Contaminación	A,D,E
	Accidente importante	A,D,E

	Destrucción del equipo o los medios	A,D,E
	Polvo, corrosión, congelamiento	A,D,E
Evento Naturales	Fenómenos Climáticos	E
	Fenómenos Sísmicos	E
	Fenómenos Volcánicos	E
	Fenómenos Meteorológicos	E
	Inundación	E
Pérdida de los Servicios Esenciales	Falla en el Sistema de suministro de agua	A,D
	Pérdida de Suministro de energia	A,D,E
	Falla en el equipo de Telecomunicaciones	A,D
Perturbación debida a la radiación	Radiación electromagnética	A,D,E
	Radiación térmica	A,D,E
	Impulsos electromagnéticos	A,D,E
Compromiso de la Información	Interceptación de señales de interferencia comprometedoras	D
	Espionaje remoto	D
	Escucha encubierta	D
	Hurto de medios o documentos	D
	Hurto de equipos	D
	Recuperación de medios reciclados o desechados	D
	Divulgación	A,D
	Datos provenientes de fuentes no confiables	A,D
	Manipulación con hardware	D
	Difusión de credenciales de acceso al sistema	D
	Manipulación con software	A,D
	Detección de la posición	D
Fallas Técnicas	Falla del equipo	A
	Mal funcionamiento del equipo	A
	Saturación del sistema de información	A,D
	mal funcionamiento del software	A
	Error de actualización	A,D
	Incumplimiento en el mantenimiento del sistema de información	A,D
Acciones no autorizadas	Uso no autorizado del equipo	D
	Uso de dispositivos de almacenamiento externos	D
	Copia fraudulenta del software	D
	Uso de software falso o copiado	A,D
	Corrupción de los datos	D
	Procesamiento ilegal de los datos	D
Compromiso de las funciones	Error en el uso	A
	Abuso de derechos	A,D
	Falsificación de derechos	D
	Negación de acciones	D
	Incumplimiento en la disponibilidad del personal	A,D,E

Fuente: Los Autores.

3.1.4.3. Identificación de las vulnerabilidades:

A continuación se realiza la identificación de las vulnerabilidades que podrían ser aprovechadas por las amenazas:

Tabla 10. Identificación de las Vulnerabilidades

Tipo	Activos	Amenazas	Vulnerabilidades
Hardware	Equipo móvil Equipo Fijo Periféricos para procesamiento Medios Electrónicos Otros medios	Incumplimiento en el manejo del sistema de información	Mantenimiento Insuficiente / Instalación fallida de los medios de almacenamiento
		Destrucción de equipos o de medios	Ausencia de esquemas de reemplazo periódico
		Polvo, corrosión, congelamiento	Susceptibilidad a la humedad, el polvo y la suciedad
		Radiación Electromagnética	Sensibilidad a la radiación electromagnética
		Error en el uso	Ausencia de un eficiente control de cambios a la configuración
		Pérdida en el suministro de Energía	Susceptibilidad a las variaciones de voltaje
		Fenómenos meteorológicos	Susceptibilidad a las variaciones de temperatura
		Hurto de medios o documentos	Almacenamiento sin protección
		Uso de dispositivos de almacenamiento externos	falta de política de restricción de uso de dispositivos de almacenamiento no autorizados
		Hurto de medios o documentos	Falta de cuidado en la disposición final
		Hurto de medios o documentos	Copia no controlada
Software	Sistema Operativo Software de servicio, mantenimiento o administración Paquete de software o software estándar Aplicaciones estándar del negocio Aplicaciones específicas de negocio	Abuso de los derechos	Ausencia o insuficiencia de pruebas de software
		Uso de dispositivos de almacenamiento externos	Falta de conocimiento del estado del software y aplicativos de uso
		Difusión de credenciales de acceso al sistema	Ausencia de sistema de chequeo y control de la información en la red interna
		Abuso de los derechos	Defectos bien conocidos en el software
		Abuso de los derechos	Ausencia de "terminación de la sesión" cuando se abandona la estación de trabajo
		Abuso de los derechos	Disposición o reutilización de los medios de información sin borrado adecuado
		Abuso de los derechos	Ausencia de pistas de auditoria
		Abuso de los derechos	Asignación herrada de los derechos de acceso
		Corrupción de datos	Software ampliamente distribuido
		Corrupción de datos	En términos de tiempo utilización de datos herrados en los programas de aplicación
		Error en el uso	Interfaz de usuario compleja
		Error en el uso	Ausencia de documentación
		Error en el uso	Configuración incorrecta de parámetros
		Error en el uso	fechas incorrectas
		Falsificación de derechos	Ausencia de mecanismos de identificación y autentificación como la autentificación de usuario
		Falsificación de derechos	Tabla de contraseñas sin protección
		Falsificación de derechos	Gestión deficiente de las contraseñas

		Procesamiento ilegal de datos	Habilitación de servicios innecesarios
		Mal funcionamiento del software	Software nuevo o inmaduro
		Mal funcionamiento del software	Especificaciones incompletas o no claras para los desarrolladores
		Mal funcionamiento del software	Ausencia de control de cambios eficaz
		Manipulación con software	Descarga y uso no controlado de software
		Manipulación con software	Ausencia de copias de respaldo
		Hurto de medios o documentos	Ausencia de protección físicas de la edificación, puertas y ventanas
		Uso no autorizado del equipo	Falla en la producción de informes de gestión
Red	Medios y Soportes Transmisión pasiva o activa	Negación de acciones	Ausencia de pruebas de envio o recepción de mensajes
		Escucha encubierta	Líneas de comunicación sin protección
		Escucha encubierta	Tráfico sensible sin protección
		Falla del equipo del telecomunicaciones	Conexión deficiente de los cables
		Falla del equipo de telecomunicaciones	Punto único de falla
		Falsificación de derechos	Ausencia de identificación y de autentificación del emisor y receptor
		Espionaje remoto	Arquitectura insegura de la red
		Espionaje remoto	Transferencia de contraseñas en claro
		Saturación del sistema de información	Gestión inadecuada de la red (tolerancia a fallas en el enrutamiento)
		Uso no autorizado del equipo	Conexiones de red pública sin protección
Personal	Persona a cargo de la toma de decisiones Usuarios Personal de operación y mantenimiento Desarrolladores	Incumplimiento en la disponibilidad del personal	Ausencia del personal
		Destrucción de equipos o de medios	Procedimientos inadecuados de contratación
		Error en el uso	Entrenamiento insuficiente en seguridad
		Error en el uso	Uso incorrecto de software y hardware
		Error en el uso	Falta de conciencia acerca de la seguridad
		Procesamiento ilegal de datos	Ausencia de mecanismos de monitoreo
		Hurto de medios o documentos	Trabajo no supervisado de personal externo de limpieza
		Uso no autorizado del equipo	Ausencia de políticas para uso correcto de los medios de telecomunicaciones y mensajería
Sitio	Ambiente externo Instalaciones Zonas Servicios de comunicación Servicios públicos	Destrucción de equipos o de medios	Uso inadecuado o descuido del control de acceso físico a las edificaciones o los recintos
		Inundación	Ubicación en un área susceptible de inundación
		Pérdida en el suministro de Energía	Red energética inestable
		Hurto de equipo	Ausencia de protección físicas de la edificación, puertas y ventanas
Organización	Autoridades Estructura de la organización	Abuso de los derechos	Ausencia de procedimiento formal para el registro y retiro de usuarios

	Subcontratistas/proveedores	Abuso de los derechos	Ausencia de proceso formal para la revisión (supervisión de los derechos de acceso)
		Abuso de los derechos	Ausencia o insuficiencia de disposición (respecto a la seguridad) en los contratos con los clientes y/o terceras partes
		Abuso de los derechos	Ausencia de procedimiento de monitoreo de los recursos de procesamiento de información
		Abuso de los derechos	Ausencia de auditorías (supervisiones) regulares
		Abuso de los derechos	Ausencia de procedimientos de identificación y valoración de riesgos
		Abuso de los derechos	Ausencia de reporte de fallas en los registros de administradores y operadores
		Incumplimiento en el mantenimiento del sistema de información	Respuesta inadecuada de mantenimiento del servicio
		Incumplimiento en el mantenimiento del sistema de información	Ausencia de acuerdos de nivel de servicio o insuficiencia en los mismos
		Incumplimiento en el mantenimiento del sistema de información	Ausencia de procedimiento de control de cambios
		Corrupción de datos	Ausencia de procedimiento formal para el control de la documentación del SGSI
		Corrupción de datos	Ausencia del procedimiento formal para el registro del SGSI
		Datos provenientes de fuentes no confiables	Ausencia de procedimiento formal para la autorización de la información disponible al público
		Negación de acciones	Ausencia de asignación adecuada de responsabilidades en la seguridad de la información
		Falla del equipo	Ausencia de planes de contingencia
		Error en el uso	Ausencia de políticas de correo electrónico
		Error en el uso	Ausencia de procedimientos para la introducción del software en los sistemas operativos
		Error en el uso	Ausencia de registros en las bitácoras (LOGS) de administrador y operario.
		Error en el uso	Ausencia de procedimientos para el manejo de información clasificada
		Error en el uso	Ausencia de responsabilidades en la seguridad de la información en la descripción de los cargos
		Procesamiento ilegal de datos	Ausencia o insuficiencia en las disposiciones (con respecto a la seguridad de la información) en los contratos con los empleados.
		Hurto de equipo	Ausencia de procesos disciplinarios definidos en el caso de incidentes de seguridad de la información

		Hurto de equipo	Ausencia de política formal sobre la utilización de computadores portátiles
		Hurto de equipo	Ausencia de control de los activos que se encuentran fuera de las instalaciones
		Hurto de medios o documentos	Ausencia o insuficiencia de políticas sobre limpieza de escritorio y de pantalla
		Hurto de medios o documentos	Ausencia de autorización de los recursos de procesamiento de la información
		Hurto de medios o documentos	Ausencia de mecanismos de monitoreo
		Uso no autorizado del equipo	Ausencia de revisiones regulares por parte de la gerencia
		Uso no autorizado del equipo	Ausencia de procedimientos para la presentación de informes sobre las debilidades en la seguridad
		Uso de software falso o copiado	Ausencia de procedimientos del cumplimiento de las disposiciones con los derechos intelectuales

Fuente: Los Autores.

3.1.4.4. Identificación de Impactos

En la siguiente tabla se realiza la Identificación de los impactos que la perdida de confidencialidad, integridad y disponibilidad puede tener sobre estos activos.

Tabla 11. Impacto en la Confidencialidad

Confidencialidad		
Valor	**Descripción**	**Razón**
5	Reservada	Información de alta sensibilidad que debe ser protegida por su relevancia sobre decisiones estratégicas, impacto de negocio, potencial de fraude o requisitos legales, dado su nivel de complejidad y afectación de los procesos misionales de la Alcaldía.
4	Restringida	Información sensible, interna a áreas o proyectos a los que debe tener acceso controlado por seguridad e intereses de la Alcaldía, la difusión a partes no autorizadas interrumpiría varios procesos de la Institución
3	Uso Interno	La información debe mantenerse dentro de la Alcaldía y no debe estar disponible externamente.
2	Sensible Pública	De dominio público, puede ser conocido por los dueños de dicha información.
1	Pública	Puede ser conocida y difundida a terceras partes, su grado de afectación a los procesos de la Institución es muy bajo.

Fuente: Los Autores.

Tabla 12. Impacto en la Disponibilidad

Disponibilidad		
Valor	**Descripción**	**Razón**
5	Muy Crítico	Total grado de afectación en las operaciones de la Alcaldía si la información no se encontrara disponible, el activo esta sin funcionamiento por menos de 1 hora.
4	Crítico	Alto grado de afectación en las operaciones de la Institución si la información no se encontrara disponible, el activo puede estar afectado entre 1 y 2 horas.
3	Moderado	De no estar la información disponible, se afectarían algunos procesos de la Alcaldía. El activo puede estar sin funcionamiento entre 3 y 5 horas.
2	Leve	Bajo grado de afectación en las operaciones de la Alcaldía. El activo puede estar sin funcionamiento entre 6 y 8 horas
1	Muy Leve	De no estar disponible la información el grado de afectación en los procesos de la Alcaldía no sería notorio. El activo puede estar sin funcionamiento por más de 8 horas

Fuente: Los Autores.

Tabla 13. Impacto en la Integridad

Integridad		
Valor	**Descripción**	**Razón**
5	Muy Significativa	Alto grado de importancia dada su relación con los procesos de la Institución. La pérdida de Integridad produciría un efecto fatal en la Alcaldía dado que la información no se podrá reconstruir.
4	Significativa	La reconstrucción de la calidad necesaria de la información es compleja y costosa
3	Normal	El grado de importancia afectaría algunos procesos de la Alcaldía, la recuperación de la información se hace de forma fácil con una calidad semejante.
2	Leve	El grado de importancia solo afectaría pocos procesos de la Alcaldía, la información se puede recuperar fácilmente con la misma calidad.
1	Muy leve	No se registran alteraciones en la Alcaldía.

Fuente: Los Autores.

3.1.5. Análisis y evaluación de los riesgos

3.1.5.1. Valoración de impacto

En el anexo 2 se detalla el impacto que podría causar una falla en la seguridad de la información sobre la Alcaldía, valorada en los aspectos de confidencialidad, Disponibilidad e Integridad.

3.1.5.2. Valoración de la probabilidad

Teniendo en cuenta las amenazas, vulnerabilidades e impactos asociados con los activos identificados, se realiza la valoración de la posibilidad de que ocurra una falla en la seguridad. La siguiente tabla describe el grado de probabilidad de ocurrencia:

Tabla 14. Definición niveles de Probabilidad

Valor	NIVEL	Probabilidad	DESCRIPCIÓN
5	**Muy alta**	>80%	Se espera que ocurra en la mayoría de las circunstancias
4	**Alta**	41% al 80%	Probablemente ocurrirá en la mayoría de las circunstancias
3	**Media**	26% al 40%	Se espera que no ocurra regularmente
2	**Baja**	5% al 25%	Pudo ocurrir en algún momento
1	**Raro**	<5%	Puede ocurrir sólo en circunstancias excepcionales

Fuente: Los Autores.

Dado lo anterior se determina el grado de probabilidad de ocurrencia para cada amenaza:

Tabla 15. Probabilidad de Ocurrencia

Amenazas	Probabilidad
Abuso de los derechos	Alta
Corrupción de datos	Baja
Datos provenientes de fuentes no confiables	Baja
Destrucción de equipos o de medios	Baja
Difusión de credenciales de acceso al sistema	Alta
Error en el uso	Alta
Escucha encubierta	Raro
Espionaje remoto	Raro
Falla del equipo	Alta

Falla del equipo del telecomunicaciones	Alta
Falsificación de derechos	Baja
Fenómenos meteorológicos	Raro
Hurto de equipo	Media
Hurto de medios o documentos	Baja
Incumplimiento en el manejo del sistema de información	Media
Incumplimiento en el mantenimiento del sistema de información	Media
Incumplimiento en la disponibilidad del personal	Baja
Inundación	Raro
Mal funcionamiento del software	Media
Manipulación con software	Media
Negación de acciones	Media
Pérdida en el suministro de Energía	Baja
Polvo, corrosión, congelamiento	Baja
Procesamiento ilegal de datos	Baja
Radiación Electromagnética	Baja
Saturación del sistema de información	Muy Alta
Uso de dispositivos de almacenamiento externos	Alta
Uso de software falso o copiado	Media
Uso no autorizado del equipo	Media

Fuente: Los Autores.

Una vez determinado el impacto que puede ocasionar una falla y hallada la posibilidad de su ocurrencia, se realiza la respectiva valoración de riesgo. En el anexo 3 se presenta cada activo valorado para cada amenaza y su posibilidad de ocurrencia.

3.1.5.3. Estimación de los niveles de Riesgo

Dado el resultado obtenido en la valoración del riesgo, se clasifica cada resultado en niveles de riesgo y se agrupan con el fin de obtener el número de incidencias en cada nivel.

Tabla 16. Niveles de Riesgo

Nivel Riesgo	**Rangos NR**	**Frecuencia**
BAJO	1 – 4	408
MODERADO	5—9	362
ALTO	10—16	144
EXTREMO	20—25	20

Fuente: Los Autores.

3.1.5.4. Criterios de Aceptación

La definición de los criterios de aceptación se basa en la recopilación de información de los autores y la política interna de la Alcaldía, con el fin de determinar el grado de aceptación o necesidad de tratamiento del riesgo. Se establecen los siguientes criterios de aceptación, los cuales demarcan las acciones que se deben emprender para cada riesgo evaluado.

Tabla 17. Criterios de Aceptación

Extremo	El riesgo es inaceptable, es aconsejable eliminar la actividad que genera el riesgo en la medida de lo posible, de lo contrario se deben implementar controles de prevención para evitar la probabilidad del riesgo y de protección para disminuir el impacto.
Alto	Se deben diseñar planes de contingencia para protegerse en caso de su ocurrencia como transferir a partes externas los riesgos de la Alcaldía.
Moderado	Se deben tomar medidas para llevar el riesgo en lo posible a la zona

	de riesgo bajo, mediante la implementación de controles.
Bajo	El riesgo se encuentra en un nivel que se puede aceptar sin tomar otras medidas de control diferentes a las que se poseen.

Fuente: Los Autores.

3.1.6. Opciones de tratamiento

Las opciones de tratamiento del riesgo se determinan según el siguiente criterio, teniendo en cuenta el nivel en el cual el riesgo ha sido clasificado.

Tabla 18. Opciones de tratamiento

Extremo	Evitar
Alto	Transferir
Moderado	Reducir
Bajo	Aceptar

Fuente: Los Autores.

- Evitar el Riesgo: Los riesgos identificados se consideran muy altos, Se deben modificar las actividades que lo originan por medio de la eliminación de la actividad o mediante el cambio de las condiciones bajo las cuales se efectúan las actividades.
- Trasferir: Se acude a esta opción cuando los niveles de riesgo son muy altos, y su reducción es difícil para la organización. No resulta económicamente factible implementar controles para disminuir los factores de riesgo, por la tanto es necesario tomar la decisión de compartir algunos riesgos con partes externas. La trasferencia del riesgo puede crear riesgos nuevos o modificar los riesgos identificados existentes.
- Reducir: El nivel de riesgo se debe reducir por medio de la implementación de controles, de manera que el riesgo residual se pueda considera con aceptable.

- Aceptar: Si el nivel de riesgo satisface los criterios para su aceptación, no es necesario implementar controles adicionales, es riesgo se acepta.

3.1.7. Objetivos de Control y Controles de Tratamiento del Riesgo

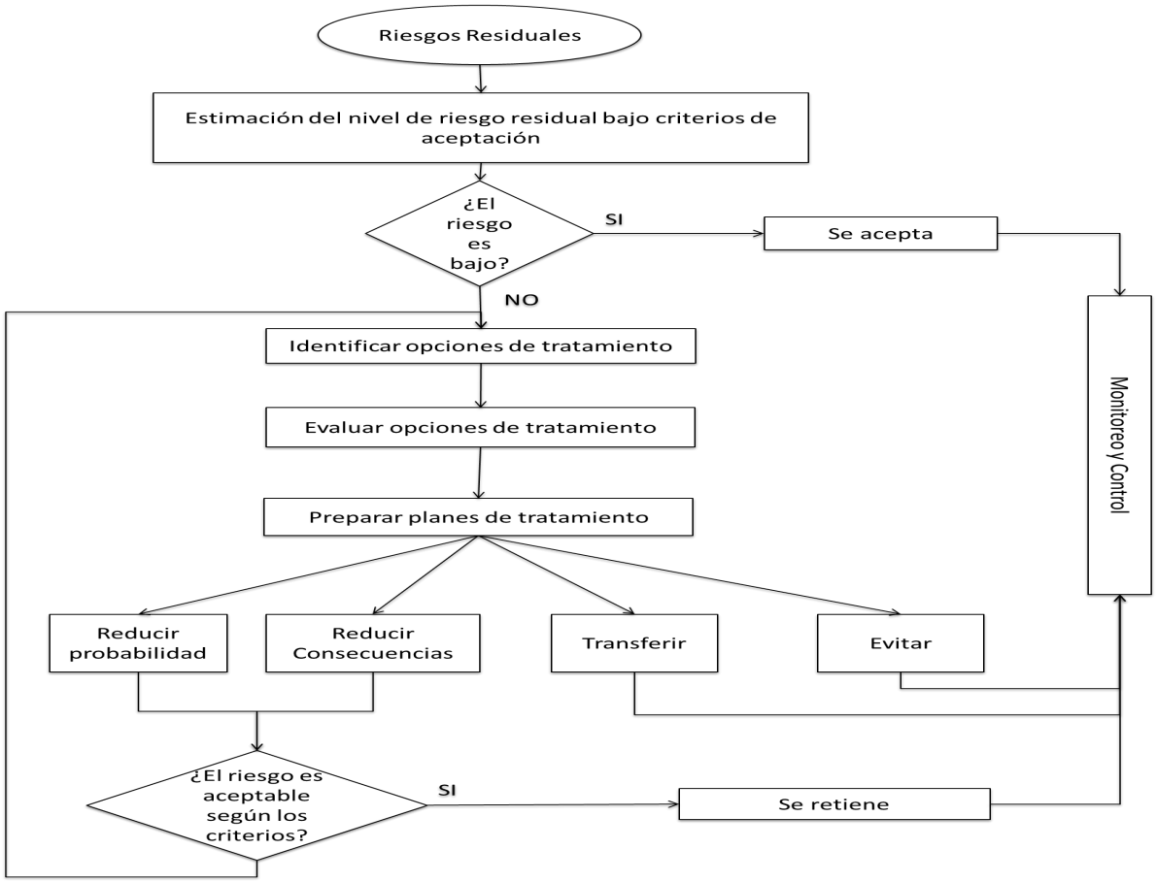
Los objetivos de control sugeridos en el Anexo A de la norma ISO 27001, proporcionan asesoría y orientación sobre las mejores prácticas y se deben seleccionar como parte del proceso de SGSI expresado en su numeral 4.2.1. Por ende especifica las áreas donde es necesario mantener un adecuado control de seguridad y cumplir con el objeto de mantener la confidencialidad, integridad y disponibilidad de la información.

En el anexo 4 se presenta una tabla con los controles expuestos en la norma ISO 27001, mediante la declaración de aplicabilidad para la alcaldía de Floridablanca, exponiendo los controles seleccionados, los controles implementados actualmente y los cuales fueron excluidos del proceso con su respectiva justificación.

3.1.8. Proceso de aprobación de la Dirección sobre los riesgos residuales

Los riesgos de seguridad de la información son riesgos de negocio por lo que soló la dirección tiene la facultad de tomar decisiones sobre su aceptación o tratamiento. Luego de fijar la metodología para la gestión del riesgo en la Alcaldía para su respectiva aceptación, se describe el siguiente diagrama de flujo donde se presenta las actividades en las que participa el riesgo una vez que ha sido tratado.

Figura 4. Proceso de aprobación de la Dirección sobre los riesgos residuales



Fuente: Los Autores

La figura 4 describe, las actividades por las que el riesgo residual debe ser sometido para que sea aceptado por la dirección, teniendo en cuenta aspectos

como su factibilidad en costos y beneficios, recomendaciones de estrategias de tratamiento alineadas con el SGSI y criterios establecidos anteriormente. Dado que, el riesgo residual es el que queda (aún después de aplicar controles) y el "riesgo cero" no existe, el proceso de aprobación centra su base en el proceso de monitoreo y control de los riesgos que han sido gestionados.

3.1.9. Proceso de autorización de la dirección para implementar y operar el SGSI

Listado de requisitos exigidos por la dirección para la implementación y operación del SGSI

- ✓ Declaración de la política
- ✓ Declaración de los Objetivos
- ✓ Declaración del Alcance
- ✓ Declaración de los procedimientos y controles de apoyo
- ✓ Descripción de la metodología de valoración de riesgos
- ✓ Plan de tratamiento de riesgos
- ✓ Registros
- ✓ Declaración de aplicabilidad

3.2. SEGUIMIENTO Y REVISIÓN DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN

La etapa de seguimiento y revisión corresponde a los procesos que permiten verificar el rendimiento del SGSI en la alcaldía. En esta etapa se obtienen datos de eficiencia sobre los controles implementados permitiendo hacer mejorías al plan de gestión. La siguiente figura representa el flujo de proceso de la Alcaldía para realizar el respectivo Seguimiento y revisión al SGSI.

Figura 5. Etapas del proceso de seguimiento y revisión del SGSI

Fuente: Los Autores

3.2.1. Ejecutar procedimientos de monitoreo

El resultado de la aplicación de procedimientos de monitoreo debe incluir cualquier decisión y acción relacionada con:

- ✓ La detección de errores en los resultados del procesamiento de información.
- ✓ La identificación de incidentes e intentos de violación en la seguridad de la información.
- ✓ La determinación de si las actividades de seguridad se ejecutan correctamente.
- ✓ La detección de eventos de seguridad.
- ✓ La determinación de la eficacia de las acciones de seguridad implementadas.

3.2.2. Revisar regularmente la eficacia del SGSI

El insumo del proceso de revisión de la eficacia debe incluir:

- ✓ Resultados de auditorías y revisiones del SGSI
- ✓ Relación de incidentes
- ✓ Retroalimentación de las partes interesadas
- ✓ Técnicas, productos o procedimientos, que podrían utilizarse en la entidad para mejorar el desempeño y la eficacia del SGSI
- ✓ Estado de las acciones preventivas y correctivas
- ✓ Vulnerabilidades o amenazas no tratadas adecuadamente en la evaluación de riesgos anterior
- ✓ Resultados de mediciones de la eficacia
- ✓ Acciones de seguimiento y revisión usadas por la dirección anteriormente
- ✓ Cambios que podrían afectar el SGSI
- ✓ Recomendaciones para la mejora

Las revisiones de la eficacia traen como resultado:

- ✓ La verificación del cumplimiento de la política y objetivos de seguridad de la entidad
- ✓ La revisión de los controles de seguridad implementados

3.2.3. Medir la eficacia de los controles implementados

La eficacia se mide mediante el análisis de indicadores, cada indicador constara de ocho componentes básicos[8]:

a) Nombre del indicador: Se debe seleccionar un nombre significativo, no excesivamente largo, que de una idea de cuál es la medición que se está realizando.

[8]UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA. Implementar el plan de SGSI ISO 27001. [En línea]. Disponible en <http://datateca.unad.edu.co/contenidos/233003/modulo/modulo-233003-online/512_fase_2_hacer_implantar_el_plan_de_sgsi.html>

b) Descripción del indicador: Explicación del objetivo de medida de dicho indicador.

c) Control de seguridad que respalda: A que control o controles está dando cobertura.

d) Fórmula de medición: Descripción de la fórmula aplicada para obtener la medición. Es importante que los parámetros que intervienen sean concretos y no se presten a ambigüedad.

e) Unidades de medida: las unidades de medida deben estar claramente especificadas.

f) Frecuencia de medición: Cada cuánto se debe recoger la medición. Es posible establecer una frecuencia inicial durante un período de tiempo, y una frecuencia posterior mayor (por ejemplo, quincenal los tres primeros meses, y mensual a partir del cuarto mes). En cualquier caso, la frecuencia dependerá de la variabilidad en el tiempo de la medición.

g) Cuando sea posible, valor objetivo y valor umbral, es decir cuál es el valor que sería correcto para la compañía y cuál es el valor por debajo del cual se debiera levantar una alarma.

h) Responsable de la medida: Sobre quién o, preferiblemente, sobre qué cargo recae la responsabilidad de proporcionar el resultado de la medida

3.2.4. Revisar la valoración de los riesgos a intervalos planificados

El insumo del proceso de revisión debe incluir:

- ✓ Los cambios que se han presentado en la organización
- ✓ Los cambios en la tecnología
- ✓ Los cambios en los objetivos y procesos del negocio
  a. Amenazas identificadas
  b. Eficacia de los controles implementados

c. Eventos externos

La revisión de la valoración de los riesgos trae como resultado la evaluación de los parámetros establecidos con anterior en cuanto a:

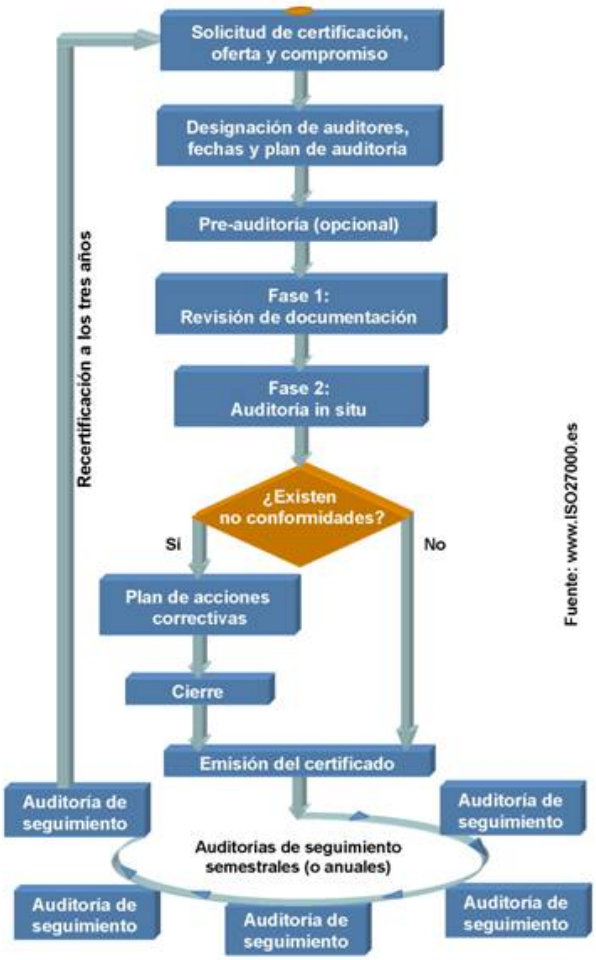
- ✓ Los niveles de riesgo residual
- ✓ Los niveles de riesgo aceptable

3.2.5. Realizar auditorías internas del SGSI

Este proceso incluye las siguientes actividades:

- ✓ Realizar listados de todos los controles a revisar
- ✓ Identificar los aspectos del sistema que necesitan ser analizados
- ✓ Realizar revisiones sobre el sistema
- ✓ Identificar mejoras del sistema
- ✓ Priorizar de acuerdo a la gravedad las mejoras identificadas

Figura 6. Diagrama del proceso de auditoría y certificación



Fuente: Diagrama del proceso de auditoría y certificación, <http://es.scribd.com/doc/115521165/IMPLEMENTACION-DE-UN-SGSI>

3.2.6. Realizar revisiones del SGSI por parte de la dirección

Los principales objetivos de las revisiones por parte de la dirección son:

- Verificar el alcance del SGSI definido
- Identificar mejoras del SGSI

El insumo para la revisión gerencial debe incluir[9]:

- ✓ Informes de auditorías internas del SGS
- ✓ Incidencias detectadas
- ✓ Informes del comité de gestión de seguridad de la información
- ✓ Informes de acciones realizadas por parte de los actores involucrados en el sistema
- ✓ Estado de las incidencias reportadas y la solución dada a las mismas
- ✓ Revisión de los objetivos propuestos en cada fase así como el grado de cumplimiento de los mismos
- ✓ Resumen de los cambios sufridos en la organización

El resultado debe incluir cualquier decisión y acción relacionada con lo siguiente:

- ✓ Mejoramiento de la efectividad del SGSI
- ✓ Actualización de la evaluación del riesgo y el plan de tratamiento del riesgo
- ✓ Modificación de procedimientos y controles que afectan la seguridad de la información, para responder a eventos internos o externos que pudieran tener impacto sobre el SGSI
- ✓ Necesidades de recursos
- ✓ Mejoramiento de la medición de efectividad de los controles

3.2.7. Actualizar los planes de seguridad

Posterior a las revisiones es necesario actualizar:

- ✓ Políticas
- ✓ Procedimientos
- ✓ Planes
- ✓ Revisión y programación de auditorias

[9]INSTITUTO NACIONAL DE DE TECNOLOGIAS DE LA COMUNICACIÓN. Implantación de un SGSI en la empresa. [En línea]. Disponible en <http://cert.inteco.es/extfrontinteco/img/File/intecocert/sgsi/img/Guia_apoyo_SGSI.pdf>

3.2.8. Registrar las acciones y eventos que impacten el desempeño del SGSI

Las acciones de mejora del desempeño del SGSI son de dos tipos:

- Mejoras del sistema
- Mejoras para subsanar incidentes encontrados

Es necesario que el registro de mejoras incluya la siguiente información:

- ✓ Mejoras que se llevaran a cabo
- ✓ Repercusión económica de la aplicación de la mejora
- ✓ Repercusión laboral en la entidad debida a la aplicación de la mejora

3.3. MANTENIMIENTO Y MEJORA DEL SGSI

Mantener y mejorar el sistema de gestión es un proceso que itera a lo largo del plan dado que utiliza los resultados obtenidos de la etapa anterior para aplicarlas al sistema de gestión y así complementarlo para su respectivo mejoramiento. A través de acciones correctivas y preventivas e implementando las mejoras identificadas, el ciclo de vida del plan permite ir mejorando el esquema de seguridad implementado.

Figura 7. Etapas del proceso de mantenimiento y mejora del SGSI

Fuente: Los Autores

3.3.1. Implementar las mejoras identificadas en el SGSI

Esta etapa requiere la realización de las siguientes actividades[10]:

- ✓ Establecer un Grupo de trabajo de procesos y mejora continua, el cual será responsable de administrar las mejoras a los procesos, de manera ordenada y orientada al beneficio de la Institución.
- ✓ Registrar en el Repositorio de solicitudes de mejora, las solicitudes recibidas.
- ✓ Elaborar el Informe de análisis de mejoras propuestas, mediante la revisión, análisis, priorización y selección de las solicitudes de mejora de procesos. Para efectuar la selección de dichas solicitudes se considerará lo siguiente:

  a) Menor costo y horas de trabajo.
  b) Mayores beneficios tangibles e intangibles.
  c) Mayor contribución de las mejoras propuestas al cumplimiento de los objetivos.
  d) Menores obstáculos o riesgos potenciales.

- ✓ Documentar las solicitudes de mejoras de procesos como proyectos de implementación de mejora de procesos, conforme a lo establecido, para su evaluación y, en su caso, autorización correspondiente.
- ✓ Ejecutar los proyectos de implementación de mejora de los procesos y dar seguimiento a las “no conformidades” hasta su cierre, así como validar las acciones correctivas implementadas.
- ✓ Elaborar el documento de Resultado de mejoras implementadas, con los datos provenientes de las actividades respectivas.

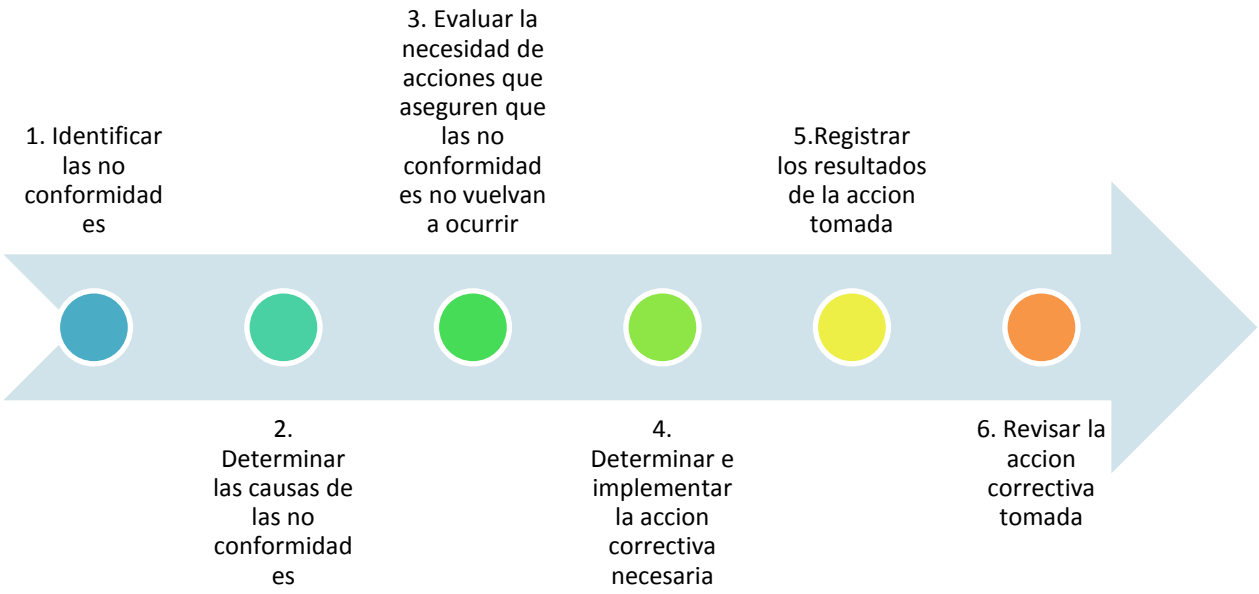
[10]SECRETARIA DE LA FUNCION PÚBLICA. Operación del sistema de gestión y mejora de los procesos de la UTIC. [En línea]. Disponible en <http://www.normateca.gob.mx/Archivos/PTIC/OSGP.htm#c22655dc-16fb-4824-8d70-908d8ce7c188>

- ✓ Iniciar un nuevo ciclo del proyecto de mejora implementado, si las acciones realizadas no tienen el resultado esperado.
- ✓ Integrar la información del resultado de mejoras implementadas a los repositorios de este proceso y asegurarse que dichos resultados se incorporen al Repositorio de conocimiento.
- ✓ Difundir los resultados obtenidos a los involucrados.

3.3.2. Emprender las acciones correctivas y preventivas adecuadas

Las acciones correctivas se aplican con el objetivo de eliminar la causa de no conformidades asociadas a los requisitos del SGSI, para evitar que ocurran nuevamente. El procedimiento para la determinación de las acciones correctivas se presenta a continuación:

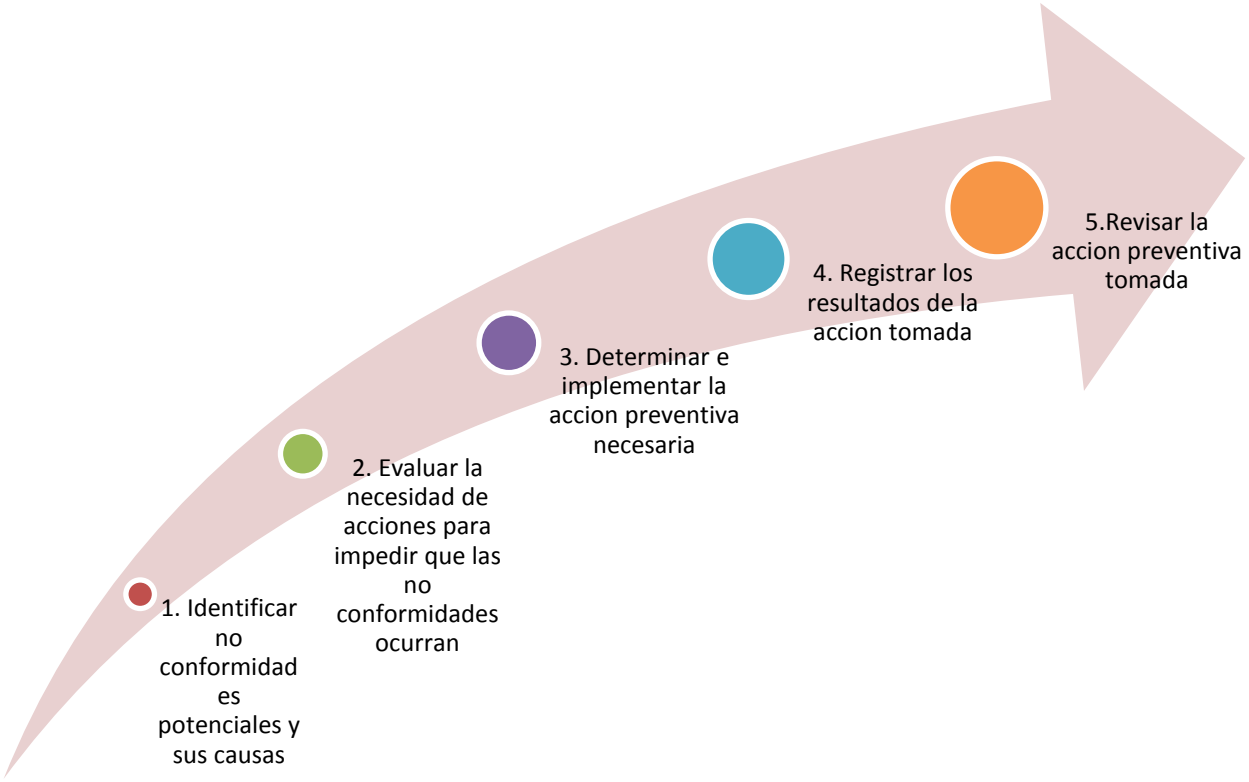
Figura 8. Procedimiento para la acción correctiva



Fuente: Los Autores

Las acciones preventivas tomadas deben ser apropiadas al impacto de los problemas potenciales, el procedimiento para la determinación de acciones preventivas es el siguiente:

Figura 9. Procedimiento para la acción preventiva



Fuente: Los Autores

3.3.3. Comunicar las acciones y mejoras a las partes interesadas

Debe incluir:

- ✓ El nivel de detalle apropiado
- ✓ Los acuerdos de la forma en que procederán las partes interesadas

3.3.4. Asegurar que las mejoras logren los objetivos previstos

Es necesario tener claridad sobre los objetivos que se alcanzarán con la implantación de las mejoras en el SGSI, adicionalmente se sitúan diferentes tipos de indicadores, de acuerdo a la naturaleza del elemento medido; esto permitirá evaluar el cumplimiento del objetivo específico con respecto a la mejora implementada.

En el caso de que la mejora implementada no permita llegar al cumplimiento del objetivo, es necesario iniciar un nuevo ciclo del proyecto de mejora implementado, ya que las acciones realizadas no arrojaron el resultado esperado.

4. PLAN DE GESTIÓN DEL PROYECTO

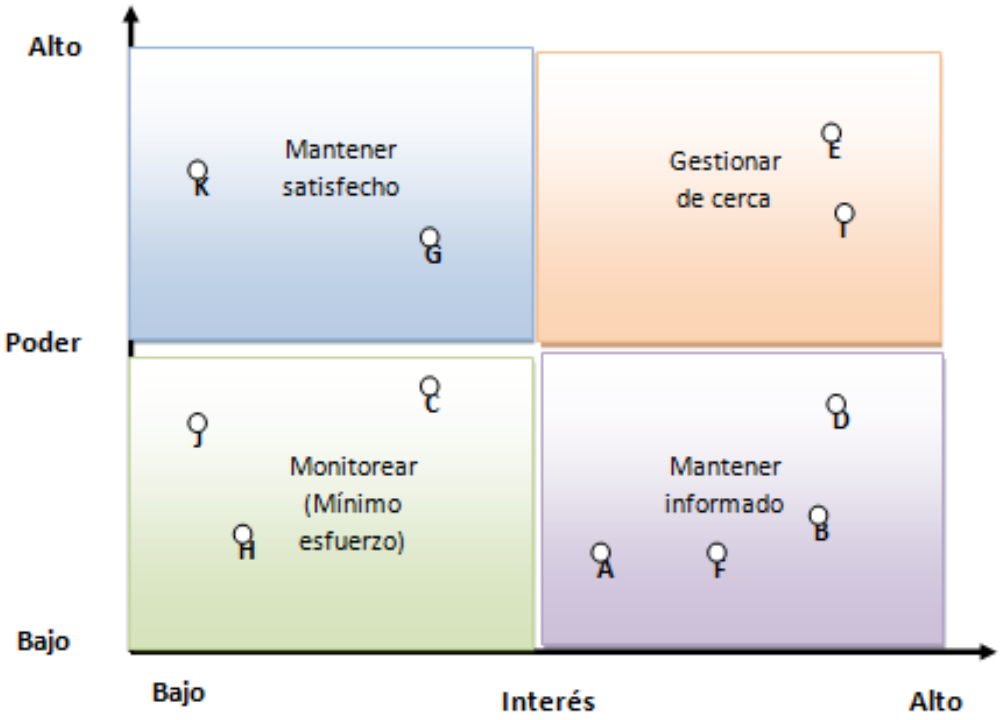
4.1. IDENTIFICAR LOS INTERESADOS

Es el proceso de identificar las personas, grupos u organizaciones que podría afectar o ser afectados por una decisión, actividad o resultado del proyecto; a continuación se mencionan los principales interesados del proyecto:

A. Alcaldía de Floridablanca
B. Comunidad
C. Servidores públicos
D. Equipo del proyecto
E. Director del proyecto
F. Oficina de sistemas
G. Secretarias de la Alcaldía
H. Proveedores
I. Autoridad municipal
J. Entidades descentralizadas
K. Entidades de control

La siguiente matriz resume de una forma gráfica el grado de poder/interés de cada uno de los interesados en el proyecto:

Figura 10. Matriz poder/interés con interesados



Fuente: Los Autores

4.2. RECOPILAR REQUISITOS

Es el proceso de determinar, documentar y gestionar las necesidades y los requisitos de los interesados para cumplir con los objetivos del proyecto.

Los requisitos del producto están contemplados en la norma ISO 27001; esta especifica los requisitos para establecer, implementar, operar, hacer seguimiento, revisar, mantener y mejorar un SGSI dentro del contexto de los riesgos globales de la organización. Especifica los requisitos para la implementación de controles de seguridad adaptados a las necesidades de las organizaciones individuales.

Los requisitos establecidos en la norma son genéricos y están diseñados para ser aplicables a todas las organizaciones, independientemente de su tamaño, naturaleza o tipo.

Adicionalmente los requisitos del proyecto incluyen la determinación de la situación actual de la entidad, junto con la gestión del proyecto por medio de la selección de los grupos de procesos definidos en la guía del PMBOK que se ajustan al proyecto.

4.3. DEFINIR EL ALCANCE

Es el proceso de desarrollar una descripcion detallada del proyecto y del producto.

Descripcion del producto:

Diseñar un Sistema de Gestión de la Seguridad de la Información ISO 27001 para la Alcaldía de Floridablanca para cumplir con los requerimientos de la Ley 1581 del 2012 y con los objetivos estratégicos de la organización.

Inicialmente se analizará la situacion actual en la que se encuentra la entidad en cuanto a la seguridad de la informacion, para posteriormente realizar el establecimiento del sistema de gestion de seguridad de la informacion según los lineamientos de la ISO 27001, la implementacion del sistema no se llevará a cabo debibo a que esta fase se centra en el diseño del sistema de gestion.

El seguimiento y revision del SGSI junto con su mantenimiento y mejora no se llevarán a cabo en esta fase del proyecto por lo que no es comtemplada la implementación, pero se realizará el diseño de estos procesos, lo que permitira tener las bases para llevar a cabo estas etapas posteriormente.

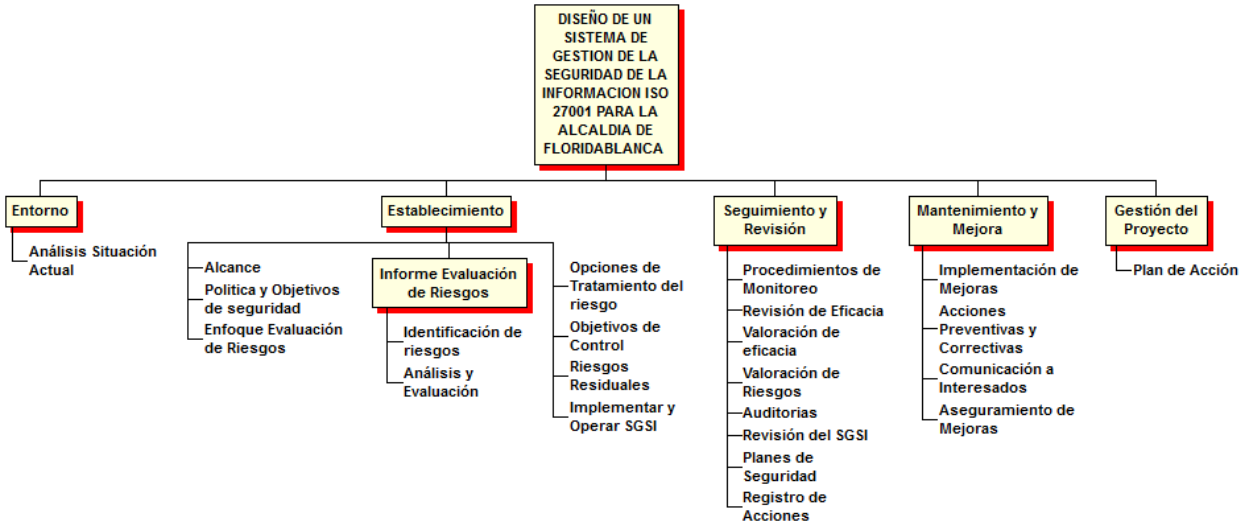
Descripcion del proyecto:

Incluye los procesos seleccionados para llevar a cabo la gestión del proyecto en la etapa de diseño del sistema de gestión de seguridad de la información, entre ellos están:

I. Identificar los interesados del proyecto
II. Recopilar requisitos del proyecto
III. Definir el alcance
IV. Crear la WBS
V. Definir las actividades del proyecto
VI. Establecer la secuencia de las actividades del proyecto
VII. Estimar los recursos de las actividades
VIII. Establecer la duración de la actividades
IX. Establecer el cronograma del proyecto
X. Estimar los costos del proyecto
XI. Determinar el presupuesto del proyecto
XII. Planear la gestión de recursos humanos
XIII. Planificar la gestión de las comunicaciones
XIV. Identificar los riesgos
XV. Realizar el análisis de los riesgos
XVI. Planificar la respuesta a los riesgos

4.4. CREAR LA WBS/EDT

Figura 11. EDT



Fuente: Los Autores

4.5. DEFINIR LAS ACTIVIDADES

Este proceso da a conocer las acciones específicas que se deben realizar para generar los entregables que han sido identificados. La siguiente lista presenta las actividades definidas para cada entregable de proyecto:

1.1. Entorno

1.1.1. Análisis Situación Actual

- ✓ Analizar la estructura organizacional
- ✓ Analizar la Visión
- ✓ Analizar la Misión
- ✓ Analizar la Política de Seguridad
- ✓ Analizar los Objetivos de Calidad
- ✓ Realizar reporte de la situación
- ✓ Analizar el marco legal

1.2. Establecimiento

1.2.1. Alcance

- ✓ Definir el Alcance del SGSI

1.2.2. Política y Objetivos de seguridad

- ✓ Definir la Política de Seguridad
- ✓ Definir los objetivos de seguridad
- ✓ Definir las políticas generales
- ✓ Definir la política de control de acceso
- ✓ Definir la política de correo electrónico
- ✓ Definir la política del uso de Internet
- ✓ Definir política de uso de los sistemas de Información
- ✓ Definir la política para la realización de copias de respaldo

1.2.3. Enfoque Evaluación de Riesgos

- ✓ Establecer la metodología para la evaluación de riesgos
- ✓ Desarrollar criterios para la aceptación de riesgos

1.2.4. Informe Evaluación de Riesgos

1.2.4.1. Identificación de riesgos

- ✓ Identificar los activos dentro del alcance del SGSI
- ✓ Identificar las amenazas de los activos
- ✓ Identificar las vulnerabilidades
- ✓ Identificar los Impactos

1.2.4.2. Análisis y Evaluación

- ✓ Valorar el impacto
- ✓ Valorar la probabilidad de ocurrencia
- ✓ Estimar los niveles de riesgo
- ✓ Determinar la aceptación del riesgo

1.2.5. Opciones de Tratamiento del Riesgo

- ✓ Definir las opciones de tratamiento

1.2.6. Objetivos de Control

- ✓ Seleccionar objetivos de control
- ✓ Elaborar la declaración de aplicabilidad

1.2.7. Riesgos Residuales

- ✓ Desarrollar el proceso para obtener la aprobación de la dirección sobre los riesgos residuales

1.2.8. Implementar y Operar SGSI

- ✓ Definir el listado de requisitos para obtener la aprobación de la dirección para implementar y operar el SGSI

1.3. Seguimiento y Revisión

1.3.1. Procedimientos de Monitoreo

- ✓ Definir requisitos

1.3.2. Revisión de Eficacia

- ✓ Definir procedimiento

1.3.3. Valoración de eficacia

- ✓ Definir procedimiento

1.3.4. Valoración de Riesgos

- ✓ Definir requisitos

1.3.5. Auditorias

- ✓ Definir actividades

1.3.6. Revisión del SGSI

- ✓ Definir procedimiento

1.3.7. Planes de Seguridad

- ✓ Definir planes de actualización

1.3.8. Registro de Acciones

- ✓ Definir procedimiento

1.4. Mantenimiento y Mejora

1.4.1. Implementación de Mejoras

- ✓ Definir actividades

1.4.2. Acciones Preventivas y Correctivas

- ✓ Definir procedimiento

1.4.3. Comunicación a Interesados

- ✓ Definir requisitos

1.4.4. Aseguramiento de Mejoras

- ✓ Definir procedimiento

4.6. ESTABLECER LA SECUENCIA DE LAS ACTIVIDADES

En este proceso se identifica y se documenta las relaciones entre las actividades establecidas para cada entregable. La siguiente tabla presenta las dependencias entre las actividades establecidas según su orden y prioridad:

Tabla 19. Secuencia de las Actividades

Id	Nombre de tarea	Predecesoras
2	**Entorno**	
3	**Análisis Situación Actual**	
4	Analizar la estructura organizacional	
5	Analizar la Visión	4
6	Analizar la Misión	5CC
7	Analizar la Política de Seguridad	6CC
8	Analizar los Objetivos de Calidad	7
9	Realizar reporte de la situación	8
10	Analizar el marco legal	9
11	**Establecimiento**	
12	**Alcance**	
13	Definir el Alcance del SGSI	10
14	**Política y Objetivos de seguridad**	
15	**Definir la Política de Seguridad**	
16	Definir los objetivos de seguridad	13
17	Definir las políticas generales	16
18	Definir la política de control de acceso	17
19	Definir la política de correo electrónico	18
20	Definir la política del uso de Internet	19
21	Definir política de uso de los sistemas de Información	20
22	Definir la política para la realización de copias de respaldo	21
23	**Enfoque Evaluación de Riesgos**	
24	Establecer la metodología para la evaluación de riesgos	22

25	Desarrollar criterios para la aceptación de riesgos	24
26	**Informe Evaluación de Riesgos**	
27	**Identificación de riesgos**	
28	Identificar los activos dentro del alcance del SGSI	25
29	Identificar las amenazas de los activos	28
30	Identificar las vulnerabilidades	29
31	Identificar los Impactos	30
32	**Análisis y Evaluación**	
33	Valorar el impacto	31
34	Valorar la probabilidad de ocurrencia	33
35	Estimar los niveles de riesgo	34
36	Determinar la aceptación del riesgo	35
37	**Opciones de Tratamiento del Riesgo**	
38	Definir las opciones de tratamiento	36
39	**Objetivos de Control**	
40	Seleccionar objetivos de control	38
41	Elaborar la declaración de aplicabilidad	40
42	**Riesgos Residuales**	
43	Desarrollar el proceso para obtener la aprobación de la dirección sobre los riesgos residuales	41
44	**Implementar y Operar SGSI**	
45	Definir el listado de requisitos para obtener la aprobación de la dirección para implementar y operar el SGSI	43
46	**Seguimiento y Revisión**	
47	**Procedimientos de Monitoreo**	
48	Definir requisitos	45
49	**Revisión de Eficacia**	
50	Definir procedimiento	48
51	**Valoración de eficacia**	
52	Definir procedimiento	50
53	**Valoración de Riesgos**	
54	Definir requisitos	52
55	**Auditorias**	
56	Definir actividades	54
57	**Revisión del SGSI**	
58	Definir procedimiento	56

59	**Planes de Seguridad**	
60	Definir planes de actualización	58
61	**Registro de Acciones**	
62	Definir procedimiento	60
63	**Mantenimiento y Mejora**	
64	**Implementación de Mejoras**	
65	Definir actividades	62
66	**Acciones Preventivas y Correctivas**	
67	Definir procedimiento	65
68	**Comunicación a Interesados**	
69	Definir requisitos	67
70	**Aseguramiento de Mejoras**	
71	Definir procedimiento	69

Fuente: Los Autores

4.7. ESTIMAR LOS RECURSOS DE LAS ACTIVIDADES

En este proceso se estima el tipo y cantidades de personas, equipos y materiales requeridos para llevar a cabo las actividades planificadas. En el anexo 5 se presenta una tabla con información detallada de los recursos necesarios para la ejecución de cada actividad programada.

4.8. ESTIMAR LA DURACIÓN DE LAS ACTIVIDADES

En este proceso se realiza la estimación de la cantidad de periodos de trabajo que son necesarios para finalizar las actividades con los recursos asignados. La siguiente tabla presenta la cantidad de tiempo requerido por cada actividad:

Tabla 20. Duración de las Actividades

Nombre de tarea	Duración
Entorno	**23 días**
Análisis Situación Actual	**23 días**
Analizar la estructura organizacional	1 sem
Analizar la Visión	3 días
Analizar la Misión	3 días
Analizar la Política de Seguridad	5 días
Analizar los Objetivos de Calidad	5 días

Realizar reporte de la situación	3 días
Analizar el marco legal	1 sem
Establecimiento	**329 días**
Alcance	**5 días**
Definir el Alcance del SGSI	1 sem
Política y Objetivos de seguridad	**144 días**
Definir la Política de Seguridad	**144 días**
Definir los objetivos de seguridad	10 días
Definir las políticas generales	2 sem.
Definir la política de control de acceso	15 días
Definir la política de correo electrónico	14 días
Definir la política del uso de Internet	12 sem.
Definir política de uso de los sistemas de Información	20 días
Definir la política para la realización de copias de respaldo	15 días
Enfoque Evaluación de Riesgos	**30 días**
Establecer la metodología para la evaluación de riesgos	3 sem.
Desarrollar criterios para la aceptación de riesgos	15 días
Informe Evaluación de Riesgos	**95 días**
Identificación de riesgos	**65 días**
Identificar los activos dentro del alcance del SGSI	4 sem.
Identificar las amenazas de los activos	3 sem.
Identificar las vulnerabilidades	3 sem.
Identificar los Impactos	3 sem.
Análisis y Evaluación	**30 días**
Valorar el impacto	1 sem
Valorar la probabilidad de ocurrencia	2 sem.
Estimar los niveles de riesgo	1 sem
Determinar la aceptación del riesgo	2 sem.
Opciones de Tratamiento del Riesgo	**15 días**
Definir las opciones de tratamiento	15 días
Objetivos de Control	**20 días**
Seleccionar objetivos de control	15 días
Elaborar la declaración de aplicabilidad	5 días
Riesgos Residuales	**10 días**
Desarrollar el proceso para obtener la aprobación de la dirección sobre los riesgos residuales	2 sem.
Implementar y Operar SGSI	**10 días**
Definir el listado de requisitos para obtener la aprobación de la dirección para implementar y operar el SGSI	2 sem.
Seguimiento y Revisión	**40 días**

Procedimientos de Monitoreo	**5 días**
Definir requisitos	1 sem
Revisión de Eficacia	**5 días**
Definir procedimiento	1 sem
Valoración de eficacia	**5 días**
Definir procedimiento	1 sem
Valoración de Riesgos	**5 días**
Definir requisitos	1 sem
Auditorias	**5 días**
Definir actividades	1 sem
Revisión del SGSI	**5 días**
Definir procedimiento	1 sem
Planes de Seguridad	**5 días**
Definir planes de actualización	1 sem
Registro de Acciones	**5 días**
Definir procedimiento	1 sem
Mantenimiento y Mejora	**30 días**
Implementación de Mejoras	**15 días**
Definir actividades	15 días
Acciones Preventivas y Correctivas	**5 días**
Definir procedimiento	1 sem
Comunicación a Interesados	**5 días**
Definir requisitos	1 sem
Aseguramiento de Mejoras	**5 días**
Definir procedimiento	1 sem

Fuente: Ms Project 2010 y Los Autores

4.9. DESARROLLAR EL CRONOGRAMA

Teniendo en cuenta las secuencias de las actividades programadas, las duraciones estimadas, los recursos necesarios, se crea el modelo de programación del proyecto. El Anexo 6 presenta el modelo de programación con las fechas planificadas que indican la iniciación y culminación de cada actividad del proyecto.

4.10. ESTIMAR COSTOS

En este proceso se desarrolla una estimación aproximada de los recursos monetarios necesarios para completar las actividades del proyecto. En las siguientes tablas se presenta el monto de los costos de los recursos y los requeridos para completar el trabajo del proyecto:

4.10.1. Costo de los recursos:

Tabla 21. Costos de los Recursos

Nombre del recurso	Tipo	Iniciales	Capacidad máxima	Tasa estándar
Director del Proyecto	Trabajo	DP	100%	$ 16.600,00/hora
Ingeniero TI 1	Trabajo	I1	100%	$ 13.300,00/hora
Ingeniero TI 2	Trabajo	I2	100%	$ 13.300,00/hora
Ingeniero TI 3	Trabajo	I3	100%	$ 13.300,00/hora

Fuente: Ms Project 2010 y Los Autores

4.10.2. Costo de las Actividades:

Tabla 22. Costo de las Actividades

Nombre de tarea	Costo	Nombres de los recursos
Entorno	**$ 5.397.600,00**	
Análisis Situación Actual	**$ 5.397.600,00**	
Analizar la estructura organizacional	$ 904.000,00	Director del Proyecto;Ingeniero TI 1;Ingeniero TI 2;Ingeniero TI 3
Analizar la Visión	$ 212.800,00	Ingeniero TI 1
Analizar la Misión	$ 212.800,00	Ingeniero TI 2
Analizar la Política de Seguridad	$ 478.400,00	Director del Proyecto;Ingeniero TI 3
Analizar los Objetivos de Calidad	$ 425.600,00	Ingeniero TI 1;Ingeniero TI 2
Realizar reporte de la situación	$ 1.808.000,00	Director del Proyecto;Ingeniero TI 1;Ingeniero TI 2;Ingeniero TI 3
Analizar el marco legal	$ 1.356.000,00	Director del Proyecto;Ingeniero TI 1;Ingeniero TI 2;Ingeniero TI 3
Establecimiento	**$ 57.616.000,00**	
Alcance	**$ 663.999,96**	
Definir el Alcance del SGSI	$ 663.999,96	Director del Proyecto

Política y Objetivos de seguridad	**$ 15.368.000,00**	
Definir la Política de Seguridad	**$ 15.368.000,00**	
Definir los objetivos de seguridad	$ 1.808.000,00	Director del Proyecto;Ingeniero TI 1;Ingeniero TI 2;Ingeniero TI 3
Definir las políticas generales	$ 2.260.000,00	Director del Proyecto;Ingeniero TI 1;Ingeniero TI 2;Ingeniero TI 3
Definir la política de control de acceso	$ 2.260.000,00	Director del Proyecto;Ingeniero TI 1;Ingeniero TI 2;Ingeniero TI 3
Definir la política de correo electrónico	$ 2.260.000,00	Director del Proyecto;Ingeniero TI 1;Ingeniero TI 2;Ingeniero TI 3
Definir la política del uso de Internet	$ 2.260.000,00	Director del Proyecto;Ingeniero TI 1;Ingeniero TI 2;Ingeniero TI 3
Definir política de uso de los sistemas de Información	$ 2.260.000,00	Director del Proyecto;Ingeniero TI 1;Ingeniero TI 2;Ingeniero TI 3
Definir la política para la realización de copias de respaldo	$ 2.260.000,00	Director del Proyecto;Ingeniero TI 1;Ingeniero TI 2;Ingeniero TI 3
Enfoque Evaluación de Riesgos	**$ 6.780.000,00**	
Establecer la metodología para la evaluación de riesgos	$ 4.520.000,00	Director del Proyecto;Ingeniero TI 1;Ingeniero TI 2;Ingeniero TI 3
Desarrollar criterios para la aceptación de riesgos	$ 2.260.000,00	Director del Proyecto;Ingeniero TI 1;Ingeniero TI 2;Ingeniero TI 3
Informe Evaluación de Riesgos	**$ 20.340.000,00**	
Identificación de riesgos	**$ 11.300.000,00**	
Identificar los activos dentro del alcance del SGSI	$ 4.520.000,00	Director del Proyecto;Ingeniero TI 1;Ingeniero TI 2;Ingeniero TI 3
Identificar las amenazas de los activos	$ 2.260.000,00	Director del Proyecto;Ingeniero TI 1;Ingeniero TI 2;Ingeniero TI 3
Identificar las vulnerabilidades	$ 2.260.000,00	Director del Proyecto;Ingeniero TI 1;Ingeniero TI 2;Ingeniero TI 3
Identificar los Impactos	$ 2.260.000,00	Director del Proyecto;Ingeniero TI 1;Ingeniero TI 2;Ingeniero TI 3
Análisis y Evaluación	**$ 9.040.000,00**	
Valorar el impacto	$ 2.260.000,00	Director del Proyecto;Ingeniero TI 1;Ingeniero TI 2;Ingeniero TI 3
Valorar la probabilidad de ocurrencia	$ 2.260.000,00	Director del Proyecto;Ingeniero TI 1;Ingeniero TI 2;Ingeniero TI 3
Estimar los niveles de riesgo	$ 2.260.000,00	Director del Proyecto;Ingeniero TI 1;Ingeniero TI 2;Ingeniero TI 3

Determinar la aceptación del riesgo	$ 2.260.000,00	Director del Proyecto;Ingeniero TI 1;Ingeniero TI 2;Ingeniero TI 3
Opciones de Tratamiento del Riesgo	**$ 3.164.000,00**	
Definir las opciones de tratamiento	$ 3.164.000,00	Director del Proyecto;Ingeniero TI 1;Ingeniero TI 2;Ingeniero TI 3
Objetivos de Control	**$ 6.780.000,00**	
Seleccionar objetivos de control	$ 4.520.000,00	Director del Proyecto;Ingeniero TI 1;Ingeniero TI 2;Ingeniero TI 3
Elaborar la declaración de aplicabilidad	$ 2.260.000,00	Director del Proyecto;Ingeniero TI 1;Ingeniero TI 2;Ingeniero TI 3
Riesgos Residuales	**$ 2.260.000,00**	
Desarrollar el proceso para obtener la aprobación de la dirección sobre los riesgos residuales	$ 2.260.000,00	Director del Proyecto;Ingeniero TI 1;Ingeniero TI 2;Ingeniero TI 3
Implementar y Operar SGSI	**$ 2.260.000,00**	
Definir el listado de requisitos para obtener la aprobación de la dirección para implementar y operar el SGSI	$ 2.260.000,00	Director del Proyecto;Ingeniero TI 1;Ingeniero TI 2;Ingeniero TI 3
Seguimiento y Revisión	**$ 8.588.000,00**	
Procedimientos de Monitoreo	**$ 1.356.000,00**	
Definir requisitos	$ 1.356.000,00	Director del Proyecto;Ingeniero TI 1;Ingeniero TI 2;Ingeniero TI 3
Revisión de Eficacia	**$ 1.356.000,00**	
Definir procedimiento	$ 1.356.000,00	Director del Proyecto;Ingeniero TI 1;Ingeniero TI 2;Ingeniero TI 3
Valoración de eficacia	**$ 1.356.000,00**	
Definir procedimiento	$ 1.356.000,00	Director del Proyecto;Ingeniero TI 1;Ingeniero TI 2;Ingeniero TI 3
Valoración de Riesgos	**$ 1.356.000,00**	
Definir requisitos	$ 1.356.000,00	Director del Proyecto;Ingeniero TI 1;Ingeniero TI 2;Ingeniero TI 3
Auditorias	**$ 904.000,00**	
Definir actividades	$ 904.000,00	Director del Proyecto;Ingeniero TI 1;Ingeniero TI 2;Ingeniero TI 3
Revisión del SGSI	**$ 904.000,00**	
Definir procedimiento	$ 904.000,00	Director del Proyecto;Ingeniero TI 1;Ingeniero TI 2;Ingeniero TI 3
Planes de Seguridad	**$ 452.000,00**	

Definir planes de actualización	$ 452.000,00	Director del Proyecto;Ingeniero TI 1;Ingeniero TI 2;Ingeniero TI 3
Registro de Acciones	**$ 904.000,00**	
Definir procedimiento	$ 904.000,00	Director del Proyecto;Ingeniero TI 1;Ingeniero TI 2;Ingeniero TI 3
Mantenimiento y Mejora	**$ 4.068.000,00**	
Implementación de Mejoras	**$ 1.356.000,00**	
Definir actividades	$ 1.356.000,00	Director del Proyecto;Ingeniero TI 1;Ingeniero TI 2;Ingeniero TI 3
Acciones Preventivas y Correctivas	**$ 904.000,00**	
Definir procedimiento	$ 904.000,00	Director del Proyecto;Ingeniero TI 1;Ingeniero TI 2;Ingeniero TI 3
Comunicación a Interesados	**$ 904.000,00**	
Definir requisitos	$ 904.000,00	Director del Proyecto;Ingeniero TI 1;Ingeniero TI 2;Ingeniero TI 3
Aseguramiento de Mejoras	**$ 904.000,00**	
Definir procedimiento	$ 904.000,00	Director del Proyecto;Ingeniero TI 1;Ingeniero TI 2;Ingeniero TI 3

Fuente: Ms Project 2010 y Los Autores

4.11. DETERMINAR EL PRESUPUESTO

En este proceso se suman los costos estimados de las actividades individuales para establecer una línea base de costos autorizada. En la siguiente tabla se presenta la línea base de costos del proyecto:

Tabla 23. Línea Base de Costos

Nombre de tarea	Costo
Entorno	**$ 5.397.600,00**
Análisis Situación Actual	**$ 5.397.600,00**
Analizar la estructura organizacional	$ 904.000,00
Analizar la Visión	$ 212.800,00
Analizar la Misión	$ 212.800,00
Analizar la Política de Seguridad	$ 478.400,00
Analizar los Objetivos de Calidad	$ 425.600,00
Realizar reporte de la situación	$ 1.808.000,00
Analizar el marco legal	$ 1.356.000,00

Establecimiento	**$ 57.616.000,00**
Alcance	**$ 663.999,96**
Definir el Alcance del SGSI	$ 663.999,96
Política y Objetivos de seguridad	**$ 15.368.000,00**
Definir la Política de Seguridad	**$ 15.368.000,00**
Definir los objetivos de seguridad	$ 1.808.000,00
Definir las políticas generales	$ 2.260.000,00
Definir la política de control de acceso	$ 2.260.000,00
Definir la política de correo electrónico	$ 2.260.000,00
Definir la política del uso de Internet	$ 2.260.000,00
Definir política de uso de los sistemas de Información	$ 2.260.000,00
Definir la política para la realización de copias de respaldo	$ 2.260.000,00
Enfoque Evaluación de Riesgos	**$ 6.780.000,00**
Establecer la metodología para la evaluación de riesgos	$ 4.520.000,00
Desarrollar criterios para la aceptación de riesgos	$ 2.260.000,00
Informe Evaluación de Riesgos	**$ 20.340.000,00**
Identificación de riesgos	**$ 11.300.000,00**
Identificar los activos dentro del alcance del SGSI	$ 4.520.000,00
Identificar las amenazas de los activos	$ 2.260.000,00
Identificar las vulnerabilidades	$ 2.260.000,00
Identificar los Impactos	$ 2.260.000,00
Análisis y Evaluación	**$ 9.040.000,00**
Valorar el impacto	$ 2.260.000,00
Valorar la probabilidad de ocurrencia	$ 2.260.000,00
Estimar los niveles de riesgo	$ 2.260.000,00
Determinar la aceptación del riesgo	$ 2.260.000,00
Opciones de Tratamiento del Riesgo	**$ 3.164.000,00**
Definir las opciones de tratamiento	$ 3.164.000,00
Objetivos de Control	**$ 6.780.000,00**
Seleccionar objetivos de control	$ 4.520.000,00
Elaborar la declaración de aplicabilidad	$ 2.260.000,00
Riesgos Residuales	**$ 2.260.000,00**

Desarrollar el proceso para obtener la aprobación de la dirección sobre los riesgos residuales	$ 2.260.000,00
Implementar y Operar SGSI	**$ 2.260.000,00**
Definir el listado de requisitos para obtener la aprobación de la dirección para implementar y operar el SGSI	$ 2.260.000,00
Seguimiento y Revisión	**$ 8.588.000,00**
Procedimientos de Monitoreo	**$ 1.356.000,00**
Definir requisitos	$ 1.356.000,00
Revisión de Eficacia	**$ 1.356.000,00**
Definir procedimiento	$ 1.356.000,00
Valoración de eficacia	**$ 1.356.000,00**
Definir procedimiento	$ 1.356.000,00
Valoración de Riesgos	**$ 1.356.000,00**
Definir requisitos	$ 1.356.000,00
Auditorias	**$ 904.000,00**
Definir actividades	$ 904.000,00
Revisión del SGSI	**$ 904.000,00**
Definir procedimiento	$ 904.000,00
Planes de Seguridad	**$ 452.000,00**
Definir planes de actualización	$ 452.000,00
Registro de Acciones	**$ 904.000,00**
Definir procedimiento	$ 904.000,00
Mantenimiento y Mejora	**$ 4.068.000,00**
Implementación de Mejoras	**$ 1.356.000,00**
Definir actividades	$ 1.356.000,00
Acciones Preventivas y Correctivas	**$ 904.000,00**
Definir procedimiento	$ 904.000,00
Comunicación a Interesados	**$ 904.000,00**
Definir requisitos	$ 904.000,00
Aseguramiento de Mejoras	**$ 904.000,00**
Definir procedimiento	$ 904.000,00
Total	**$ 75.669.600,00**

Fuente: Ms Project 2010 y Los Autores

4.11.1. Resumen del proyecto programado en tiempo y costos

La siguiente tabla presenta el resumen de la programación del proyecto en tiempo y costos:

Tabla 24. Resumen del proyecto programado en tiempo y costos

Fechas			
Comienzo:	03/02/2014	Fin:	03/09/2014
Comienzo previst	NOD	Fin previsto:	NOD
Comienzo real:	NOD	Fin real:	NOD
Variación de com	0 días	Variación de fin:	0 días
Duración			
Programada:	172,13 días	Restante:	172,13 días
Prevista:	0 días	Real:	0 días
Variación:	172,13 días	Porcentaje completado:	0
Trabajo			
Programado:	5.352 horas	Restante:	5.352 horas
Previsto:	0 horas	Real:	0 horas
Variación:	5.352 horas	Porcentaje completado:	0
Costos			
Programados:	$ 75.669.599,96	Restantes:	$ 75.669.599,96
Previstos:	$ 0,00	Reales:	$ 0,00
Variación:	$ 75.669.599,96		
Estado de las tareas		**Estado de los recursos**	
Tareas aún no	73	Recursos de trabajo:	4
Tareas en curso:	0	Recursos de trabajo sobreasignados	0
Tareas	0	Recursos materiales:	0
Total de tareas:	73	Total de recursos:	4

Fuente: Ms Project 2010 y Los Autores

A continuación se presentan las tablas con las inversiones y gastos de administración requeridos del proyecto en la Alcaldía del Floridablanca:

Tabla 25. Inversiones

Inversiones			
Inversión en activos fijos	**Cantidad**	**Valor Unitario**	**Valor**
Computador Portátil Latitude 14[11]	4	$ 1.654.801	$ 6.619.204
Proyector [12]	1	$ 1.507.753	$ 1.507.753
Disco Externo USB 8 GB[13]	4	$ 14.900	$ 59.600
Norma ISO 27001 versión pdf[14]	2	$ 239.309	$ 478.617
Total Inversiones			$ 8.665.174

Fuente: Los Autores

Tabla 26. Gastos de Administración

Gastos de administración		
Concepto	**Valor mensual**	**Valor Proyectado**
Servicios Públicos	$ 600.000	$ 4.200.000
Papelería	$ 45.000	$ 315.000
Total Gastos de administración		$ 4.515.000

Fuente: Los Autores

Finalmente se obtiene el valor total del presupuesto que requiere el proyecto. Dado que es un proyecto financiado en su totalidad por la Alcaldía de Floridablanca debido a la necesidad identificada de la institución para implantar un

[11] DELL COLOMBIA. Portátil Latitude 3440. [En línea]. Disponible en <http://www.dell.com/co/empresas/p/latitude-3440-laptop/pd>

[12] DELL COLOMBIA. Proyector Dell s320. [En línea]. Disponible en <http://accessories.la.dell.com/sna/productdetail.aspx?c=co&l=es&sku=225-3956&s=bsd&cs=cobsdt1&redirect=1>

[13] FALABELLA. Sandisk Memoria USB 8GB Cruzer Pop Negra. [En línea]. Disponible en <http://www.falabella.com.co/falabella-co/product/1801045/Memoria-USB-8GB-Cruzer-Pop-Negra;jsessionid=9B57D4B218D08AB87A9FBF107495C48D.node24?passedNavAction=push>

[14] INTERNATIONAL ORGANIZATION FOR STANDARDIZATION. Related products. [En línea]. Disponible en <http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=54534>

sistema de gestión de la seguridad de la información ISO 27001, no se espera obtener retorno a la inversión con márgenes de ganancia.

La siguiente tabla presenta el resumen del presupuesto requerido por el proyecto.

Tabla 27. Presupuesto del Proyecto

Presupuesto del Proyecto	
Total Costo de Actividades	$ 75.669.600
Total Inversiones	$ 8.665.174
Total Gastos de administración	$ 4.515.000
Total Presupuesto	$ 88.849.774

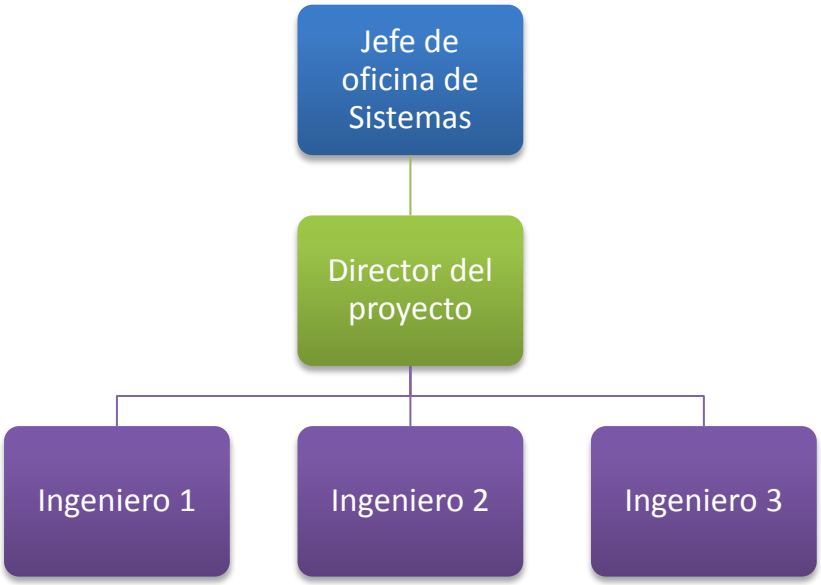
Fuente: Los Autores

4.12. PLANIFICAR LA GESTIÓN DE RECURSOS HUMANOS

Es el proceso de identificar y documentar los roles, responsabilidades, habilidades requeridas y relaciones de reporte dentro del proyecto, así como de crear el plan de gestión de personal.

4.12.1. Organigrama del proyecto:

Figura 12. Organigrama del Proyecto



Fuente: Los Autores

4.12.2. Descripción de roles y responsabilidades:

Tabla 28. Descripción de Roles y Responsabilidades

DESCRIPCION DE ROLES Y RESPONSABILIDADES					
NOMBRE DEL ROL	**RESPONSABILIDADES**	**REPORTA A**	**SUPERVISA A**	**PROFESION**	**CANTIDAD**
JEFE DE OFICINA DE SISTEMAS	Aprobar el Project Charter	Autoridad municipal	Gerente del proyecto	Ingeniero de sistemas	1
	Aprobar el alcance del proyecto				
	Aprobar el cierre del proyecto				
	Revisar los informes				
	Designar al gerente de proyecto				
	Decide sobre la modificación de las líneas base del proyecto				
	Propone e implanta mejoras en el Sistema de gestión de seguridad				
GERENTE DEL PROYECTO	Elaborar el Project Charter	Jefe de oficina de Sistemas	Equipo del proyecto	Ingeniero de sistemas especialista en proyectos	1
	Definir el alcance				
	Establecer con precisión las actividades del proyecto				
	Precisar los recursos humanos y materiales necesarios para culminar				

	el proyecto				
	Elaborar informes de estado del proyecto				
	Realizar reuniones de coordinación semanal				
	Negociar y firmar contrato con los trabajadores				
	coordina y supervisa las actividades que realiza el equipo de trabajo durante la ejecución del proyecto				
	Manejar las restricciones o limitantes del proyecto				
	Gestionar el control de cambios del proyecto				
EQUIPO DEL PROYECTO	Documentación del proyecto	Gerente del proyecto	Trabajadores externos del proyecto	Ingenieros de sistemas / Especialista en seguridad de la información	3
	Elaboración y manejo de listas de control				
	Elaboración de informes				
	Vigilar que el proyecto se desarrolles de acuerdo a los requerimientos				
	Ejecutar el proyecto				
	Solucionar problemas que se puedan presentar durante el desarrollo del proyecto				
	Brindar información para la toma de decisiones				
	Asegurar la actualización y distribución de la información				
	Proponer e implantar mejoras en el Sistema de gestión de seguridad de la información				
	Verifica los lineamientos de planificación y control de tiempo, costos y alcance del proyecto				
	Realiza seguimiento permanente del proyecto				
	Emite, difunde y asegura la aplicación de los planes de seguridad				

Fuente: Los Autores

4.13. PLANIFICAR LA GESTIÓN DE LAS COMUNICACIONES

Es el proceso de desarrollar un enfoque y un plan apropiados para las comunicaciones del proyecto con base en las necesidades y requisitos de información y en los activos organizacionales disponibles.

Información que será comunicada:

- Reportes semanales / Mensuales
- Actas de reuniones internas
- Programación semanal de actividades
- Estado de desarrollo del proyecto
- Solicitudes de cambio
- Aprobación de cambio
- Control presupuestal
- Indicadores de avance

Los métodos utilizados para la transmisión de la información serán:

Medios escritos

- Actas de reunión: Documento emitido en las reuniones ordinarias y extraordinarias, donde se muestra los avances del proyecto, acuerdos aprobados e información de interés con respecto al desarrollo del proyecto.
- Memorandos: Documento o solicitud de información dirigido de manera personalizada.
- Informes o reportes: Que muestran aspectos de interés específico del avance del proyecto.

Medios electrónicos

- Correo electrónico: Permite el envío de cualquier tipo de información referente al proyecto, es uno de los más usados.
- Mensajería instantánea: Permite la rápida comunicación entre dos partes específicas.

Medios verbales:

- Teléfono: Comunicación directa y continua.
- Video conferencia: Comunicación directa que es usada para dar explicación más detallada de asuntos específicos.
- Reuniones: De tipo formal o informal dependiendo los temas del proyecto a debatir.

La siguiente tabla presenta la matriz de comunicación que es llevaba a cabo en el proyecto:

Tabla 29. Matriz de comunicación del proyecto

MATRIZ DE COMUNICACIONES DEL PROYECTO				
INFORMACION COMUNICADA	**RESPONSABLE DE COMUNICAR**	**RECEPTOR DE LA INFORMACION**	**FRECUENCIA DE COMUNICACIÓN**	**METODO DE COMUNICACIÓN**
Compromisos del proyecto	Gerente del proyecto	Equipo del proyecto	Permanentemente	Medios de comunicación formal o informal
Alcance del proyecto	Gerente del proyecto	Equipo del proyecto	Durante la planeación del proyecto	Reuniones, medios de comunicación formal e informal
Responsabilidades del equipo de trabajo	Gerente del proyecto	Equipo del proyecto	Inducciones laborales	Verbal y/o escrito o mediante oficios
Dudas o inquietudes	Equipo del proyecto	Equipo del proyecto	cuando sea necesario	Contacto directo, reuniones
Identificación de nuevas necesidades	Gerente del proyecto	Equipo del proyecto	cuando sea necesario	Reuniones, formato de control de cambios
Indicadores de avance	Gerente del proyecto	Equipo del proyecto	Permanentemente	Reuniones

Designación del gerente del proyecto	Jefe de oficina de sistemas	Gerente del proyecto	Inicialmente	Medios de comunicación formal
Informes del estado del proyecto	Equipo del proyecto	Gerente del proyecto	Permanentemente	Medios de comunicación formal, reuniones
Programación de actividades	Gerente del proyecto	Equipo del proyecto	Permanentemente	Medios de comunicación formal
Modificación de la línea base del proyecto	Jefe de oficina de sistemas	Gerente del proyecto	cuando sea necesario	Reuniones, Medios de comunicación formal
Cronograma del proyecto	Gerente del proyecto	Equipo del proyecto/ Jefe de oficina de Sistemas	Inicialmente	Reuniones, medios de comunicación formal

Fuente: Los Autores

4.14. IDENTIFICAR LOS RIESGOS

Es el proceso de determinar los riesgos que pueden afectar al proyecto y documentar sus características.

Tabla 30. Riesgos del Proyecto

Código del riesgo	Riesgo
R1	Recurso humano no disponible
R2	Cambio de periodo municipal
R3	Falta de recursos financieros
R4	demora en la planificación del proyecto
R5	Mala interpretación en los requerimientos del sistema de gestión
R6	Demora en la contratación del personal
R7	Cambios en la normatividad vigente
R8	Mala interpretación de la norma
R9	Aumento en los costos estimados del proyecto
R10	Aumento en el tiempo estimado de ejecución
R11	Cambios en los requerimientos del proyecto
R12	Oposición de la comunidad
R13	Conflictos sindicales
R14	Restricciones contractuales
R15	Falta de claridad de los Roles y responsabilidades
R16	Alta rotación del personal

R17	Resistencia de los empleados al cambio
R18	Problemas de comunicación en el equipo de proyecto
R19	Cambio en las prioridades estratégicas institucionales
R20	Falta de reportes periódicos
R21	Falta de claridad en el alcance
R22	Falta de aprobación de recursos financieros
R23	Perdida del personal clave del proyecto
R24	Control y seguimiento inadecuado

Fuente: Los Autores

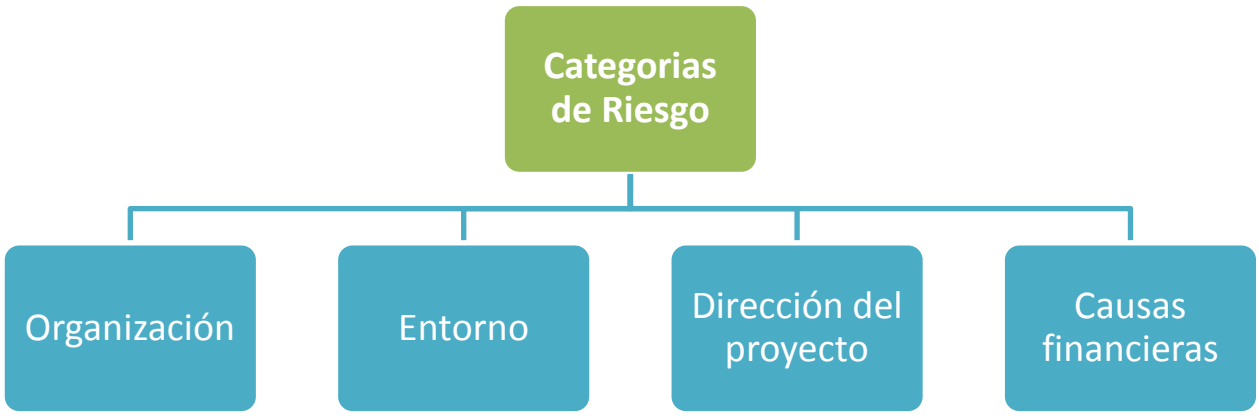
4.15. REALIZAR EL ANÁLISIS CUALITATIVO DE RIESGOS

El proceso de priorizar riesgos para análisis o acción posterior, evaluando y combinando la probabilidad de ocurrencia e impacto de dichos riesgos.

4.15.1. Categoría de riesgo

La siguiente figura presenta las categorías de riesgo del proyecto en las cuales son clasificados los riesgos:

Figura 13. Categoría de riesgos



Fuente: Los Autores

4.15.2. Definición de Probabilidad

Una vez identificada las categorías de riesgo se procede a evaluar la posibilidad realista de que un evento identificado como amenaza se materialice afectando los objetivos del proyecto. La siguiente tabla presenta el cuadro de probabilidad de ocurrencia de un evento:

Tabla 31. Probabilidad

Probabilidad	
Muy alta	>80%
Alta	60% al 80%
Media	36% al 59%
Baja	10% al 35%
Raro	<10%

Fuente: Los Autores

4.15.3. Definición de Impacto

La definición de impacto se realiza bajo dos objetivos definidos en costo y tiempo. La siguiente tabla presenta los niveles identificados:

Tabla 32. Impacto

Impacto	Muy bajo	Bajo	Medio	Alto	Muy alto
Costo	<2%	2%-5%	6%-14%	15%-30%	>30%
Tiempo	<3%	3%-7%	8%-13%	14%-29%	>29%

Fuente: Los Autores

4.15.4. Definición de tolerancia

La siguiente tabla presenta los niveles de tolerancia en los cuales será clasificado cada riesgo identificado.

Tabla 33. Definición Niveles de Tolerancia

Nivel de riesgos o nivel de severidad

Probabilidad						
	Muy Alta	Moderado	Alto	Alto	Extremo	Extremo
	Alta	Bajo	Moderado	Alto	Alto	Extremo
	Media	Bajo	Moderado	Moderado	Alto	Alto
	Baja	Bajo	Bajo	Moderado	Moderado	Alto
	Muy Baja	Bajo	Bajo	Bajo	Bajo	Moderado
		Muy Bajo	Bajo	Medio	Alto	Muy Alto
		Impacto				

Fuente: Los Autores

Extremo	Es aconsejable eliminar la actividad que genera el riesgo en la medida de lo posible, de lo contrario se deben implementar controles de prevención para evitar la probabilidad del riesgo y disminuir el impacto.
Alto	Se deben diseñar planes de contingencia para protegerse en caso de su ocurrencia.
Moderado	Se deben tomar medidas para llevar el riesgo en lo posible a la zona de riesgo bajo, mediante la implementación de controles.
Bajo	El riesgo se encuentra en un nivel que se puede aceptar sin tomar otras medidas de control diferentes a las que se poseen.

Luego de definidas las categorías de riesgo, se realiza la clasificación de cada uno agrupados en cada una. La siguiente tabla presenta la clasificación de los riesgos agrupados por categoría.

Tabla 34. Clasificación de Riesgo por Categoría

Categorías de riesgo	Código del riesgo	Riesgo
Organizacional	R6	Demora en la contratación del personal
Organizacional	R16	Alta rotación del personal
Organizacional	R14	Restricciones contractuales
Organizacional	R1	Recurso humano no disponible
Organizacional	R2	Cambio de periodo municipal
Organizacional	R17	Resistencia de los empleados al cambio
Organizacional	R19	Cambio en las prioridades estratégicas institucionales
Entorno	R12	Oposición de la comunidad
Entorno	R13	Conflictos sindicales

Entorno	R7	Cambios en la normatividad vigente
Dirección del proyecto	R8	Mala interpretación de la norma
Dirección del proyecto	R24	Control y seguimiento inadecuado
Dirección del proyecto	R21	Falta de claridad en el alcance
Dirección del proyecto	R18	Problemas de comunicación en el equipo de proyecto
Dirección del proyecto	R15	Falta de claridad de los Roles y responsabilidades
Dirección del proyecto	R10	Aumento en el tiempo estimado de ejecución
Dirección del proyecto	R4	demora en la planificación del proyecto
Dirección del proyecto	R11	Cambios en los requerimientos del proyecto
Dirección del proyecto	R23	Perdida del personal clave del proyecto
Dirección del proyecto	R20	Falta de reportes periódicos
Dirección del proyecto	R5	Mala interpretación en los requerimientos del sistema de gestión
Causas financieras	R22	Falta de aprobación de recursos financieros
Causas financieras	R9	Aumento en los costos estimados del proyecto
Causas financieras	R3	Falta de recursos financieros

Fuente: Los Autores

4.15.5. Clasificación de riesgo por impacto:

El proceso de evaluación del riesgo consiste en la determinación del impacto que tiene los riesgos sobre el proyecto, a continuación se presenta el impacto en costo y tiempo de cada riesgo en el proyecto

Tabla 35. Impacto en Costo

PROBABILIDAD	**Muy Alta**			R23		
	Alta		R13	R17, R18, R5	R6, R16, R14, R19, R24, R15, R10, R4, R9	R2, R22
	Media			R20	R8, R11	R21, R3
	Baja				R1, R12, R7	
	Muy Baja					
		Muy Baja	**Bajo**	**Medio**	**Alto**	**Muy Alto**

Fuente: Los Autores

Tabla 36. Impacto en Tiempo

PROBABILIDAD	**Muy Alta**				R23	
	Alta		R13	R9	R6, R16, R14, R17, R19, R24, R10, R4, R5, R15	R2, R22
	Media				R8, R11, R20, R21	R3
	Baja				R1, R12	R7
	Muy Baja					
		Muy Baja	**Bajo**	**Medio**	**Alto**	**Muy Alto**

Fuente: Los Autores

4.15.6. Severidad de los riesgos:

Luego de evaluar cada riesgo y determinar su nivel de impacto que estos tienen en el proyecto, se realiza la clasificación con el fin de determinar su nivel de severidad. La siguiente tabla presenta la clasificación de los riesgos organizados según su severidad.

Tabla 37. Severidad de los Riesgos

CODIGO RIESGO	SEVERIDAD/COSTO	SEVERIDAD/TIEMPO
R1	8	8
R2	20	20
R3	15	15
R4	16	16
R5	12	16
R6	16	16
R7	8	10
R8	12	12
R9	16	12

R10	16	16
R11	12	12
R12	8	8
R13	8	8
R14	16	16
R15	16	16
R16	16	16
R17	12	16
R18	12	16
R19	16	16
R20	9	12
R21	15	12
R22	20	20
R23	15	20
R24	16	16

Fuente: Los Autores

4.15.7. Ranking de riesgos por objetivo:

El listado de los riesgos clasificados permite priorizar los riesgos con el fin de identificar en que riesgos se debe prestar mayor atención debido a su nivel de impacto. Las siguientes tablas presentan los ranking establecidos para cada riesgo evaluado en Costo y Tiempo.

Tabla 38. Ranking Costo

CODIGO RIESGO	SEVERIDAD/COSTO
R1	8
R7	8
R12	8
R13	8
R20	9
R5	12
R8	12
R11	12
R17	12
R18	12
R3	15

R21	15
R23	15
R4	16
R6	16
R9	16
R10	16
R14	16
R15	16
R16	16
R19	16
R24	16
R2	20
R22	20

Fuente: Los Autores

Tabla 39. Ranking Tiempo

CODIGO RIESGO	SEVERIDAD/TIEMPO
R1	8
R12	8
R13	8
R7	10
R8	12
R9	12
R11	12
R20	12
R21	12
R3	15
R4	16
R5	16
R6	16
R10	16
R14	16
R15	16
R16	16
R17	16
R18	16

R19	16
R24	16
R2	20
R22	20
R23	20

Fuente: Los Autores

4.15.8. Planificar respuesta a los riesgos

Es el proceso de desarrollar opciones y acciones para mejorar las oportunidades y reducir las amenazas a los objetivos del proyecto.

- ✓ Extremo: Evitar
- ✓ Alto: Transmitir
- ✓ Moderado: Mitigar
- ✓ Bajo: Aceptar

- Evitar el Riesgo: Los riesgos identificados se consideran muy altos, Se deben modificar las actividades que lo originan por medio de la eliminación de la actividad o mediante el cambio de las condiciones bajo las cuales se efectúan las actividades.

- Transmitir: Se acude a esta opción cuando los niveles de riesgo son muy altos, y su reducción es difícil para la organización. No resulta económicamente factible implementar controles para disminuir los factores de riesgo, por la tanto es necesario tomar la decisión de compartir algunos riesgos con partes externas. La trasferencia del riesgo puede crear riesgos nuevos o modificar los riesgos identificados existentes.

- Mitigar: El nivel de riesgo se debe reducir por medio de la implementación de controles, de manera que el riesgo residual se pueda considera como aceptable.

- Aceptar: Si el nivel de riesgo satisface los criterios para su aceptación, no es necesario implementar controles adicionales, es riesgo se acepta.

5. CONCLUSIONES

La definición del alcance que tendría el Sistema de gestión de seguridad de la información ISO 27001 fue clave para lograr el desarrollo de este proyecto, ya que la organización no contaba con la experiencia en el manejo e implantación de un sistema de gestión de seguridad de la información y el tener claramente definido el alcance permite tener un mejor control de las variables.

El diseño del sistema de gestión de seguridad de la información ISO 27001 en la Alcaldía de Floridablanca no se verá reflejado en el crecimiento financiero de la entidad, debido a que se trata de un proyecto de continuidad de negocio, lo que permitirá tener a la entidad un mejor control sobre sus principales activos de información.

El diseño e implantación del sistema de gestión de seguridad de la información debe ir acompaño del compromiso claro de los trabajadores de la entidad, para obtener resultados visibles y lograr el mejoramiento continúo de los controles implementados.

BIBLIOGRAFIA

ALCALDIA DE FLORIDABLANCA. Política de seguridad de la información Alcaldía Municipal de Floridablanca. [En línea]. Disponible en <http://floridablanca.gov.co/wp-content/uploads/2013/06/POLITICA-DE-LA-SEGURIDAD-DE-LA-INFORMACION-1.pdf>

COLOMBIA. CONGRESO DE LA REPÚBLICA. Artículo 15 (Constitución política de Colombia, 1991)

COLOMBIA. CONGRESO DE LA REPÚBLICA. Ley 1581 (17, Octubre, 2012). Por la cual se dictan disposiciones generales para la protección de datos personales. Diario Oficial. Bogotá, D.C., 2012. No 48587.

CONGRESO DE COLOMBIA. Ley estatutaria No. 1581 del 17 de Octubre de 2012. [En línea]. Disponible en <http://www.redipd.org/legislacion/common/legislacion/Colombia/Ley_1581_2012_COLOMBIA.pdf>

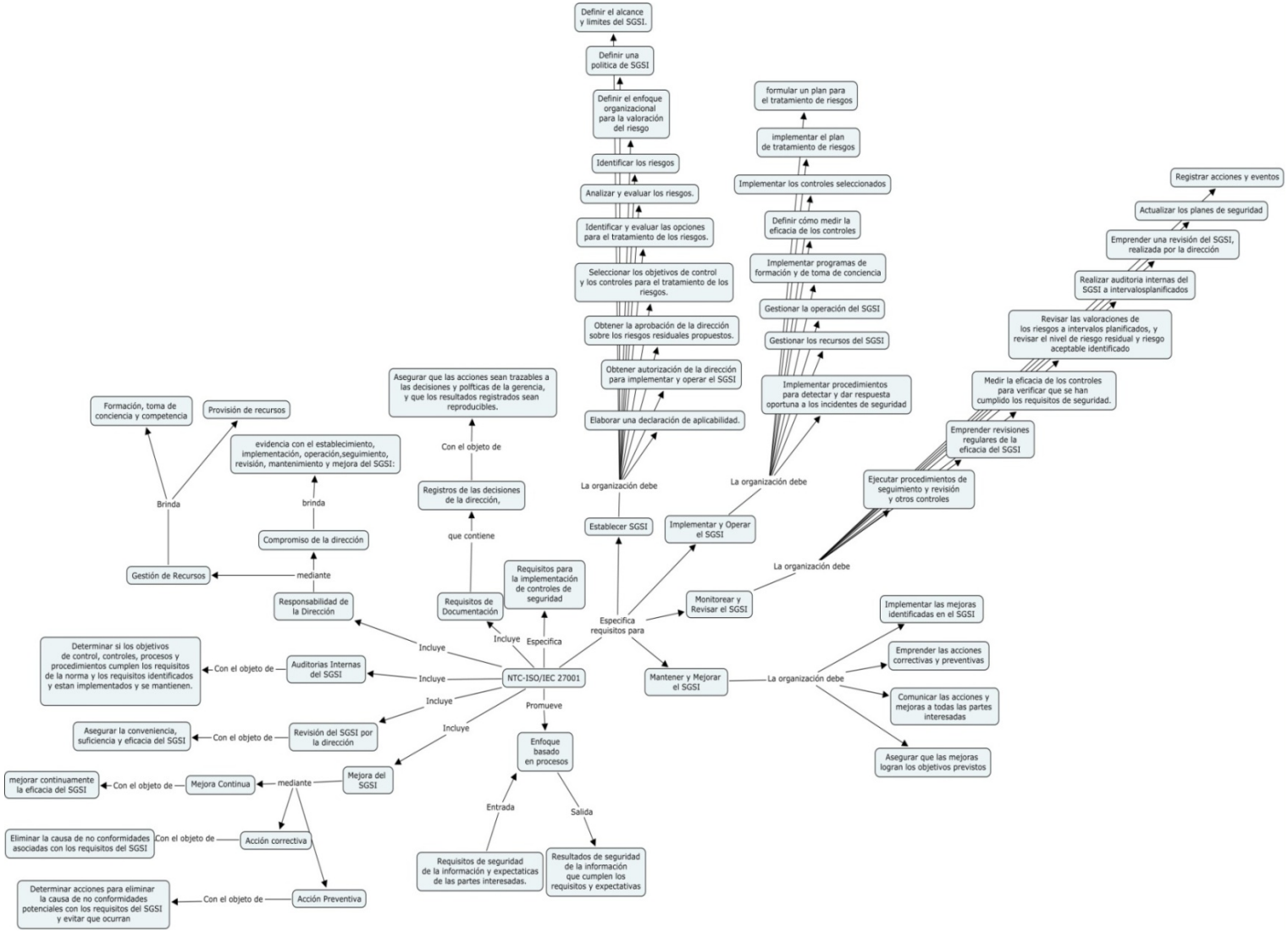
INSTITUTO COLOMBIANO DE NORMALIZACIÓN Y CERTIFICACIÓN. Sistemas de gestión de la seguridad de la información (SGSI). NTC-ISO/IEC 27001. Bogotá D.C.: El instituto, 2006. 46 p.

INSTITUTO NACIONAL DE DE TECNOLOGIAS DE LA COMUNICACIÓN. Implantación de un SGSI en la empresa. [En línea]. Disponible en <http://cert.inteco.es/extfrontinteco/img/File/intecocert/sgsi/img/Guia_apoyo_SGSI.pdf>

SECRETARIA DE LA FUNCION PÚBLICA. Operación del sistema de gestión y mejora de los procesos de la UTIC. [En línea]. Disponible en <http://www.normateca.gob.mx/Archivos/PTIC/OSGP.htm#c22655dc-16fb-4824-8d70-908d8ce7c188>

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA. Implementar el plan de SGSI ISO 27001. [En línea]. Disponible en <http://datateca.unad.edu.co/contenidos/233003/modulo/modulo-233003-online/512_fase_2_hacer_implantar_el_plan_de_sgsi.html>

ANEXO A. MAPA MENTAL ISO 27001



ANEXO B. VALORACION DEL IMPACTO

Activo	Impacto en la Confidencialidad	Impacto en la Disponibilidad	Impacto en la Integridad	Valor del Activo
Computadores portátiles	3	3	3	3
Computadores de escritorio	3	3	3	3
Servidor de software GD	5	4	5	5
Servidor de software Distrito	5	4	5	5
Servidor de telefonía IP	4	4	5	4
Servidor de Correo institucional	3	4	5	4
Impresoras	3	4	2	3
Scanner	3	2	1	2
Discos removibles	3	1	1	2
CD-Rom	3	1	1	2
Discos duros removibles	3	2	1	2
Memorias removibles	3	1	1	2
DVDs	3	1	1	2
Papeles	3	3	3	3
Fax	3	1	1	2
Transparencias	3	1	1	2
Teléfonos IP	3	3	2	3
Teléfonos convencionales	3	3	1	2
Fotocopiadoras	3	3	2	3
Contratos	4	2	3	3
Acuerdos	2	2	3	2
Comunicados	2	2	3	2
Actas	2	2	3	2
Documentos de procesos	3	2	3	3

Facturas	4	2	3	3
Recibos	4	2	3	3
Memorandos	3	2	3	3
Oficios	3	2	3	3
Reglamentos	3	1	3	2
Manuales de usuarios	3	2	3	3
Documentación del sistema	4	2	4	3
Evidencias de auditorias	3	2	3	3
Documentación almacenada en archivos	4	4	4	4
Planes de mejoramiento	4	2	3	3
Correspondencia	4	2	4	3
Windows server 2008	1	1	1	1
Windows XP Profesional SP 3	1	3	1	2
Windows 7 Ultimate	1	3	1	2
Windows 8	1	3	1	2
Antivirus ESET NOD 32	1	1	1	1
Ccleaner	1	1	1	1
Microsoft Project	1	1	1	1
Nero	1	1	1	1
Adobe Reader	1	1	1	1
Microsoft Office	1	4	1	2
Microsoft Visio	1	1	1	1
WinRar	1	1	1	1
Autocad	1	1	1	1
TeamViewer	1	1	1	1
Mozilla Thunderbird	1	3	1	2
PosgreSQL	1	1	1	1
Skype	1	1	1	1

NetBeans	1	2	1	1
Microsoft Visual basic 6.0	1	2	1	1
MySql	1	2	1	1
Eclipse	1	2	1	1
Delfin Gd	4	5	1	3
Chip (Hacienda)	3	3	1	2
MGA	3	3	1	2
Distrito	5	5	4	5
Página web de la Entidad	1	4	4	3
Aplicación Web de cuentas	4	4	4	4
Aplicación Web de ventanilla unica	4	4	4	4
Aplicación web de Manejo de Cartera	4	4	4	4
Aplicación Web de Alumbrado Publico	4	4	4	4
Intranet Institucional	4	3	4	4
Correo institucional	3	3	4	3
Aplicación web DIAN	4	4	4	4
Red pública de conmutación telefónica	3	3	3	3
Ethernet	3	5	3	4
GigabitEthernet	3	5	3	4
Línea de suscriptor digital asimétrica (ASDL)	3	4	3	3
WiFi 802.11	3	3	3	3
Modems	3	5	3	4
Switch	3	5	4	4
Routers	3	5	4	4
PBX	3	4	4	4
Alcalde	3	1	1	2

Secretaría general	3	3	1	2
Secretaría de Hacienda	3	3	1	2
Secretaría de infraestructuta	3	3	1	2
Secretaría de desarrollo economico y social	3	3	1	2
Secretaría de educacion	3	3	1	2
Secretaría de gobierno	3	3	1	2
Secretaría de salud	3	3	1	2
Oficina de control interno	3	3	1	2
Oficina de contratación	3	3	1	2
Oficina de control interno disciplinario	3	3	1	2
Oficina asesora jurídica	3	3	1	2
Oficina asesora de planeación	3	3	1	2
Administrador del sistema	3	3	1	2
Funcionarios a cargo de copias de seguridad	3	3	1	2
Jefe de Oficina	3	3	1	2
Desarrolladores de aplicación	3	3	1	2
Domicilios del personal	1	1	1	1
Instalaciones de otras organizaciones	1	1	1	1
Ambiente Fuera de la Alcaldía	1	1	1	1
Establecimiento	1	3	4	3
Edificaciones	1	3	4	3
Oficina	2	3	4	3
Zonas de acceso reservado	3	2	4	3
Líneas telefónicas	3	3	3	3

Internet	1	5	3	3
Redes telefónicas internas	3	3	3	3
Suministro de energía	1	5	3	3
Suministro de agua	1	4	3	3
Disposición de residuos	1	2	3	2
Despacho	1	3	1	2
Secretarías	1	3	1	2
Contratistas	1	3	1	2

Fuente: Los Autores.

ANEXO C. VALORACION DEL RIESGO

	MAPA DE RIESGOS																												
	AMENAZAS	Abuso de los derechos	Corrupción de datos	Datos provenientes de fuentes no confiables	Destrucción de equipos o de medios	Difusión de credenciales de acceso al sistema	Error en el uso	Escucha encubierta	Espionaje remoto	Falla del equipo	Falla del equipo del telecomunicaciones	Falsificación de derechos	Fenómenos meteorológicos	Hurto de equipo	Hurto de medios o documentos	Incumplimiento en el manejo del sistema de información	Incumplimiento en el mantenimiento del sistema de información	Incumplimiento en la disponibilidad del personal	Inundación	Mal funcionamiento del software	Manipulación con software	Negación de acciones	Pérdida en el suministro de Energía	Polvo, corrosión, congelamiento	Procesamiento ilegal de datos	Radiación Electromagnética	Saturación del sistema de información	Uso de dispositivos de almacenamiento externos	Uso de software falso o copiado	Uso no autorizado del equipo
	PROB. OCURRENCIA (P)	5	2	2	2	4	4	1	1	4	4	2	1	3	2	3	3	2	1	3	3	3	2	2	2	2	5	4	3	3
ACTIVO DE INFORMACIÓN	**IMPACTO (I)**																													
Computadores portátiles	3				6		12						3		6	9							6	6		6		12		

Computadores de escritorio	3				6		12					3	6	9						6	6		6		12		
Servidor de software GD	5				10		20					5	10	15						10	10		10		20		
Servidor de software Distrito	5				10		20					5	10	15						10	10		10		20		
Servidor de telefonía IP	4				8		16					4	8	12						8	8		8		16		
Servidor de Correo institucional	4				8		16					4	8	12						8	8		8		16		
Impresoras	3				6		12					3	6	9						6	6		6		12		
Scanner	2				4		8					2	4	6						4	4		4		8		
Discos removibles	2				4		8					2	4	6						4	4		4		8		
CD-Rom	2				4		8					2	4	6						4	4		4		8		
Discos duros removibles	2				4		8					2	4	6						4	4		4		8		
Memorias removibles	2				4		8					2	4	6						4	4		4		8		
DVDs	2				4		8					2	4	6						4	4		4		8		
Papeles	3				6		12					3	6	9						6	6		6		12		
Fax	2				4		8					2	4	6						4	4		4		8		
Transparencias	2				4		8					2	4	6						4	4		4		8		
Teléfonos IP	3				6		12					3	6	9						6	6		6		12		
Teléfonos convencionales	2				4		8					2	4	6						4	4		4		8		
Fotocopiadoras	3				6		12					3	6	9						6	6		6		12		
Contratos	3				6		12					3	6	9						6	6		6		12		
Acuerdos	2				4		8					2	4	6						4	4		4		8		

Comunicados	2				4		8					2	4	6						4	4		4		8					
Actas	2				4		8					2	4	6						4	4		4		8					
Documentos de procesos	3				6		12					3	6	9						6	6		6		12					
Facturas	3				6		12					3	6	9						6	6		6		12					
Recibos	3				6		12					3	6	9						6	6		6		12					
Memorandos	3				6		12					3	6	9						6	6		6		12					
Oficios	3				6		12					3	6	9						6	6		6		12					
Reglamentos	2				4		8					2	4	6						4	4		4		8					
Manuales de usuarios	3				6		12					3	6	9						6	6		6		12					
Documentación del sistema	3				6		12					3	6	9						6	6		6		12					
Evidencias de auditorias	3				6		12					3	6	9						6	6		6		12					
Documentación almacenada en archivos	4				8		16					4	8	12						8	8		8		16					
Planes de mejoramiento	3				6		12					3	6	9						6	6		6		12					
correspondencia	3				6		12					3	6	9						6	6		6		12					
Windows server 2008	1	5	2			4	4					2			2					3	3				2			4		3
Windows XP Profesional SP 3	2	10	4			8	8					4			4					6	6				4			8		6
Windows 7 Ultimate	2	10	4			8	8					4			4					6	6				4			8		6
Windows 8	2	10	4			8	8					4			4					6	6				4			8		6
Antivirus ESET NOD 32	1	5	2			4	4					2			2					3	3				2			4		3

Ccleaner	1	5	2			4	4				2		2				3	3			2			4		3
Microsoft Project	1	5	2			4	4				2		2				3	3			2			4		3
Nero	1	5	2			4	4				2		2				3	3			2			4		3
Adobe Reader	1	5	2			4	4				2		2				3	3			2			4		3
Microsoft Office	2	10	4			8	8				4		4				6	6			4			8		6
Microsoft Visio	1	5	2			4	4				2		2				3	3			2			4		3
WinRar	1	5	2			4	4				2		2				3	3			2			4		3
Autocad	1	5	2			4	4				2		2				3	3			2			4		3
TeamViewer	1	5	2			4	4				2		2				3	3			2			4		3
Mozilla Thunderbird	2	10	4			8	8				4		4				6	6			4			8		6
PosgreSQL	1	5	2			4	4				2		2				3	3			2			4		3
Skype	1	5	2			4	4				2		2				3	3			2			4		3
NetBeans	1	5	2			4	4				2		2				3	3			2			4		3
Microsoft Visual basic 6.0	1	5	2			4	4				2		2				3	3			2			4		3
MySql	1	5	2			4	4				2		2				3	3			2			4		3
Eclipse	1	5	2			4	4				2		2				3	3			2			4		3
Delfin Gd	3	15	6			12	12				6		6				9	9			6			12		9
Chip (Hacienda)	2	10	4			8	8				4		4				6	6			4			8		6
MGA	2	10	4			8	8				4		4				6	6			4			8		6
Distrito	5	25	10			20	20				10		10				15	15			10			20		15
Página web de la Entidad	3	15	6			12	12				6		6				9	9			6			12		9
Aplicación Web de cuentas	4	20	8			16	16				8		8				12	12			8			16		12
Aplicación Web de ventanilla única	4	20	8			16	16				8		8				12	12			8			16		12
Aplicación web de Manejo de Cartera	4	20	8			16	16				8		8				12	12			8			16		12

Aplicación Web de Alumbrado Publico	4	20	8			16	16					8			8					12	12				8			16		12
Intranet Institucional	4	20	8			16	16					8			8					12	12				8			16		12
Correo institucional	3	15	6			12	12					6			6					9	9				6			12		9
Aplicación web DIAN	4	20	8			16	16					8			8					12	12				8			16		12
Red pública de conmutación telefónica	3							3	3		12	6										9					15			9
Ethernet	4							4	4		16	8										12					20			12
GigabitEthernet	4							4	4		16	8										12					20			12
Línea de suscriptor digital asimétrica (ASDL)	3							3	3		12	6										9					15			9
WiFi 802.11	3							3	3		12	6										9					15			9
Modems	4							4	4		16	8										12					20			12
Switch	4							4	4		16	8										12					20			12
Routers	4							4	4		16	8										12					20			12
PBX	4							4	4		16	8										12					20			12
Alcalde	2				4		8								4			4							4					6
Secretaría general	2				4		8								4			4							4					6
Secretaría de Hacienda	2				4		8								4			4							4					6
Secretaría de infraestructuta	2				4		8								4			4							4					6

Secretaría de desarrollo económico y social	2				4		8							4			4						4					6	
Secretaría de educación	2				4		8							4			4						4					6	
Secretaría de gobierno	2				4		8							4			4						4					6	
Secretaría de salud	2				4		8							4			4						4					6	
Oficina de control interno	2				4		8							4			4						4					6	
Oficina de contratación	2				4		8							4			4						4					6	
Oficina de control interno disciplinario	2				4		8							4			4						4					6	
Oficina asesora jurídica	2				4		8							4			4						4					6	
Oficina asesora de planeación	2				4		8							4			4						4					6	
Administrador del sistema	2				4		8							4			4						4					6	
Funcionarios a cargo de copias de seguridad	2				4		8							4			4						4					6	
Jefe de Oficina	2				4		8							4			4						4					6	
Desarrolladores de aplicación	2				4		8							4			4						4					6	
Domicilios del personal	1				2									3					1				2						
Instalaciones de otras organizaciones	1				2									3					1				2						
Ambiente Fuera de la Alcaldía	1				2									3					1				2						
Establecimiento	3				6									9					3				6						

Edificaciones	3				6									9					3				6							
Oficina	3				6									9					3				6							
Zonas de acceso reservado	3				6									9					3				6							
Líneas telefónicas	3				6									9					3				6							
Internet	3				6									9					3				6							
Redes telefónicas internas	3				6									9					3				6							
Suministro de energía	3				6									9					3				6							
Suministro de agua	3				6									9					3				6							
Disposición de residuos	2				4									6					2				4							
Despacho	2	10	4	4			8			8	8			6	4		6					6			4				6	6
Secretarías	2	10	4	4			8			8	8			6	4		6					6			4				6	6
Contratistas	2	10	4	4			8			8	8			6	4		6					6			4				6	6

ANEXO D. OBJETIVOS DE CONTROL

Objetivo de Control	Controles	Aplicabilidad	Control /Justificación
A.5.1 Política de seguridad de la información. Objetivo: Brindar apoyo y orientación a la dirección con respecto a la seguridad de la información, de acuerdo a los requisitos del negocio y los reglamentos y las leyes pertinentes.	A.5.1.1 Documento de la política de seguridad de la información.	NO	La política de seguridad de la información ya está documentada según como lo indica la norma.
	A.5.1.2 Revisión de la política de seguridad de la información.	SI	Se deben realizar revisiones periódicas de la política de seguridad para evitar que no se contemplen los principales parámetros que garanticen la seguridad dentro de la entidad.
A.6.1 Organización interna. Objetivo: Gestionar la seguridad de la información dentro de la organización.	A.6.1.1 Compromiso de la Dirección con la seguridad de la información.	SI	Debe ser manifestado por la máxima autoridad de la entidad el compromiso con la seguridad de la información, para así poder determinar las estrategias para su gestión.
	A.6.1.2 Coordinación de la seguridad de la información.	SI	Es necesario que se conozcan los roles y funciones en cada parte de la entidad en todo lo concerniente a la seguridad de la información.
	A.6.1.3 Asignación de responsabilidades para la seguridad de la información.	SI	Se deben definir claramente todas las responsabilidades en cuanto a seguridad de la información, esto incluye responsabilidades sobre los activos de información, claridad en el personal que estará a cargo del SGSI.
	A.6.1.4 Proceso de autorización de recursos para los servicios de procesamiento de la información.	SI	Se debe definir e implementar un proceso de autorización de la dirección para el uso de nuevos servicios que involucren el procesamiento de datos, para así evitar pasar por alto el cumplimiento de parámetros de seguridad.
	A.6.1.5 Acuerdos sobre confidencialidad.	SI	La entidad debe reflejar la necesidad de protección de la información por medio de la firma de acuerdos que garanticen la no divulgación de datos de uso interno.
	A.6.1.6 Contacto con las autoridades.	NO	Este control ya se encuentra implementado, se tiene contacto directo con las principales autoridades.
	A.6.1.7 Contacto con grupos de interés especiales.	SI	Es necesario mantenerse al día en cuanto a normatividad, tecnología e investigaciones sobre la seguridad de la información, esto podría traer grandes aportes a la entidad.

	A.6.1.8 Revisión independiente de la seguridad de la información.	SI	El enfoque que adopta la organización en cuanto a la seguridad de la información debe ser revisado a intervalos de tiempo planificados, lo que permitirá adoptar cambios significativos en el momento que sea necesario.
A.6.2 Partes externas. Objetivo: Mantener la seguridad de la información y de los servicios de procesamiento de información de organización a los cuales tienen acceso partes externas o que son procesados, comunicados o dirigidos por estas.	A.6.2.1 Identificación de los riesgos relacionados con las partes externas.	SI	Se necesita identificar los riesgos que una asociación con entidades externas pueden traer a la entidad, lo que permitiría implantar los controles adecuados con el objetivo de minimizar el impacto del riesgo.
	A.6.2.2 Consideraciones de la seguridad cuando se trata con los clientes.	SI	Todos los requisitos de seguridad deben considerarse para dar acceso a los clientes a los activos o a la información de la entidad para evitar que sea manipulada su integridad.
	A.6.2.3 Consideraciones de la seguridad en los acuerdos con terceras partes.	SI	Cuando se involucre acceso a la información en los acuerdos con terceras partes debe cumplirse con los requisitos de seguridad, para evitar que la información se le dé un uso inadecuado.
A.7.1 Responsabilidad sobre los activos. Objetivo: Lograr y mantener la protección adecuada de los activos organizacionales.	A.7.1.1 Inventario de activos.	SI	No existe claridad en los activos que hacen parte de la entidad, lo que hace evidente la necesidad de contar con un inventario de activos.
	A.7.1.2 Propiedad de los activos.	NO	Este control ya está implementado, existe claridad sobre la parte de la entidad que es propietaria de información específica.
	A.7.1.3 Uso aceptable de los activos.	SI	Deben existir reglas sobre el uso aceptable que se le da a la información dentro de la organización.
A.7.2 Clasificación de la información. Objetivo: Asegurar que la información recibe el control adecuado.	A.7.2.1 Directrices de clasificación.	SI	La información debe ser clasificada en términos de su valor, de los requisitos legales. De su sensibilidad y la importancia para la organización.
	A.7.2.2 Etiquetado y manejo de información.	SI	Debe existir un procedimiento para el etiquetado de los activos de información teniendo en cuenta las directrices de clasificación.
A.8.1 Antes de la contratación laboral. Objetivo: Asegurar que los empleados, contratistas y usuarios por tercera parte entienden sus responsabilidades y son adecuados para los roles para los que se los considera, y reducir el riesgo de robo, fraude o uso inadecuado de las instalaciones.	A.8.1.1 Roles y responsabilidades.	NO	Este control ya está implementado, los roles y responsabilidades de los empleados son específicas.
	A.8.1.2 Selección	NO	Control implementado. Se realizan revisiones de los antecedentes de los empleados para garantizar el cumplimiento de las leyes pertinentes.

	A.8.1.3 Términos y condiciones laborales.	NO	Control implementado. Los empleados deben estar de acuerdo con sus términos y condiciones de su contrato laboral, lo que permite tener total claridad sobre sus responsabilidades dentro de la entidad.
A.8.2 Durante la vigencia de la contratación laboral Objetivo: asegurar que todos los empleados, contratistas y usuarios de terceras partes estén conscientes de las amenazas y preocupaciones respecto a la seguridad de la información, sus responsabilidades y sus deberes, y que estén equipados para apoyar la política de seguridad de la organización en el transcurso de su trabajo normal, al igual que reducir el riesgo de error humano	A.8.2.1 Responsabilidades de la Dirección.	SI	La dirección debe exigir que los empleados apliquen la seguridad según políticas y procedimientos establecidos por la organización.
	A.8.2.2 Educación, formación y concientización sobre la seguridad de la información.	SI	Los empleados de la organización deben ser informados y concientizados sobre las políticas y los procedimientos para garantizar la seguridad de la información según sus funciones laborales.
	A.8.2.3 Proceso disciplinario.	SI	Debe existir procedimiento disciplinario formal para los empleados que hayan cometido alguna violación de la seguridad.
A.8.3 Terminación o cambio de la contratación laboral Objetivo: Asegurar que los empleados, los contratistas y los usuarios de terceras partes salen de la organización o cambian su contrato laboral de forma ordenada.	A.8.3.1 Responsabilidades en la terminación.	NO	Control implementado. Están definidas las responsabilidades para llevar a cabo la terminación o el cambio de contratación laboral.
	A.8.3.2 Devolución de activos.	NO	Control implementado. Los empleados deben devolver los activos pertenecientes a la organización que estén en su poder al finalizar la contratación.
	A.8.3.3 Retiro de los derechos de acceso.	SI	Los derechos de acceso debe los empleados deben ser retirados al finalizar la contratación laboral, para evitar la manipulación de los activos de personas que no tengan algún vínculo con la entidad.
A.9.1 Áreas seguras. Objetivo: Evitar el acceso físico no autorizado, el daño e interferencia a las instalaciones y a la información de la organización.	A.9.1.1 Perímetro de seguridad física.	NO	Control implementado. Se deben utilizar perímetros de seguridad para proteger las áreas que contienen información y servicios de procesamiento de información.
	A.9.1.2 Controles de acceso físico.	SI	Las áreas seguras deben ser protegidas con controles de acceso apropiadas para asegurar que solo se permita el acceso al personal autorizado.
	A.9.1.3 Seguridad de oficinas, recintos e instalaciones.	NO	Control implementado. Se garantiza la seguridad física de las áreas de la entidad.

	A.9.1.4 Protección contra amenazas externas y ambientales.	SI	Se deben diseñar y aplicar protecciones físicas contra daño por incendio, inundación, terremoto, explosión y otras formas de desastre natural y artificial para así garantizar que este tipo de eventos no afecten los activos de información.
	A.9.1.5 Trabajo en áreas seguras.	SI	Se debe diseñar y aplicar la protección física y las directrices para trabajar en áreas seguras.
	A.9.1.6 Áreas de carga, despacho y acceso público.	NO	Control actualmente implementado
A.9.2 Seguridad de los equipos. Objetivo: Evitar perdida, daño, robo o puesta en peligro de los activos y la interrupción de las actividades de la organización.	A.9.2.1 Ubicación y protección de los equipos	SI	Los equipos deben estar ubicados o protegidos para reducir el riesgo debido a amenazas o peligros del entorno, y las oportunidades de acceso no autorizado.
	A.9.2.2 Servicios de suministro	SI	Los equipos deben estar protegidos contra fallas en el suministro de energía y otras anomalías causadas por fallas en los servicios de suministro.
	A.9.2.3 Seguridad del cableado.	SI	El cableado de energía eléctrica y de telecomunicaciones que transporta datos o presta soporte a los servicios de información debe estar protegido contra interceptaciones o daños.
	A.9.2.4 Mantenimiento de los equipos.	NO	Control actualmente implementado
	A.9.2.5 Seguridad de los equipos fuera de las instalaciones.	SI	Se deben suministrar para los equipos fuera de las instalaciones teniendo en cuenta los diferentes riesgos de trabajar fuera de las instalaciones de la organización.
	A.9.2.6 Seguridad en la reutilización o eliminación de los equipos.	SI	Se deben verificar todos los elementos del equipo que contengan medios de almacenamiento para asegurar que se haya eliminado cualquier software licenciado y datos sensibles o asegurar que se hayan sobrescrito de forma segura antes de la eliminación.
	A.9.2.7 Retiro de los activos	NO	Control actualmente implementado
A.10.1 Procedimientos operacionales y responsabilidades. Objetivo: Asegurar la operación correcta y segura de los servicios de procesamiento de información.	A.10.1.1 Documentación de los procedimientos de operación.	SI	Los procedimientos de operación se deben documentar, mantener y estar disponibles para todos los usuarios que los necesiten.
	A.10.1.2 Gestión del cambio.	SI	Se deben controlar los cambios en los servicios y los sistemas de procesamiento de información.

	A.10.1.3 Distribución de funciones	SI	Las funciones y las áreas de responsabilidad se deben distribuir para reducir las oportunidades de modificación no autorizada o no intencionalmente, o en el uso inadecuado de los activos de la organización.
	A.10.1.4 Separación de las instalaciones de desarrollo, ensayo y operación.	SI	Las instalaciones de desarrollo, ensayo y operación deben estar separadas para reducir los riesgos de acceso o cambios no autorizados en el sistema operativo.
A.10.2 Gestión de la prestación del servicio por terceras partes. Objetivo: Implementar y mantener un grado adecuado de seguridad de la información y de la prestación del servicio, de conformidad con los acuerdos de prestación del servicio por terceras partes.	A.10.2.1 Prestación del servicio	NO	Control actualmente implementado
	A.10.2.2 Monitoreo y revisión de los servicios por terceras partes.	NO	Control actualmente implementado
	A.10.2.3 Gestión de los cambios en los servicios por terceras partes.	SI	Los cambios en la prestación de los servicios, incluyendo mantenimiento y mejora de las políticas existentes de seguridad de la información, en los procedimientos y los controles se deben gestionar teniendo en cuenta la importancia de los sistemas y procesos del negocio involucrados, así como la reevaluación de los riesgos.
A.10.3 Planificación y aceptación del sistema. Objetivo: Minimizar el riesgo de fallas de los sistemas.	A.10.3.1 Gestión de la capacidad.	SI	Se debe hacer seguimiento y adaptación del uso de los recursos, así como proyecciones de los requisitos de la capacidad futura para asegurar el desempeño requerido del sistema.
	A.10.3.2 Aceptación del sistema.	NO	Control actualmente implementado
A.10.4 Protección contra el código malicioso y descargable.	A.10.4.1 Controles contra códigos maliciosos.	SI	Se deben implementar controles de detección, prevención y recuperación para proteger contra códigos maliciosos, así como procedimientos apropiados de concientización de los usuarios.
	A.10.4.2 Controles contra códigos móviles	SI	Cuando se autoriza la utilización de códigos moviles, la configuración debe asegurar que dichos códigos operan de acuerdo con la política de seguridad claramente definida, y se debe evitar la ejecución de los códigos moviles no autorizados.
A.10.5 Respaldo Objetivo: Mantener la integridad y disponibilidad de la información y de los servicios de procesamiento de información.	A.10.5.1 Respaldo de la información.	SI	SE deben hacer copias de respaldo de la información y del software, y se deben poner a prueba con regularidad de acuerdo con la política de respaldo acordada.

A.10.6 Gestión de la seguridad de las redes. Objetivo: Asegurar la protección de la información en las redes y la protección de la estructura de soporte.	A.10.6.1 Controles de las redes	SI	Las redes se deben mantener y controlar adecuadamente para protegerlas de las amenazas y mantener la seguridad de los sistemas y aplicaciones que usan la red, incluyendo la información en tránsito.
	A.10.6.2 Seguridad de los servicios de red.	SI	En cualquier acuerdo sobre los servicios de la red se deben identificar e incluir las características de seguridad, los niveles de servicio y los requisitos de gestión de todos los servicios de la red, sin importar si los servicios se prestan en la organización o se contratan externamente.
A.10.7 Manejo de los medios. Objetivos: Evitar la divulgación, modificación, retiro o destrucción de activos no autorizada, y la interrupción en las actividades del negocio.	A.10.7.1 Gestión de los medios removibles.	SI	Se deben establecer procedimientos para la gestión de los medios removibles.
	A.10.7.2 Eliminación de los medios.	SI	Cuando ya no se requieran estos medios, su eliminación se debe hacer de forma segura y sin riesgo, utilizando los procedimientos formales.
	A.10.7.3 Procedimientos para el manejo de la información.	SI	Se deben establecer procedimientos para el manejo y almacenamiento de la información con el fin de proteger dicha información contra divulgación no autorizada o uso inadecuado.
	A.10.7.4 Seguridad de la documentación del sistema.	SI	La documentación del sistema debe estar protegida contra el acceso no autorizado.
A.10.8 Intercambio de información. Objetivo: Mantener la seguridad de la información y del software que se intercambiaran dentro de la organización y con cualquier entidad externa.	A.10.8.1 Políticas y procedimientos de intercambio de información.	SI	Se deben establecer políticas, procedimientos y controles formales de intercambio para proteger la información mediante el uso de todo tipo de servicios de comunicación.
	A.10.8.2 Acuerdos para el intercambio.	SI	Se deben establecer acuerdos para el intercambio de la información y del software entre la organización y partes externas.
	A.10.8.3 Medios físicos en tránsito.	SI	Los medios que contienen información se deben proteger contra el acceso no autorizado, el uso inadecuado o la corrupción durante el transporte más allá de los límites físicos de la organización.
	A.10.8.4 Mensajería electrónica.	NO	Control actualmente implementado

	A.10.8.5 Sistemas de información del negocio.	SI	Se deben establecer, desarrollar e implementar políticas y procedimientos para proteger la información asociada con la interconexión de los sistemas de información del negocio.
A.10.9 Servicios de comercio electrónico. Objetivo: Garantizar la seguridad de los servicios de comercio electrónico, y su utilización segura.	A.10.9.1 Comercio electrónico.	SI	La información involucrada en el comercio electrónico que se transmite por las redes públicas debe estar protegida contra actividades fraudulentas, disputas por contratos y divulgación o modificación no autorizada.
	A.10.9.2 Transacciones en línea.	SI	La información involucrada en las transacciones en línea debe estar protegida para evitar transmisión incompleta, enrutamiento inadecuado, alteración, divulgación, duplicación o repetición no autorizada del mensaje.
	A.10.9.3 Información disponible al público.	SI	La integridad de la información que se pone a disposición en un sistema de acceso público debe estar protegida para evitar la modificación no autorizada.
A.10.10 Monitoreo. Objetivo: Detectar actividades de procesamiento de la información no autorizadas.	A.10.10.1 Registros de auditorías.	NO	Control actualmente implementado
	A.10.10.2 Monitoreo del uso del sistema.	SI	Se deben establecer procedimientos para el monitoreo del uso de los servicios de procesamiento de información, y los resultados de las actividades de monitoreo se deben revisar con regularidad.
	A.10.10.3 Protección de la información del registro.	SI	Los servicios y la información de la actividad de registro se deben proteger contra el acceso o la manipulación no autorizados.
	A.10.10.4 Registros del administrador y operador.	SI	Se deben registrar las actividades tanto del operador como del administrador del sistema.
	A.10.10.5 Registro de fallas.	SI	Las fallas se deben registrar y analizar, y se deben tomar las acciones adecuadas.
	A.10.10.6 Sincronización de relojes.	SI	Los relojes de todos los sistemas de procesamiento de información pertinentes dentro de la organización o del dominio de seguridad deben estar sincronizados con una fuente de tiempo exacta y acordada.
A.11.1 Requisitos de negocio para el control de acceso. Objetivo: Asegurar el acceso de usuarios y evitar el acceso de usuarios no autorizados a los sistemas de información.	A.11.1.1 Política de control de acceso.	SI	Se deben establecer, documentar y revisar la política de control de acceso con base en los requisitos del negocio y de la seguridad para el acceso.

A.11.2 Gestión de acceso de usuario.	A.11.2.1 Registro de usuario.	SI	Debe existir un procedimiento formal para el registro y cancelación de usuarios con el fin de conceder y revocar el acceso a todos los sistemas y servicios de información.
	A.11.2.2 Gestión de privilegios.	NO	Control implementado actualmente
	A.11.2.3 Gestión de contraseñas para usuario.	SI	La asignación de contraseñas se debe controlar a través de un proceso formal de gestión.
	A.11.2.4 Revisión de los derechos de acceso de usuario.	SI	La dirección debe establecer un procedimiento formal de revisión periódica de los derechos de acceso de los usuarios.
A.11.3 Responsabilidades de los usuarios. Objetivo: Evitar el acceso de usuarios no autorizados. El robo o la puesta en peligro de la información de los servicios de procesamiento de información.	A.11.3.1 Uso de contraseñas.	SI	Se debe exigir a los usuarios el cumplimiento de buenas prácticas de seguridad en la selección y el uso de las contraseñas.
	A.11.3.2 Equipo de usuario desatendido.	SI	Los usuarios deben asegurarse de que a los equipos desatendidos se les da atención apropiada.
	A.11.3.3 Política de escritorio despejado y de pantalla despejada.	SI	Se debe adoptar una política de escritorio despejado para reportes y medios de almacenamiento removibles y una política de pantalla despejada para los servicios de procesamiento de información.
A.11.4 Control de acceso a las redes. Objetivo: Evitar el acceso no autorizado a servicios en red.	A.11.4.1 Política de uso de los servicios en red.	SI	Los usuarios sólo deben tener acceso a los servicios para cuyo uso están específicamente autorizados.
	A.11.4.2 Autenticación de usuario para conexiones externas.	SI	Se deben emplear métodos apropiados de autenticación para controlar el acceso de usuarios remotos.
	A.11.4.3 Identificación de los equipos en las redes.	SI	La identificación automática de los equipos se debe considerar un medio para autenticar conexiones de equipos v ubicaciones específicas.
	A.11.4.4 Protección de los puertos de configuración y diagnóstico remoto.	SI	El acceso lógico y físico a los puertos de configuración y de diagnóstico debe estar controlado
	A.11.4.5 Separación en las redes.	SI	En las redes se deben separar los grupos de servicios de información, usuarios y sistemas de información.

	A.11.4.6 Control de la conexión a las redes.	SI	Para redes compartidas, especialmente aquellas que se extienden más allá de las fronteras de la organización, se debe restringir la capacidad de los usuarios para conectarse a la red, de acuerdo con la política de control de acceso y los requisitos de aplicación del negocio.
	A.11.4.7 Control de enrutamiento en la red.	SI	Se deben implementar controles de enrutamiento en las redes con el fin de asegurar que las conexiones entre computadores y los flujos de información no incumplan la política de control del acceso de las aplicaciones del negocio.
A.11.5 Control de acceso al sistema operativo. Objetivo: Evitar el acceso no autorizado a los sistemas operativos.	A.11.5.1 Procedimientos ingreso seguros.	SI	El acceso a los sistemas operativos se debe controlar mediante un procedimiento de registro de inicio seguro.
	A.11.5.2 Identificación y autenticación de usuario.	SI	Todos los usuarios deben tener un identificador único (ID del usuario) únicamente para su uso personal, y se debe elegir una técnica apropiada de autenticación para comprobar la identidad declarada de un usuario.
	A.11.5.3 Sistema de gestión de contraseñas.	SI	Los sistemas de gestión de contraseñas deben ser interactivos y deben asegurar la calidad de las contraseñas.
	A.11.5.4 Uso de utilidades del sistema.	SI	Se debe restringir y controlar estrictamente el uso de programas utilitarios que pueden anular los controles del sistema y de la aplicación.
	A.11.5.5 Desconexión automática de sesión.	NO	Control implementado actualmente
	A.11.5.6 Limitación del tiempo de conexión.	SI	Se deben utilizar restricciones en los tiempos de conexión para brindar seguridad adicional para las aplicaciones de alto riesgo.
A.11.6 Control de acceso a las aplicaciones y a la información. Objetivo: Evitar el acceso no autorizado a la información contenida en los sistemas de información.	A.11.6.1 Restricción de acceso a la información.	SI	Se debe restringir el acceso a la información y a las funciones del sistema de aplicación por parte de los usuarios y del personal de soporte, de acuerdo con la política definida de control de acceso.
	A.11.6.2 Aislamiento de sistemas sensibles.	SI	Los sistemas sensibles deben tener un entorno informático dedicado.
A.11.7 Computación móvil y trabajo remoto	A.11.7.1 Computación y comunicaciones móviles.	SI	Se debe establecer una política formal y se deben adoptar las medidas de seguridad apropiadas para la protección contra los riesgos debidos al uso de dispositivos de computación y comunicaciones móviles.

	A.11.7.2 Trabajo remoto.	SI	Se deben desarrollar e implementar políticas, planes operativos y procedimientos para las actividades de trabajo remoto.
A.12.1 Requisitos de seguridad de los sistemas de información. Objetivo: Garantizar que la seguridad es parte integral de los sistemas de información.	A.12.1.1 Análisis y especificación de los requisitos de seguridad.	SI	Las declaraciones sobre los requisitos del negocio para nuevos sistemas de información o mejoras a los sistemas existentes deben especificar los requisitos para los controles de seguridad.
A.12.2 Procesamiento correcto de las aplicaciones. Objetivo: Evitar errores, pérdidas, modificaciones no autorizadas o uso inadecuado de la información en las aplicaciones.	A.12.2.1 Validación de los datos de entrada.	SI	Se deben validar los datos de entrada a las aplicaciones para asegurar que dichos datos son correctos y apropiados.
	A.12.2.2 Control del procesamiento interno.	NO	Control implementado actualmente
	A.12.2.3 Integridad del mensaje.	SI	Se deben identificar los requisitos para asegurar la autenticidad y proteger la integridad del mensaje en las aplicaciones, así como identificar e implementar los controles adecuados.
	A.12.2.4 Validación de los datos de salida.	NO	Control implementado actualmente
A.12.3 Controles criptográficos. Objetivo: Proteger la confidencialidad, autenticidad o integridad de la información, por medios criptograficos.	A.12.3.1 Política de uso de los controles criptográficos.	SI	Se debe desarrollar e implementar una política sobre el uso de controles criptográficos para la protección de la información.
	A.12.3.2 Gestión de llaves.	SI	Se debe implementar un sistema de gestión de llaves para apoyar el uso de las técnicas criptográficas por parte de la organización.
A.12.4 Seguridad de los archivos de sistema. Objetivo: Garantizar la seguridad de los archivos del sistema.	A.12.4.1 Control del software operativo.	NO	Control implementado actualmente
	A.12.4.2 Protección de los datos de prueba del sistema.	SI	Los datos de prueba deben seleccionarse cuidadosamente, así como protegerse y controlarse.
	A.12.4.3 Control de acceso al código fuente de los programas.	SI	Se debe restringir el acceso al código fuente de los programas.
A.12.5 Seguridad en los procesos de desarrollo y soporte. Objetivo: Mantener la seguridad del software y de la información del sistema de aplicaciones.	A.12.5.1 Procedimientos de control de cambios.	SI	Se deben controlar la implementación de cambios utilizando procedimientos formales de control de cambios.
	A.12.5.2 Revisión técnica de las aplicaciones tras efectuar cambios en el sistema operativo.	NO	Control implementado actualmente

	A.12.5.3 Restricciones a los cambios en los paquetes de software.	SI	Se debe desalentar la realización de modificaciones a los paquetes de software, limitarlas a los cambios necesarios, y todos los cambios se deben controlar estrictamente.
	A.12.5.4 Fugas de información.	SI	Se deben evitar las oportunidades para que se produzca fuga de información.
	A.12.5.5 Desarrollo de software contratado externamente.	NO	Control implementado actualmente
A.12.6 Gestión de la vulnerabilidad técnica. Objetivo: Reducir los riesgos resultantes de la explotación de las vulnerabilidades técnicas publicadas.	A.12.6.1 Control de las vulnerabilidades técnicas.	SI	Se debe obtener información oportuna sobre las vulnerabilidades técnicas de los sistemas de información que están en uso, evaluar la exposición de la organización a dichas vulnerabilidades y tomar las acciones apropiadas para tratar los riesgos asociados.
A.13.1 Reporte sobre los eventos y las debilidades de la seguridad de la información. Objetivo: Asegurar que los eventos y las debilidades de la seguridad de la información asociados con los sistemas de información se comunican de forma tal que permiten tomar las acciones correctivas oportunamente.	A.13.1.1 Reporte sobre los eventos de seguridad de la información.	SI	Los eventos de seguridad de la información se deben informar a través de los canales de gestión apropiados tan pronto como sea posible.
	A.13.1.2 Reporte sobre las debilidades de la seguridad.	SI	Se debe exigir a todos los empleados, contratistas y usuarios de terceras partes de los sistemas y servicios de información que observen y reporten todas las debilidades observadas o sospechadas en los sistemas o servicios.
A.13.2 Gestión de incidentes y mejoras de seguridad de la información. Objetivo: Asegurar que se aplica un enfoque consistente y eficaz para la gestión de los incidentes de seguridad de la información.	A.13.2.1 Responsabilidades y procedimientos.	SI	Se deben establecer las responsabilidades y los procedimientos de gestión para asegurar una respuesta rápida, eficaz y ordenada a los incidentes de seguridad de la información.
	A.13.2.2 Aprendizaje de los incidentes de seguridad de la información.	SI	Deben existir mecanismos que permitan cuantificar y monitorear todos los tipos, volúmenes y costos de los incidentes de seguridad de la información.
	A.13.2.3 Recolección de evidencias.	SI	Cuando una acción de seguimiento contra una persona u organización después de un incidente de seguridad de la información implica acciones legales, la evidencia se debe recolectar, retener y presentar para cumplir con las reglas para la evidencia establecidas en la jurisdicción pertinente.

A.14.1 Aspectos de seguridad de la información en la gestión de la continuidad del negocio. Objetivo: Contrarrestar las interrupciones en las actividades del negocio y proteger sus procesos críticos contra los efectos de fallas importantes en los sistemas de información o contra desastres , y asegurar su recuperación oportuna.	A.14.1.1 Inclusión de la seguridad de la información en el proceso de gestión de la continuidad del negocio.	SI	Se debe desarrollar y mantener un proceso de gestión para la continuidad del negocio en toda la organización el cual trate los requisitos de seguridad de la información necesarios para la continuidad del negocio de la organización.
	A.14.1.2 Continuidad del negocio y evaluación de riesgos.	SI	Se deben identificar los eventos que pueden ocasionar interrupciones en los procesos del negocio junto con la probabilidad y el impacto de dichas interrupciones, así como sus consecuencias para la seguridad de la información.
	A.14.1.3 Desarrollo e implantación de planes de continuidad que incluyan la seguridad de la información.	SI	Se deben desarrollar e implementar planes para mantener o recuperar las operaciones y asegurar la disponibilidad de la información en el grado y la escala de tiempo requerido, después de la interrupción o la falla de los procesos críticos para el negocio.
	A.14.1.4 Estructura para la planificación de la continuidad del negocio.	SI	Se debe mantener una sola estructura de los planes de continuidad del negocio, para asegurar que todos los planes son consistentes, y considerar los requisitos de la seguridad de la información de forma consistente, así como identificar las prioridades para pruebas y mantenimiento.
	A.14.1.5 Pruebas, mantenimiento y reevaluación de planes de continuidad del negocio.	SI	Los planes de continuidad del negocio se deben someter a pruebas y revisiones periódicas para asegurar su actualización y su eficacia.
A.15.1 Cumplimiento de los requisitos legales. Objetivo: Evitar el incumplimiento de cualquier ley, de obligaciones estatuarias, reglamentarias o contractuales y de cualquier requisito de seguridad.	A.15.1.1 Identificación de la legislación aplicable.	SI	Todos los requisitos estatuarios, reglamentarios y contractuales pertinentes, así como el enfoque de la organización para cumplir estos requisitos se deben definir explícitamente, documentar y mantener actualizados para cada sistema de información y para la organización.
	A.15.1.2 Derechos de propiedad intelectual (DPI).	SI	Se deben implementar procedimientos apropiados para asegurar el cumplimiento de los requisitos legales, reglamentarios y contractuales sobre el uso del material con respecto al cual pueden existir derechos de propiedad intelectual y sobre el uso de productos de software patentados.
	A.15.1.3 Protección de los documentos de la organización.	SI	Los registros importantes se deben proteger contra pérdida, destrucción y falsificación, de acuerdo con los requisitos estatuarios, reglamentarios, contractuales y del negocio.

	A.15.1.4 Protección de datos y privacidad de la información de carácter personal.	SI	Se debe garantizar la protección de los datos y la privacidad, de acuerdo con la legislación y los reglamentos pertinentes y, si se aplica, con las cláusulas del contrato.
	A.15.1.5 Prevención del uso inadecuado de los servicios de procesamiento de información.	SI	Se debe disuadir a los usuarios de utilizar los servicios de procesamiento de información para propósitos no autorizados.
	A.15.1.6 Reglamentación de los controles criptográficos.	SI	Se deben utilizar controles criptográficos que cumplan todos los acuerdos, las leyes y los reglamentos pertinentes.
A.15.2 Cumplimiento de las políticas y normas de seguridad y cumplimiento técnico. Objetivos: Asegurar que los sistemas cumplen con las normas y políticas de seguridad de la organización.	A.15.2.1 Cumplimiento de las políticas y normas de seguridad.	SI	Los directores deben garantizar que todos los procedimientos de seguridad dentro de sus áreas de responsabilidad se llevan a cabo correctamente para lograr el cumplimiento con las políticas y las normas de seguridad.
	A.15.2.2 Verificación del cumplimiento técnico.	SI	Los sistemas de información se deben verificar periódicamente para determinar el cumplimiento con las normas de implementación de la seguridad.
A.15.3 Consideraciones sobre las auditorías de los sistemas de información. Objetivo: Maximizar la eficacia de los procesos de auditoría de los sistemas de información minimizar su interferencia.	A.15.3.1 Controles de auditoría de los sistemas de información.	SI	Los requisitos y las actividades de auditoría que implican verificaciones de los sistemas operativos se deben planificar y acordar cuidadosamente para minimizar el riesgo de interrupciones de los procesos del negocio.
	A.15.3.2 Protección de las herramientas de auditoría de los sistemas de información.	SI	Se debe proteger el acceso a las herramientas de auditoría de los sistemas de información para evitar su uso inadecuado o ponerlas en peligro.

ANEXO E. RECURSOS DEL PROYECTO

Nombre de tarea	Nombres de los recursos
Entorno	
Análisis Situación Actual	
Analizar la estructura organizacional	Director del Proyecto; Ingeniero TI 1;Ingeniero TI 2;Ingeniero TI 3
Analizar la Visión	Ingeniero TI 1
Analizar la Misión	Ingeniero TI 2
Analizar la Política de Seguridad	Director del Proyecto;Ingeniero TI 3
Analizar los Objetivos de Calidad	Ingeniero TI 1;Ingeniero TI 2
Realizar reporte de la situación	Director del Proyecto;Ingeniero TI 1;Ingeniero TI 2;Ingeniero TI 3
Analizar el marco legal	Director del Proyecto;Ingeniero TI 1;Ingeniero TI 2;Ingeniero TI 3
Establecimiento	
Alcance	
Definir el Alcance del SGSI	Director del Proyecto
Política y Objetivos de seguridad	
Definir la Política de Seguridad	
Definir los objetivos de seguridad	Director del Proyecto;Ingeniero TI 1;Ingeniero TI 2;Ingeniero TI 3
Definir las políticas generales	Director del Proyecto;Ingeniero TI 1;Ingeniero TI 2;Ingeniero TI 3
Definir la política de control de acceso	Director del Proyecto;Ingeniero TI 1;Ingeniero TI 2;Ingeniero TI 3
Definir la política de correo electrónico	Director del Proyecto;Ingeniero TI 1;Ingeniero TI 2;Ingeniero TI 3
Definir la política del uso de Internet	Director del Proyecto;Ingeniero TI 1;Ingeniero TI 2;Ingeniero TI 3
Definir política de uso de los sistemas de Información	Director del Proyecto;Ingeniero TI 1;Ingeniero TI 2;Ingeniero TI 3
Definir la política para la realización de copias de respaldo	Director del Proyecto;Ingeniero TI 1;Ingeniero TI 2;Ingeniero TI 3
Enfoque Evaluación de Riesgos	
Establecer la metodología para la evaluación de riesgos	Director del Proyecto;Ingeniero TI 1;Ingeniero TI 2;Ingeniero TI 3
Desarrollar criterios para la aceptación de riesgos	Director del Proyecto; Ingeniero TI 1;Ingeniero TI 2;Ingeniero TI 3
Informe Evaluación de Riesgos	
Identificación de riesgos	
Identificar los activos dentro del alcance del SGSI	Director del Proyecto; Ingeniero TI 1;Ingeniero TI 2;Ingeniero TI 3

Identificar las amenazas de los activos	Director del Proyecto; Ingeniero TI 1;Ingeniero TI 2;Ingeniero TI 3
Identificar las vulnerabilidades	Director del Proyecto;Ingeniero TI 1;Ingeniero TI 2;Ingeniero TI 3
Identificar los Impactos	Director del Proyecto;Ingeniero TI 1;Ingeniero TI 2;Ingeniero TI 3
Análisis y Evaluación	
Valorar el impacto	Director del Proyecto;Ingeniero TI 1;Ingeniero TI 2;Ingeniero TI 3
Valorar la probabilidad de ocurrencia	Director del Proyecto;Ingeniero TI 1;Ingeniero TI 2;Ingeniero TI 3
Estimar los niveles de riesgo	Director del Proyecto;Ingeniero TI 1;Ingeniero TI 2;Ingeniero TI 3
Determinar la aceptación del riesgo	Director del Proyecto;Ingeniero TI 1;Ingeniero TI 2;Ingeniero TI 3
Opciones de Tratamiento del Riesgo	
Definir las opciones de tratamiento	Director del Proyecto; Ingeniero TI 1;Ingeniero TI 2;Ingeniero TI 3
Objetivos de Control	
Seleccionar objetivos de control	Director del Proyecto; Ingeniero TI 1;Ingeniero TI 2;Ingeniero TI 3
Elaborar la declaración de aplicabilidad	Director del Proyecto; Ingeniero TI 1;Ingeniero TI 2;Ingeniero TI 3
Riesgos Residuales	
Desarrollar el proceso para obtener la aprobación de la dirección sobre los riesgos residuales	Director del Proyecto; Ingeniero TI 1;Ingeniero TI 2;Ingeniero TI 3
Implementar y Operar SGSI	
Definir el listado de requisitos para obtener la aprobación de la dirección para implementar y operar el SGSI	Director del Proyecto;Ingeniero TI 1;Ingeniero TI 2;Ingeniero TI 3
Seguimiento y Revisión	
Procedimientos de Monitoreo	
Definir requisitos	Director del Proyecto;Ingeniero TI 1;Ingeniero TI 2;Ingeniero TI 3
Revisión de Eficacia	
Definir procedimiento	Director del Proyecto;Ingeniero TI 1;Ingeniero TI 2;Ingeniero TI 3
Valoración de eficacia	
Definir procedimiento	Director del Proyecto;Ingeniero TI 1;Ingeniero TI 2;Ingeniero TI 3
Valoración de Riesgos	

Definir requisitos	Director del Proyecto;Ingeniero TI 1;Ingeniero TI 2;Ingeniero TI 3
Auditorias	
Definir actividades	Director del Proyecto;Ingeniero TI 1;Ingeniero TI 2;Ingeniero TI 3
Revisión del SGSI	
Definir procedimiento	Director del Proyecto;Ingeniero TI 1;Ingeniero TI 2;Ingeniero TI 3
Planes de Seguridad	
Definir planes de actualización	Director del Proyecto;Ingeniero TI 1;Ingeniero TI 2;Ingeniero TI 3
Registro de Acciones	
Definir procedimiento	Director del Proyecto;Ingeniero TI 1;Ingeniero TI 2;Ingeniero TI 3
Mantenimiento y Mejora	
Implementación de Mejoras	
Definir actividades	Director del Proyecto;Ingeniero TI 1;Ingeniero TI 2;Ingeniero TI 3
Acciones Preventivas y Correctivas	
Definir procedimiento	Director del Proyecto;Ingeniero TI 1;Ingeniero TI 2;Ingeniero TI 3
Comunicación a Interesados	
Definir requisitos	Director del Proyecto;Ingeniero TI 1;Ingeniero TI 2;Ingeniero TI 3
Aseguramiento de Mejoras	
Definir procedimiento	Director del Proyecto;Ingeniero TI 1;Ingeniero TI 2;Ingeniero TI 3

ANEXO F. CRONOGRAMA DEL PROYECTO

Id	Nombre de tarea	Duración	Comienzo	Fin	Predecesoras
2	**Entorno**	**13 días**	**03/02/2014**	**18/02/2014**	
3	**Análisis Situación Actual**	**13 días**	**03/02/2014**	**18/02/2014**	
4	Analizar la estructura organizacional	2 días	03/02/2014	04/02/2014	
5	Analizar la Visión	2 días	04/02/2014	06/02/2014	4
6	Analizar la Misión	2 días	04/02/2014	06/02/2014	5CC
7	Analizar la Política de Seguridad	2 días	04/02/2014	06/02/2014	6CC
8	Analizar los Objetivos de Calidad	2 días	06/02/2014	10/02/2014	7
9	Realizar reporte de la situación	4 días	10/02/2014	13/02/2014	8
10	Analizar el marco legal	3 días	13/02/2014	18/02/2014	9
11	**Establecimiento**	**131 días**	**18/02/2014**	**30/07/2014**	
12	**Alcance**	**5 días**	**18/02/2014**	**24/02/2014**	
13	Definir el Alcance del SGSI	5 días	18/02/2014	24/02/2014	10
14	**Política y Objetivos de seguridad**	**34 días**	**25/02/2014**	**08/04/2014**	
15	Definir la Política de Seguridad	**34 días**	**25/02/2014**	**08/04/2014**	
16	Definir los objetivos de seguridad	4 días	25/02/2014	28/02/2014	13
17	Definir las políticas generales	5 días	28/02/2014	06/03/2014	16
18	Definir la política de control de acceso	5 días	07/03/2014	13/03/2014	17
19	Definir la política de correo electrónico	5 días	13/03/2014	19/03/2014	18
20	Definir la política del uso de Internet	5 días	19/03/2014	26/03/2014	19
21	Definir política de uso de los sistemas de Información	5 días	26/03/2014	01/04/2014	20
22	Definir la política para la realización de copias de respaldo	5 días	01/04/2014	08/04/2014	21
23	**Enfoque Evaluación de Riesgos**	**15 días**	**08/04/2014**	**25/04/2014**	
24	Establecer la metodología para la evaluación de riesgos	2 sem.	08/04/2014	21/04/2014	22
25	Desarrollar criterios para la aceptación de riesgos	1 sem	21/04/2014	25/04/2014	24
26	**Informe Evaluación de Riesgos**	**45 días**	**25/04/2014**	**20/06/2014**	
27	**Identificación de riesgos**	**25 días**	**25/04/2014**	**27/05/2014**	
28	Identificar los activos dentro del alcance del SGSI	2 sem.	25/04/2014	08/05/2014	25
29	Identificar las amenazas de los activos	1 sem	08/05/2014	14/05/2014	28
30	Identificar las vulnerabilidades	1 sem	14/05/2014	21/05/2014	29

31	Identificar los Impactos	1 sem	21/05/2014	27/05/2014	30
32	**Análisis y Evaluación**	**20 días**	**27/05/2014**	**20/06/2014**	
33	Valorar el impacto	1 sem	27/05/2014	03/06/2014	31
34	Valorar la probabilidad de ocurrencia	1 sem	03/06/2014	09/06/2014	33
35	Estimar los niveles de riesgo	1 sem	09/06/2014	16/06/2014	34
36	Determinar la aceptación del riesgo	1 sem	16/06/2014	20/06/2014	35
37	**Opciones de Tratamiento del Riesgo**	**7 días**	**20/06/2014**	**30/06/2014**	
38	Definir las opciones de tratamiento	7 días	20/06/2014	30/06/2014	36
39	**Objetivos de Control**	**15 días**	**30/06/2014**	**18/07/2014**	
40	Seleccionar objetivos de control	10 días	30/06/2014	11/07/2014	38
41	Elaborar la declaración de aplicabilidad	5 días	11/07/2014	18/07/2014	40
42	**Riesgos Residuales**	**5 días**	**18/07/2014**	**24/07/2014**	
43	Desarrollar el proceso para obtener la aprobación de la dirección sobre los riesgos residuales	5 días	18/07/2014	24/07/2014	41
44	**Implementar y Operar SGSI**	**5 días**	**24/07/2014**	**30/07/2014**	
45	Definir el listado de requisitos para obtener la aprobación de la dirección para implementar y operar el SGSI	5 días	24/07/2014	30/07/2014	43
46	**Seguimiento y Revisión**	**19 días**	**31/07/2014**	**22/08/2014**	
47	**Procedimientos de Monitoreo**	**3 días**	**31/07/2014**	**04/08/2014**	
48	Definir requisitos	3 días	31/07/2014	04/08/2014	45
49	**Revisión de Eficacia**	**3 días**	**04/08/2014**	**07/08/2014**	
50	Definir procedimiento	3 días	04/08/2014	07/08/2014	48
51	**Valoración de eficacia**	**3 días**	**07/08/2014**	**11/08/2014**	
52	Definir procedimiento	3 días	07/08/2014	11/08/2014	50
53	**Valoración de Riesgos**	**3 días**	**12/08/2014**	**14/08/2014**	
54	Definir requisitos	3 días	12/08/2014	14/08/2014	52
55	**Auditorias**	**2 días**	**14/08/2014**	**18/08/2014**	
56	Definir actividades	2 días	14/08/2014	18/08/2014	54
57	**Revisión del SGSI**	**2 días**	**18/08/2014**	**20/08/2014**	
58	Definir procedimiento	2 días	18/08/2014	20/08/2014	56
59	**Planes de Seguridad**	**1 día**	**20/08/2014**	**21/08/2014**	
60	Definir planes de actualización	1 día	20/08/2014	21/08/2014	58
61	**Registro de Acciones**	**2 días**	**21/08/2014**	**22/08/2014**	
62	Definir procedimiento	2 días	21/08/2014	22/08/2014	60
63	**Mantenimiento y Mejora**	**9 días**	**22/08/2014**	**03/09/2014**	
64	**Implementación de Mejoras**	**3 días**	**22/08/2014**	**27/08/2014**	
65	Definir actividades	3 días	22/08/2014	27/08/2014	62

66	**Acciones Preventivas y Correctivas**	**2 días**	**27/08/2014**	**29/08/2014**	
67	Definir procedimiento	2 días	27/08/2014	29/08/2014	65
68	**Comunicación a Interesados**	**2 días**	**29/08/2014**	**02/09/2014**	
69	Definir requisitos	2 días	29/08/2014	02/09/2014	67
70	**Aseguramiento de Mejoras**	**2 días**	**02/09/2014**	**03/09/2014**	
71	Definir procedimiento	2 días	02/09/2014	03/09/2014	69
72	**Gestión del Proyecto**	172,13 días	03/02/2014	**03/09/2014**	
73	Plan de Acción	172,13 días	03/02/2014	03/09/2014	