PROPUESTA DE UN SISTEMA DE GESTION DE SEGURIDAD DE LA INFORMACION PARA LA ALCALDIA MUNICIPAL DE GUACHETA-CUNDINAMARCA, BASADO EN LA NORMA ISO/IEC 27001:2013

FANNY ESPERANZA LOPEZ CRISTANCHO

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA UNAD
ESCUELA DE CIENCIAS BÁSICAS DE TECNOLOGÍA E INGENIERÍA
ESPECIALIZACIÓN EN SEGURIDAD EN INFORMÁTICA
BOGOTA
2018

PROPUESTA DE UN SISTEMA DE GESTION DE SEGURIDAD DE LA INFORMACION PARA LA ALCALDIA MUNICIPAL DE GUACHETA-CUNDINAMARCA, BASADO EN LA NORMA ISO/IEC 27001:2013

FANNY ESPERANZA LOPEZ CRISTANCHO

Monografía para optar el título de
Especialista en Seguridad informática.

Director del proyecto
Esp. Ing. Freddy Enrique Acosta

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA
ESCUELA DE CIENCIAS BÁSICAS DE TECNOLOGÍA E INGENIERÍA
PROGRAMA ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
BOGOTA
2018

Nota de aceptación:

_____
_____
_____
_____
_____
_____

_____
Firma del presidente del jurado

_____
Firma del jurado

_____
Firma del jurado

Bogotá D.C, Mayo 08 de 2018

Dedico este trabajo a Dios por regalarme la vida, y permitirme llegar este momento y seguir cumpliendo mis metas a nivel profesional, a mis padres por el apoyo incondicional brindado siempre, por ser las personas trabajadoras, que con arduo esfuerzo han apoyado cada uno de mis sueños y metas, a mis hermanos por estar siempre conmigo.

Fanny Esperanza

AGRADECIMIENTOS

Fanny Esperanza expresa sus agradecimientos a:

Esp. Ing. Freddy Enrique Acosta, asesor del proyecto, por su apoyo y orientación en el desarrollo de la presente monografía.

Lic. Pablo Enrique Quicazan Ballesteros, Alcalde Municipal Alcaldía de Guachetá Cundinamarca, por permitirme desarrollar el proyecto en esta entidad.

Ing. Salomón González, Asesor inicial proyecto, por apoyo y conocimientos brindados en el desarrollo del proyecto.

CONTENIDO

Pág.

LISTA DE TABLAS

Pág.

LISTA DE ILUSTRACIONES

Pág.

ANEXOS

Pág.

GLOSARIO

Activo informático: Cualquier dato, dispositivo u otro componente del entorno que apoya actividades relacionadas con la información. Los activos informáticos comprenden hardware, software, información confidencial[1].

Amenaza: Una amenaza informática es toda circunstancia, evento o persona que tiene el potencial de causar daño a un sistema en forma de robo, destrucción, divulgación, modificación de datos o negación de servicio (DoS)[2].

Backup: respaldo copia de seguridad.

Ciberdelito: El ciberdelito es un delito que se comete usando una computadora, red o hardware. La computadora o dispositivo puede ser el agente, el facilitador o el objeto del delito. El delito puede ocurrir en la computadora o en otros lugares[3].

Controles de seguridad: Es el conjunto de medidas preventivas y reactivas de las organizaciones y los sistemas tecnológicos, que permiten proteger la información, buscando cumplir los principios de confidencialidad, disponibilidad, integridad[4].

Hardware: Elementos físicos o materiales que forman el computador o sistema informático.

Información: Grupo de datos organizados, procesados, categorizados que representa un mensaje.

Políticas de seguridad: Una política de seguridad es un conjunto de directrices, normas, procedimientos e instrucciones que guía las actuaciones de trabajo y defínelos criterios de seguridad para que sean adoptados a nivel local o institucional, con el objetivo de establecer, estandarizar y normalizar la seguridad tanto en el ámbito humano como en el tecnológico[5].

Riesgo: Posibilidad de que una amenaza llegue a desestabilizar un sistema informático.

---

[1] COPRO. Activo seguridad Informática. Disponible en internet http://copro.com.ar/Activo_(seguridad_informatica).html

[2] SYMANTEC. Confianza en un mundo conectado. Glosario de seguridad 101. América Latina. (1995-2017). Disponible en Internet en: https://www.symantec.com/es/mx/theme.jsp?themeid=glosario-de-seguridad

[3] SYMANTEC. Confianza en un mundo conectado. Glosario de seguridad 101. América Latina. (1995-2017). Disponible en Internet en: https://www.symantec.com/es/mx/theme.jsp?themeid=glosario-de-seguridad

[4]RONQUILLO Sixto. PREZZI. Controles en la seguridad de la información.(17 Diciembre 2014).Disponible en: https://prezi.com/gkwjvmaeivtc/controles-en-la-seguridad-de-la-informac

[5] COLS C. slideshare. Políticas y medidas de seguridad. (2011).Disponible en internet: https://es.slideshare.net/carolcols/politicas-y-medidas-de-seguridad

SECOP: Portal único de contratación.

Seguridad de la información: Conjunto de normas que permite la integridad, confidencialidad, disponibilidad de la información y los datos importantes de una organización.

SIFA: Sistema de información de Mas Familias en Acción.

Sistema informático: un sistema interrelacionado compuesto hardware, software, personal informático, que permite el debido proceso de la información y protección de la misma.

SGSI: Sistema de gestión de seguridad de la información, son políticas de administración de la información.

Software: conjunto de programas que permite al computador realizar determinadas tareas.

Vulnerabilidad: Debilidad o grado de exposición de un sistema.

RESUMEN

En el desarrollo de la presente monografía se propone realizar un sistema de seguridad de la información para la alcaldía municipal de Guachetá, basado en la Norma ISO/IEC 27001:2013", la información de la entidad está expuesta a vulnerabilidades y amenazas que afectan la disponibilidad, integridad, confidencialidad, autenticidad de la misma.

La propuesta se desarrolla partiendo del análisis general de la entidad, posteriormente se genera la descripción del área de sistemas, funciones del administrador de sistemas, diagrama de red, política de uso de internet, política de uso de los equipos de cómputo, y descripción visual de visita realizada a la entidad.

La clasificación de los activos de información se realiza de acuerdo a lo indicado en el libro II de MAGERIT 3.0, lo cual permite mostrar resultados de forma clara y coherente; partiendo de esta clasificación de activos, se genera la clasificación de la información, y se diseña la descripción de las amenazas latentes para los activos informáticos de la entidad.

De acuerdo a los análisis realizados se genera la matriz de riesgo, teniendo presente la frecuencia y el impacto que generan las amenazas a los activos de información de la entidad.

El análisis arroja un riesgo intolerante de los activos de información de la entidad, lo que lleva a la aplicación de los controles de la norma ISO 27001:2013 para implementar políticas que se deben desarrollar en el ente estatal para salvaguardar y proteger la información y activos informáticos, preservando la confidencialidad, integridad, disponibilidad de la información.

Palabras claves

AMENAZAS, VULNERABILIDADES, RIESGO, ISO/IEC 27001:2013, SEGURIDAD, CONTROLES, INFORMACIÓN, ATAQUES, CONTINGENCIA, CONFIDENCIALIDAD, INTEGRIDAD, NO REPUDIO, TRAZABILIDAD.

ABSTRACT

In the development of the present monograph, it is proposed to create an information security system for the municipal government of Guachetá, based on ISO / IEC 27001: 2013, "the information of the entity is exposed to vulnerabilities and threats that affect the availability, integrity, confidentiality, authenticity of it.

The proposal is developed based on the general analysis of the entity, then the description of the systems area, system administrator functions, network diagram, internet use policy, computer equipment usage policy, and visual description is generated. Of visit made to the entity.

The classification of the information assets is carried out according to what is indicated in book II of MAGERIT 3.0, which allows to show results in a clear and coherent way; Based on this classification of assets, the classification of the information is generated, and the description of the latent threats for the IT assets of the entity is designed.

According to the analyzes carried out, the risk matrix is generated, bearing in mind the frequency and impact generated by the threats to the information assets of the entity.

The analysis shows an intolerant risk of the information assets of the entity, which leads to the application of the controls of ISO 27001: 2013 to implement policies that must be developed in the state entity to safeguard and protect information and assets computer, preserving the confidentiality, integrity, availability of information.

Keywords

THREATS, VULNERABILITIES, RISK, ISO / IEC 27001: 2013, SECURITY, CONTROLS, INFORMATION, ATTACKS, CONTINGENCY, CONFIDENTIALITY, INTEGRITY, NON-REPUDIATION, TRACEABILITY.

INTRODUCCIÓN

Diversos estudios indican, que hoy en día la mayor cantidad de ataques de seguridad de la información provienen del interior de sus propias empresas (empleados descontentos, fraude interno, acceso no autorizado, falta de motivación, ausencia de entrenamiento organizacional, etcétera). Así mismo se ejecutan ataques a través de la ingeniería social, que vulneran los sistemas de seguridad y cifrado. En algunas organizaciones, con tan sólo recorrer algunos lugares de trabajo, se pueden encontrar contraseñas escritas y pegadas en la pantalla o debajo del teclado[6].

La creación de modelos, políticas, bajo estrategias ludicopedagogicas permite concientizar y entrenar a los trabajadores de la importancia de la seguridad de la información buscando cambiar el actuar, referente a este tema.

El ministerio de las tecnologías de la información y las comunicaciones – MINTIC a través de la Dirección de Estándares y Arquitectura de TI y la Subdirección de Seguridad y Privacidad de TI, dando cumplimiento a sus funciones; publica el Modelo de seguridad privacidad de la información (MSPI), el cual se encuentra alineado dentro de la estrategia GEL (Estrategia de gobierno en línea): TIC para servicios, TIC para gobierno abierto y TIC para gestión[7]

Mediante la adopción del Modelo de Seguridad y Privacidad por parte de las Entidades del Estado, buscan contribuir al incremento de la transparencia en la Gestión Pública, promoviendo el uso de las mejores prácticas de Seguridad de la Información como base de la aplicación del concepto de Seguridad Digital[8].

La implementación del Modelo de Seguridad y Privacidad de la Información - MSPI, en la Entidad está determinado por las necesidades objetivas, los requisitos de seguridad, procesos, el tamaño y la estructura de la misma, todo con el objetivo de preservar la confidencialidad, integridad, disponibilidad de los activos de información, garantizando su buen uso y la privacidad de los datos[9].

El COMPES 3854 del 11 de Abril de 2016, implementa la política nacional de seguridad digital que se ejecutara durante los años 2016-2019, en las principales entidades del gobierno, siendo ejemplo para que las demás organizaciones estatales avancen en la construcción del Modelo de gestión de seguridad de la información, teniendo en cuenta que actualmente el número de riesgos asociados

[6] VILLAMIZAR. R. Carlos. CISA.CISM.CGEIT. CRISC.Cobit Foundation Certificate e ISO 27001LA. (Agosto 2013). Jugando a crear cultura de seguridad de la información de la teoría a la práctica. Disponible en internet: http://www.magazcitum.com.mx/?p=236

[7] COLOMBIA. MINTIC. Modelo de seguridad. Disponible en internet: http://www.mintic.gov.co/gestionti/615/w3-propertyvalue-7275.html

[8] Ibíd., http://www.mintic.gov.co/gestionti/615/w3-propertyvalue-7275.html

[9] Ibid., http://www.mintic.gov.co/gestionti/615/w3-propertyvalue-7275.html

a equipos, sistemas de información y comunicación, han aumentado de manera significativa y no cuenta con los controles de seguridad.[10]

Cada día los ataques a la seguridad de la información a las organizaciones son más sólidos y robustos, donde se hace difícil defenderse, como se viene trabajando en cada dependencia, es por ello la importancia establecer el modelo de seguridad para prevenir fallas, fugas en los sistemas.

Las políticas de privacidad y seguridad de la información salvaguardan a la misma de grandes amenazas, garantizando el equilibrio y continuidad de los sistemas de información, minimizando riesgos, evitando daños y permitiendo que las entidades cumplan sus objetivos.

La monografía presenta la propuesta de un sistema de gestión de seguridad de la información para la alcaldía municipal de Guachetá -Cundinamarca, bajo el estándar de la NTC: ISO/IEC 27001:2013, buscando la transparencia y acceso a la información pública, logrando mejor gestión y protección de la información de la entidad, garantizando que los riesgos de seguridad que presenta cada una de las dependencias sean minimizados en base a las políticas establecidas en el sistema de gestión de seguridad informática (SGSI).

[10] COLOMBIA, CONSEJO NACIONAL DE POLITICA SOCIAL. Política social de seguridad digital. Bogotá. (11 de Abril 2016). Disponible en: https://colaboracion.dnp.gov.co/CDT/Conpes/Econ%C3%B3micos/3854.pdf

1.DEFINICION DEL PROBLEMA

1.1 PLANTEAMIENTO DEL PROBLEMA

Día tras día el crecimiento de la tecnología y el uso de las Tecnologías de la información y la comunicación, para el desarrollo de las actividades empresariales, nuevos avances técnicos, implementación de software para apoyar los procesos de las entidades estatales, trae consigo nuevos riesgos y vulnerabilidades que pueden llegar a comprometer los sistemas de información, a través de virus, software malicioso en la red, ingeniería social, que alteran dichos procesos, que conllevan a cometer fraude, generando traumatismos.

Otro de aspectos a tener en cuenta son los ataques cibernéticos que aumenta a diario, es así que el día 11 de Mayo de 2017, se detectó vulnerabilidad de Microsoft Windows donde pone en jaque la seguridad informática mundial, en Colombia se vieron afectadas 12 empresas, una de ellas estatal, sector salud, el virus malicioso conocido como Ransom:Win32. WannaCrypt. Herramienta que permite bloquear los datos de miles de computadoras de todo el mundo[11].

La alcaldía municipal de Guachetá siendo empresa del sector público, maneja gran volumen de información que debe ser protegido en su contenido y valor, en la actualidad no se ha implementado un modelo de seguridad informática para la entidad, que permita generar un inventario de los activos informáticos, conocer las vulnerabilidades, amenazas y riesgos que presentan, y construir las políticas de seguridad para preservar la confidencialidad, integridad y disponibilidad del sistema de información.

Por este motivo se presenta la propuesta del sistema de gestión de seguridad de la información para la alcaldía municipal de Guachetá-Cundinamarca bajo el estándar de la NTC: ISO/IEC 27001:2013

1.2 FORMULACION DEL PROBLEMA

¿Cómo se debe documentar la propuesta del sistema de gestión de seguridad de la información para mitigar el riesgo de los activos informáticos de la alcaldía municipal de Guachetá-Cundinamarca?

[11]RCN RADIO. Ataque cibernético en Colombia ha afectado a unas 11 empresas privadas. (Mayo 2015).Disponible en internet: http://www.rcnradio.com/nacional/ataque-cibernetico-en-colombia-ha-afectado-a-unas-11-em

1.3 OBJETIVOS

1.3.1 Objetivo general

Proponer el sistema de gestión de seguridad de la información para la alcaldía municipal de Guachetá-Cundinamarca, basado en la norma ISO/IEC 27001:2013, utilizando como metodología de análisis de riesgo MAGERIT V3.

1.3.2 Objetivos específicos

- Revisar el estado actual de la seguridad de la información en la alcaldía municipal de Guachetá.
- Clasificar los activos de información con que cuenta la alcaldía municipal de Guachetá, utilizando la metodología MAGERIT V3.
- Determinar las amenazas y riesgos a que están expuestos los activos de información.
- Aplicar controles de la norma ISO 27001:2013 a los activos de información.
- Proponer las políticas de seguridad de la información basadas en la norma ISO 27001:2013.

1.4 JUSTIFICACIÓN

La seguridad de la información hace parte de lo administrativo de la entidad, y teniendo en cuenta que la legislación colombiana indica el deber de la protección de la información y los datos, las empresas están en la necesidad de implementar el modelo del sistema de gestión de seguridad de la información, para salvaguardar los activos informáticos.

Un sistema de seguridad de la información implica crear el plan de diseño, implementación, y mantenimiento de una serie de procesos que permita gestionar de manera eficiente la información, para asegurar la integridad, confidencialidad, y disponibilidad de la misma. Un Sistema de Gestión de Seguridad de la Información debe ser considerado a la hora de administrar la seguridad de la organización, en especial cuando la entidad cuenta con alto nivel de complejidad, para conseguir así una mayor eficiencia y garantía en la protección de sus activos de información[12].
Las organizaciones y sus sistemas de información están expuestos a un número cada vez más elevado de amenazas que, aprovechando cualquiera de las

[12] PACHECO. Federico. Welivesecurity. s.f. Disponible en internet: https://www.welivesecurity.com/la-es/2010/09/10/la-importancia-de-un-sgsi/

vulnerabilidades existentes, pueden someter a activos críticos de información a diversas formas de fraude, espionaje, sabotaje o vandalismo. Los virus informáticos, el “hacking” o los ataques de denegación de servicio son algunos ejemplos comunes y conocidos, pero también se deben considerar los riesgos de sufrir incidentes de seguridad causados voluntaria o involuntariamente desde dentro de la propia organización o aquellos provocados accidentalmente por catástrofes naturales y fallos técnicos[13].

El gobierno nacional dentro de las estrategias de gobierno en línea, busca potencializar los cambios que se han venido presentando en la sociedad, partiendo de los principios de eficiencia, eficacia, visibilidad y publicidad, aprovechando el uso de la tecnología, garantizando mayor comunicación e interacción con la ciudadanía, y mejores servicios por parte del Estado[14].
Partiendo de este principio y haciendo relación a la alcaldía municipal de Guachetá-Cundinamarca, la entidad requiere de un sistema de gestión de seguridad de la información, bajo los lineamientos del estándar NTC:ISO/IEC 27001:2013, documentado, socializado, para administrar de forma correcta la información, generando control, disminuyendo riesgos, garantizando la protección de los activos de información.

El sistema de gestión de seguridad de la información, permitirá que la entidad de cumplimiento a lo establecido en la normatividad del estado colombiano, la estrategia gobierno en línea GEL, referente al uso adecuado de las Tecnologías de la información y la comunicación TIC´s, gobiernos más transparentes, de servicio a la comunidad, respondiendo a las necesidades de los ciudadanos[15].
El proponer el sistema de gestión de seguridad de la información en la entidad permitirá garantizar la seguridad de los activos de información, cumpliendo los principios de la seguridad informática como es la: confidencialidad, integridad, disponibilidad, generando en los empleados la concientización del valor de los activos informáticos.

Con la implementación del Sistema de Gestión de Seguridad de la Información, la gerencia, funcionarios, contratistas y usuarios externos tendrán políticas documentadas, lineamientos claros que se deben poner en práctica, para cumplir con sus funciones en virtud del cuidado y custodia de la información de la entidad.

---

[13] __Sistema de gestión de la seguridad de la información. s.f. Disponible en: http://www.iso27000.es/download/doc_sgsi_all.pdf. p3.
[14]COLOMBIA.MINISTERIO DE LAS TECNOLIGAS DE INFORMACION Y COMUNICACIÓN. Estrategia GEL. Disponible en internet: http://estrategia.gobiernoenlinea.gov.co
[15] COLOMBIA.MINISTERIO DE LAS TECNOLIGAS DE INFORMACION Y COMUNICACIÓN. Implementación de la estrategia de gobierno en línea. Disponible en internet: http://estrategia.gobiernoenlinea.gov.co/623/w3-propertyvalue-7652.html

1.5 ALCANCE Y LIMITACIONES

1.5.1 Alcances

La presente monografía se encuentra entre los proyectos de gestión de seguridad y lo que pretende es proponer de un sistema de gestión de seguridad de la información para la alcaldía municipal de Guachetá-Cundinamarca basado en la norma NTC/-ISO—IEC27001:2013, para el análisis y gestión del riesgo se utilizara la metodología MAGERIT V3.

1.5.2 Limitaciones

Es conveniente resaltar que la presente monografía no abarca temas como los que se definen a continuación:

- Implementar el modelo de sistema de gestión de seguridad de la información para alcaldía municipal de Guachetá-Cundinamarca.
- Garantizar revisión, mantenimiento y continuidad del modelo de sistema de gestión de seguridad de la información para alcaldía municipal de Guachetá.

1.6 DISEÑO METODOLÓGICO

1.6.1 Unidad de análisis

Los activos informáticos de la alcaldía municipal de Guachetá.

1.6.2 Población y muestra

1.6.2.1 Población: Activos informáticos de la Alcaldía municipal de Guachetá.

1.6.2.2 Muestra: Se llevara a cabo el desarrollo del proyecto tomando como muestra los activos informáticos de las siguientes dependencias.

- Desarrollo social
- Secretaria de Hacienda
- Secretaria de Gobierno
- Secretaria de Planeación
- Secretaria de Servicios Públicos
- Almacén y archivo
- Área de sistemas.

1.6.3 Estudio metodológico

El método holístico se utilizara para construir la propuesta del sistema de gestión de seguridad de la información para la alcaldía municipal de Guachetá-Cundinamarca, bajó la norma ISO 27001:2013, es una propuesta integrativa de la investigación y de la metodología.

Los holotipos de investigación son eventos que trascienden a sí mismos pues cada uno procede y contiene a un holotipo anterior y prosigue a un holotipo posterior en un proceso dinámico, las características esenciales que lo definen son tan genéricas, que pueden ser aplicables a cualquier área del conocimiento[16].

1.6.3.1 Tipos de investigación: Para el desarrollo de la monografía se implementaran

La investigación exploratoria: observación, lectura y registro.
La investigación descriptiva: características de la descripción de los hechos.
La investigación comparativa: antecedentes, diferencias y semejanzas[17].

Teniendo en cuenta lo anterior la presente monografía corresponde a una propuesta del sistema de gestión de seguridad de la información para la alcaldía municipal de Guachetá, bajo referencia de la norma ISO 27001:2013.
Se resalta que se apoyara la investigación con el tipo de investigación de campo, Documental, con la sugerencia de la definición del Manual de trabajos de grado de especialización y maestría y tesis doctorado.

1.6.3.2 Línea de investigación: La línea de investigación para el desarrollo de la propuesta es la de Gestión de sistemas de información, teniendo como precedente las líneas de investigación de la Escuela de ciencias básicas tecnología e ingeniería, cadena de sistemas, de la Universidad Nacional Abierta y a Distancia[18]

1.6.3.3 Etapas de la investigación
Diagnóstico, planteamiento y fundamentación de la propuesta.
Procedimiento metodológico
Recursos necesarios para la ejecución
Análisis y conclusiones

[16] HURTADO DE BECERRA, Jacqueline. Metodología de la investigación holística. Caracas Venezuela, Edit. Sypal. 2000. Pág 38.
[17] HURTADO DE BECERRA, Jacqueline. Metodología de la investigación holística. Caracas Venezuela, Edit. Sypal. 2000. Pág 39.
[18] UNAD. Grupo de investigación ECBTI.Bogota.2016. Disponible en internet: https://academia.unad.edu.co/ecbti/investigacion-y-productividad/grup

1.6.3.4 Instrumentos de recolección de datos de la investigación: Para el desarrollo del proyecto de grado se utilizaran los siguientes instrumentos de recolección de datos de investigación:

- Encuestas
- Observaciones
- Entrevista con los funcionarios de la entidad.
- Entrevista con los funcionarios del área de sistemas.
- Documentos gubernamentales relacionados con el tema de seguridad informática.
- Libros, artículos de internet, revistas, normas, leyes, entre otros de forma física o electrónica.

1.6.3.5 Fases Metodológicas: El proyecto se desarrollara de acuerdo a las siguientes fases:

Tabla 1. Fases metodológicas

Fase I	**Fase II**	**Fase III**
Recolección y análisis de datos	Seleccionar y evaluar alternativas Seleccionar y evaluar alternativas de solución de los antecedentes encontrados	Construcción
Analizar el estado actual de la información de la alcaldía municipal de Guachetá Verificar la clasificación de los activos informáticos. Identificar amenazas.	Aplicar controles de la norma ISO: 27001:2013. Crear políticas de seguridad de la información	Documentación de la información.

Fuente: Propiedad del autor

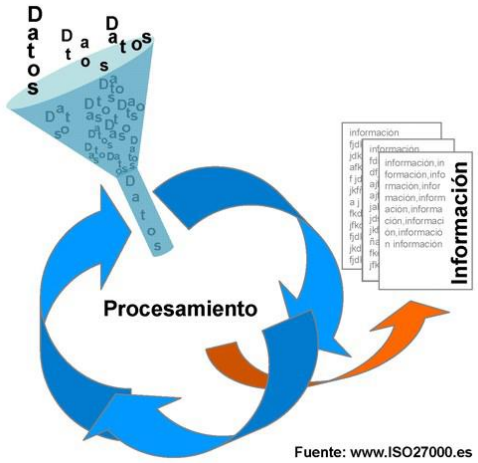
2.MARCO DE REFERENCIA

2.1 MARCO TEÓRICO

SGSI es la abreviatura utilizada para referirse a un Sistema de Gestión de la Seguridad de la Información. En el contexto aquí tratado, se entiende por información todo aquel conjunto de datos organizados en poder de una entidad que posean valor para la misma, independientemente de la forma en que se guarde o transmita (escrita, en imágenes, oral, impresa en papel, almacenada electrónicamente, proyectada, enviada por correo, fax o e-mail, transmitida en conversaciones, etc.), de su origen (de la propia organización o de fuentes externas) o de la fecha de elaboración[19].

A continuación la Imagen 1, Diagrama de la información permite visualizar el proceso de gestión de la información.

Ilustración 1. Diagrama de la información



Fuente: WWW.ISO27000.ES.Sistema de gestión de la seguridad de la información. s.f. p2.Disponible en internet: http://www.iso27000.es/download/doc_sgsi_all.pdf. p2.

De acuerdo a lo establecido en la norma ISO 27001 se busca cumplir con los siguientes principios fundamentales:

Confidencialidad**:** La información se debe dar a conocer a personas autorizadas.

Integridad: Es la cualidad que posee un documento o archivo que no ha sido alterado y que además permite comprobar que no se ha producido manipulación alguna en el documento original.

[19] __Sistema de gestión de la seguridad de la información. s.f. Disponible en: http://www.iso27000.es/download/doc_sgsi_all.pdf. p2.

Disponibilidad: La disponibilidad de la información hace referencia a que la información pueda ser recuperada en el momento que se necesite, esto es, evitar su pérdida o bloqueo, bien sea por ataque doloso, mala operación accidental o situaciones fortuitas o de fuerza mayor.

Con un Sistema de Gestión de la seguridad de la información, la organización conoce los riesgos a los que está sometida su información y los asume, minimiza, transfiere o controla mediante una sistemática definida, documentada y conocida por todos, que se revisa y mejora constantemente[20].

A continuación la Imagen 2. Riesgos, describe los riesgos presentes en un sistema de información.

Ilustración 2.Riesgos

Fuente: Fuente: WWW.ISO27000.ES.Sistema de gestión de la seguridad de la información. s.f. p4. Disponible en internet: http://www.iso27000.es/download/doc_sgsi_all.pdf. p4.

2.1.1 Plan de establecer un sistema de gestión de seguridad de la información

La seguridad que se puede lograr a través de medios técnicos es limitada, por lo que para garantizar la custodia de la información podemos contar con un Sistema de Gestión de Seguridad de la Información, que permite analizar y ordenar la estructura de los sistemas de información.

La Imagen 3. Planificación de un Sistema de Gestión de Seguridad de la Información, describe como planificar un sistema de gestión de seguridad de la información en una entidad.

[20]Sistema de gestión de la seguridad de la información. s.f. Disponible en: http://www.iso27000.es/download/doc_sgsi_all.pdf. p4.

Ilustración 3. Planificación de un SGSI

Fuente: Sistema de Gestión de Seguridad de la Información. (2015). Disponible en: http://audicaribe.com/sgsi-1/

Para implantar un Sistema de Gestión de Seguridad de la Información es necesaria la total implicación y apoyo de la dirección en el proyecto y un correcto diseño del mismo. El diseño del Sistema de Gestión de Seguridad de la Información, debe tener en cuenta el alcance y los objetivos que se pretenden. El Sistema de Gestión de Seguridad de la Información incluirá el diseño de la política de seguridad de la empresa, la realización de un inventario de la información a custodiar y un análisis de los riesgos de cada tipo de información.[21]

2.1.2 Normas de seguridad informática

2.1.2.1 ISO 27000: Es una familia de estándares de ISO e IEC que proporciona un marco para la gestión de la seguridad de la información. Estas normas especifican los requisitos para establecer, implantar, poner en funcionamiento, controlar, revisar, mantener y mejorar un SGSI22.

2.1.2.2 ISO 27001: Es la norma principal de la serie ISO/EIC 27000 y se puede aplicar a cualquier tipo de organización, sin importar su tamaño o su actividad comercial. La Norma contiene los requisitos para establecer, implementar, operar, supervisar, revisar, mantener y mejorar un Sistema de Gestión de la Seguridad de la Información, documentado dentro del contexto global de los riesgos de negocio de la organización[23].

[21] __Sistema de Gestión de Seguridad de la Información. (2015). Disponible en: http://audicaribe.com/sgsi-1/

[22] RAMÍREZ VILLEGAS. Gabriel. CONSTAIN MORENO. Gustavo. modelos y estándares de seguridad informática. Zona centro sur: Cead Palmira, Cead Popayán.UNAD.2012.25p.

[23] RAMÍREZ VILLEGAS. Gabriel. CONSTAIN MORENO. Gustavo. modelos y estándares de seguridad informática. Zona centro sur: Cead Palmira, Cead Popayán.UNAD.2012.30p.

2.1.2.3 ISO 27002: La NORMA ISO/IEC 27002 es una guía de buenas prácticas que recoge las recomendaciones sobre las medidas a tomar para asegurar los sistemas de información en una organización. Para ello describe 11 áreas de actuación, 39 objetivos de control o aspectos a asegurar dentro de cada área y 133 controles o mecanismos para asegurar los distintos objetivos de control[24].

2.1.2.4 ISO 27003: Consiste en una guía de implementación de Sistema de Gestión de Seguridad de la Información e información acerca del uso del modelo PDCA (planificar, hacer, verificar, actuar) y de los requerimientos de sus diferentes fases. Tiene su origen en el anexo B de la norma BS7799-2 y en la serie de documentos publicados por BSI a lo largo de los años con recomendaciones y guías de implantación.

Bajo el estándar de la NTC: ISO/IEC 27001:2013 se puede demostrar a usuarios existentes y potenciales, proveedores la integridad de sus datos y sistemas, así como su compromiso con la seguridad de la información. También puede dar lugar a nuevas oportunidades de negocio con clientes preocupados por la seguridad; puede mejorar la ética de los empleados y fortalecer la noción de confidencialidad en todo el lugar de trabajo. Además, le permite reforzar la seguridad de la información y reducir el posible riesgo de fraude, pérdida de información y divulgación[25].

2.1.2.5 ISO 27005: Establece las directrices para la gestión del riesgo en la seguridad de la información. Apoya los conceptos generales especificados en la norma ISO/IEC 27001 y está diseñada para ayudar a la aplicación satisfactoria de la seguridad de la información basada en un enfoque de gestión de riesgos[26]

2.1.3 Metodología MAGERIT V3

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

2.1.3.1 Objetivos de MAGERIT

[24] RAMÍREZ VILLEGAS. Gabriel. CONSTAIN MORENO. Gustavo. modelos y estándares de seguridad informática. Zona centro sur: Cead Palmira, Cead Popayán.UNAD.2012.32p.
[25] Salud y Seguridad. ISO 27001:2013. Sistemas de gestión de seguridad de la información. Disponible en internet: http://www.sgs.co/es-ES/Health-Safety/Quality-Health-Safety-and-Environment/Risk-Assessment-and-Management/Security-Management/ISO-27001-2013-Information-Security-Management-Systems.aspx
[26] RAMÍREZ VILLEGAS. Gabriel. CONSTAIN MORENO. Gustavo. modelos y estándares de seguridad informática. Zona centro sur: Cead Palmira, Cead Popayán.UNAD.2012.34p.

- Concienciar a los responsables de las organizaciones de información de la existencia de riesgos y de la necesidad de gestionarlos
- Ofrecer un método sistemático para analizar los riesgos derivados del uso de tecnologías de la información y comunicaciones (TIC)
- Ayudar a descubrir y planificar el tratamiento oportuno para mantener los riesgos bajo control Indirectos:
- Preparar a la Organización para procesos de evaluación, auditoría, certificación o acreditación, según corresponda en cada caso[27].

2.2 MARCO CONCEPTUAL

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

Hasta la aparición y difusión del uso de los sistemas informáticos, toda información de interés de una organización se guardaba en papel, y se almacenaba en grandes cantidades de abultados archivadores. Datos de clientes, proveedores de la organización o empleados quedaban registrados en papel, con todos los problemas que luego acarreaba, su almacenaje, transporte, acceso y procesado.

Los Sistema informáticos permiten la digitalización de grandes cantidades de volumen de información, reduciendo el espacio ocupado, pero sobre todo facilitando su análisis y procesado, se gana espacio, acceso, rapidez en el procesado de dicha información, y se garantiza mejor presentación de la información[28].

El sistema informático está compuesto por software, hardware, recurso humano, que permite el desarrollo eficiente y eficaz en la digitalización de la información.

La imagen 4. Recursos sistema informático, describe los recursos informáticos de una entidad.

[27] ESPAÑA. PORTAL DE ADMINISTRACION ELECTRONICA. MAGERIT v.3: Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Libro 1. 2012.
[28] ESPAÑA, GOBIERNO DE EDUCACION CULTURA Y DEPORTE, Monográfico Introducción a la seguridad informática/seguridad de la información, 2012.P2. Disponible en internet: http://recursostic.educacion.es/observatorio/web/ca/software/software-general/1040-introduccion-a-la-eguridad-informatica?start=1

Ilustración 4. Recursos sistema informático

Fuente: ALEGSA. Definición del sistema informático.Santafe.Argentina.1997-2017, Disponible en: http://www.alegsa.com.ar/Dic/sistema_informatico.php

El objetivo de un sistema de gestión de seguridad de la información es proteger la información, para ello lo primero que debe es identificar los activos que deben ser protegidos y en qué grado.

Un activo de acuerdo a lo estitpulado en la ISO 27001, son los recursos del sistema de seguridad de la informacion, necesaria para que la empresa funcione y consiga los objetivos que se ha propuesto en la alta direccion[29].

La imagen 5. Descripción del activo, permite observar con claridad que es un activo en su totalidad.

Ilustración 5. Descripción del activo

Fuente: Collazos Balaguer. M. La nueva version ISO 27001:2013. Peru. Un cambio de integracion de los tsistemas de gestion.p.17

[29] BLOG ESPECIALIZADO EN SISTEMAS DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN. ISO 27001:Los activos de información. 30 de Marzo 2015. Disponible en internet: http://www.pmg-ssi.com/2015/03/iso-27001-los-activos-de-i

A continuacion se presenta el listado que de algunos activos de información que se deben tener en cuenta, de acuerdo a su categoria, para desarrollar el inventario de activos en la organización.

Datos digitales

- Personales
- Financieros
- Légales
- Correo electrónico
- Contestadores automáticos
- Bases de datos
- Copias de seguridad

Software de aplicación

- Propietario desarrollo por la organización
- Cliente
- Planificación de recursos empresariales
- Gestión de la información
- Utilidades
- Herramientas de bases de datos
- Aplicaciones de comercio electrónico

Sistemas operativos

- Servidores
- Ordenadores de sobremesa
- Dispositivos de red
- Dispositivos de mano

Activos físicos

- Edificios
- Centros de datos
- Habitaciones de equipos y servidores
- Armarios de red
- Oficinas
- Escritorios
- Cajones
- Archivadores
- Salas de almacenamiento
- Dispositivos de identificación
- Control de acceso de personal
- Autentificación
- Otros dispositivos de seguridad

Hardware de tecnologías de la información (TI)

- Dispositivos de almacenamiento
- Ordenadores de mesa
- Estaciones de trabajo
- Ordenadores portátiles
- Equipos de mano
- Modem
- Líneas de terminación de red
- Dispositivo de comunicación
- Equipos multifunción

Activos de servicios tecnologías de la información (TI)

Servicios de Autenticación de usuario

- Administración de procesos
- Enlaces
- Contrafuegos
- Servidores proxy
- Servidores de red
- Servidores inalámbricos
- Anti-Spam
- Virus
- Spyware
- Detección y prevención de intrusos
- Teletrabajo
- Seguridad
- Correo electrónico
- Mensajería instantánea
- Servicios web
- Contrato de soporte
- Mantenimiento de software

Activos humanos

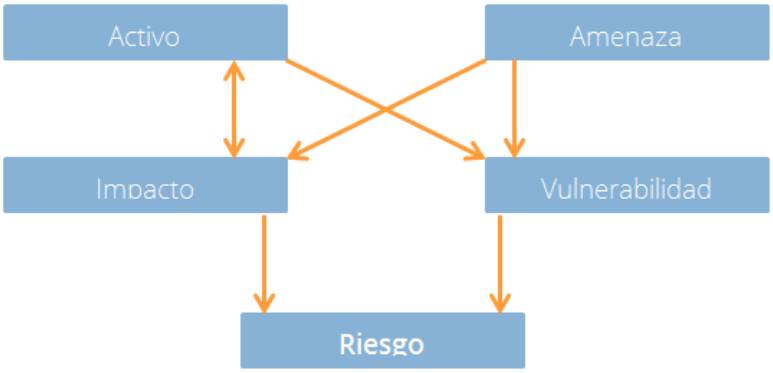
- Personal y directivos
- Arquitectos de software y desarrolladores
- Administradores de sistemas
- Administradores de seguridad
- Operadores
- Auditores
- Usuarios con poder
- Expertos en general

Externos

- Trabajadores temporales
- Consultores externos
- Asesores especialistas
- Contratistas especializados
- Proveedores
- Socios[30]

Los activos se encuentran relacionados con las demás entidades de acuerdo al siguiente esquema, representado en la imagen 6. Esquema relación del activo.

Ilustración 6. Esquema relación del activo



Fuente: Blog especializado en sistemas de gestión de seguridad de la información. ISO 27001: Los activos de información. 30 de Marzo 2015. Disponible en internet: http://www.pmg-ssi.com/2015/03/iso-27001-los-activos-de-i

Platear un sistema de gestión de seguridad de la información (SGSI), es un proceso que nunca termina, ya que los riesgos nunca se eliminan, pero se pueden gestionar, de los riesgos se desprende que los problemas de seguridad no son únicamente de naturaleza tecnológica, por este motivo nunca se eliminan en su totalidad.

Al no ser un tema tecnológico únicamente, la seguridad de la información siempre va a tener presente las vulnerabilidades, amenazas que conllevan a los riesgos.

Vulnerabilidad**:** Es la incapacidad de resistencia, cuando se presenta un fenómeno amenazante o la incapacidad para reponerse después de que ha ocurrido una amenaza.[31]

Amenaza: Es un fenómeno o proceso natural causado por el ser humano que ponen en peligro a las personas la información, las empresas, las amenazas

[30] BLOG ESPECIALIZADO EN SISTEMAS DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN. ¿Cómo realizar un inventario de activos de información? Activos de informacion.23 de Febrero 2017.disponible en internet: http://www.pmg-ssi.com/2017/02/realizar-inventario-activos-de-informacion/

[31]UNISDR. ¿Qué significa vulnerabilidad? Disponible en internet: http://www.unisdr.org/2004/campaign/booklet-spa/page8-spa.pdf

pueden ser causadas por el usuario, programas maliciosos, un intruso, un siniestro (robo, desastres naturales,), personal interno de sistemas, operadores.[32]

Riesgo: Es la probabilidad que una amenaza se convierta en un desastre, al unirse la vulnerabilidad y las amenazas representan un riesgo[33]

2.3 ANTECEDENTES

Diseño de un sistema de gestión de seguridad de la información para una entidad financiera de segundo piso, IGM S.A es un banco de segundo piso, también conocidos como bancos de desarrollo o bancos de fomento, cuyos recursos de crédito son desembolsados a los usuarios de los créditos a través de otras instituciones financieras.

La entidad cuenta con la infraestructura tecnológica adecuada y tiene implementado una serie de mecanismos de seguridad, tanto físicos como lógicos, con el propósito de poder proteger la confidencialidad, integridad y disponibilidad de la información del negocio y la privacidad de los datos de los clientes que residen en sus bases de datos. a pesar de contar con estos recursos tecnológicos y tener implementadas medidas de seguridad, la entidad no cuenta con los mecanismos adecuados y expeditos que le permitan conocer el estado real de su seguridad en cuanto a personas, procesos y tecnología, ni el nivel de efectividad de las medidas de seguridad que tiene implementadas, lo que dificulta o impide identificar y por ende gestionar de manera efectiva los riesgos asociados a la seguridad de sus activos de información y las amenazas que puedan llegar con comprometer la integridad, disponibilidad y confidencialidad de su información.

IGM S.A, requiere diseñar, implementar y mantener un sistema de gestión de seguridad de la información mediante un conjunto coherente de procesos para la gestión eficaz de acceso a la información. Se requiere como conocer el estado actual de sus activos de información, clasificarlos, priorizarlos y determinar su valor en caso de pérdida de información, lo que implica que es necesario que se conozcan los posibles riesgos que afectan la seguridad de la información y se establecen los mecanismos para minimizar el impacto en caso de presentarse la materialización de una vulnerabilidad.

El alcance del proyecto abarca el diseño un sistema de gestión de seguridad de la información para la empresa IGM s.a., el cual está orientado a cubrir la primera fase de la implementación de un sistema de gestión de seguridad de la información, que corresponde a la etapa de planeación.

[32] Vulnerabilidad. Disponible en internet: https://es.scribd.com/document/323783504/Que-Significa-Vulnerabilidad

El alcance del proyecto abarca solo el proceso de gestión de tecnología, para la sede principal de la entidad, por lo tanto, el proceso de clasificación de activos de información y valoración de riesgos solo se realizará para este proceso.
para el desarrollo del proyecto se utilizará como guía principal la norma NTC-ISOIEC 27001 versión 2013, que corresponde a un estándar referente a nivel mundial que especifica los requisitos necesarios para establecer, implantar, mantener y mejorar un sistema de gestión de seguridad de la información[34].

2.4 MARCO LEGAL

2.4.1 Ley Estatutaria 527 de 1999[35]

"Por medio de la cual se define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales".

2.4.2 Ley 1341 de 2009[36]

"Estableció el marco general del sector de las Tecnologías de la Información y las Comunicaciones, incorporando principios, conceptos y competencias sobre su organización y desarrollo e igualmente señaló que las Tecnologías de la Información y las Comunicaciones deben servir al interés general y, por tanto, es deber del Estado promover su acceso eficiente y en igualdad de oportunidades a todos los habitantes del territorio nacional".

2.4.3 Decreto 2578 de 2012[37]

"Por el cual se reglamenta el sistema nacional de archivos, se establece la red nacional de archivos, se deroga el decreto 2124 de 2004, y se dictan otras disposiciones relativas a la administración de los archivos del Estado".

[34] GUZMAN SILVA. Carlos. Alberto. Diseño de un sistema de gestión de seguridad de la información para una entidad financiera de segundo piso. Institución Universitaria POLITÉCNICO GRANA COLOMBIANO. Bogotá D. C. 2015. P13-17. Disponible en internet: http://repository.poligran.edu.co/bitstream/handle/10823/654/Proyecto%20de%20Grado%20SGSI%20-%20IGM-%20CarlosGuzman%20%28FINAL%29.pdf?sequence=1&isAllowed=y

[35] COLOMBIA. CONGRESO DE LA REPUBLICA. Ley 527 de 1999. Bogotá. (agosto 21 de 1999).Diario oficial N°43.673 de 21 de Agosto de 1999.

[36]COLOMBIA. CONGRESO DE LA REPUBLICA. Ley 1341 de 2009. Bogotá. (30 de Julio de 2009). Diario oficial N| 47.426 de 30 de Julio de 2009.

[37] COLOMBIA. CONGRESO DE LA REPUBLICA. DECRETO 2578 de 2012**.** Bogotá. (13 de Diciembre de 2012). Diario Oficial N° 48.648 del 13 de Diciembre de 2012.

2.4.4 Decreto Número - 2573 DE 2014[38]

"Por el cual se establecen los lineamientos generales de la Estrategia de Gobierno en línea, se reglamenta parcialmente la Ley 1341 de 2009 y se dictan otras disposiciones".

2.4.5 Ley 1273 DE 2009[39]

"Por medio de la cual se modifica el Código Penal, se crea un nuevo bien tutelado denominado "de la protección de la información y los datos" y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones".

2.4.6 Ley 1341 DE 2009[40]

"Por medio de la cual se definen principios y conceptos sobre la sociedad de la información y la organización de las tecnologías de la información y comunicaciones - TIC, se crea la Agencia Nacional de Espectro y se dictan otras disposiciones".

2.4.7 Ley 1150 DE 2007[41]

"Por medio de la cual se introducen medidas para la eficiencia y la transparencia en la Ley 80 de 1993 y se dictan otras disposiciones generales sobre la contratación con Recursos Públicos".

2.4.8 Ley 599 DE 2000[42]

"Por la cual se expide el Código Penal. Se crea el bien jurídico de los derechos de autor e incorpora algunas conductas relacionadas indirectamente con los delitos informáticos como el ofrecimiento, venta o compra de instrumento apto para interceptar la comunicación privada entre personas, y manifiesta que el acceso abusivo a un sistema informático protegido con medida de seguridad o contra la voluntad de quien tiene derecho a excluirlo, incurre en multa".

---

[38] COLOMBIA. CONGRESO DE LA REPUBLICA. Decreto 2573 De 2014. Bogotá. (12 de Diciembre de 2014). Diario oficial N° 49.523 del 12 de Diciembre de 2012.
[39] COLOMBIA. CONGRESO REPUBLICA DE COLOMBIA. ley 1273 de 2009. (Enero 5 2009).Diario oficial N° 47.223 del 5 de Enero de 2009.
[40] COLOMBIA. CONGRESO DE LA REPUBLICA. Ley 1341 de 2009. Bogotá. (30 de Julio de 2009).Diario oficial 47.426 de 30 de Julio de 2009.
[41] COLOMBIA. CONGRESO DE LA REPUBLICA. Ley 1150 DE 2007. Bogotá. (Septiembre 20 de 2007). Diario oficial N| 46.757 de 20 de Septiembre 2007.
[42] COLOMBIA. CONGRESO REPUBLICA DE COLOMBIA. Ley 599 DE 2000. (24 de Julio de 2000). Diario oficial N° 44.097 del 24 de Julio de 2000.

2.4.9 Ley 1712 2014[43]

“Por medio de la cual se crea la ley de transparencia y del derecho de acceso a la información pública nacional y se dictan otras disposiciones”.

2.4.10 Decreto 1078 del 26 de Mayo de 2015[44]

“Por el cual se expide el Decreto Único Reglamentario Del Sector De Tecnologías De La Información Y Las Comunicaciones”

2.4.11 Decreto 19 de 2012[45]

“Por el cual se dictan normas para suprimir o reformar regulaciones, procedimientos o trámites innecesarios existentes en la Administración Publica.”

[43] COLOMBIA.CONGRESO DE LA REPUBLICA. Ley 1712 2014.Bogota. (6 Marzo 2014). Diario Oficial N° 49.084 de 6 de Marzo de 2014.
[44] COLOMBIA, CONGRESO DE LA REPUBLICA. Decreto 1078 de 2015. Bogotá. (26 Mayo 2015). Diario oficial 49.523. 26 de Mayo de 2015.
[45] COLOMBIA. CONGRESO REPUBLICA DE COLOMBIA. Decreto 19 de 2012. Bogotá. (10 de Enero de 2012). Diario oficial N° 48.308 de 10 de Enero de 2012.

3.REVISAR EL ESTADO ACTUAL DE LA SEGURIDAD DE LA INFORMACIÓN EN LA ALCALDÍA MUNICIPAL DE GUACHETÁ

3.1 INTRODUCCION

La alcaldía municipal de Guachetá es una entidad pública, de orden gubernamental, donde no existe un Sistema de gestión de seguridad de la información (SSGI) definido, se presentan demasiadas falencias en la protección de los activos, a continuación se presenta el análisis realizado a la entidad, mediante visitas a cada una de las dependencias, entrevistas con el funcionario del área de sistemas, y demás funcionarios responsables del manejo de los equipos.

3.2 DESCRIPCION ALCALDIA MUNICIPAL DE GUACHETA

3.2.1 Razón social

Alcaldía Municipal de Guachetá Cundinamarca
Sector: Publico
Guachetá es un municipio al norte de Cundinamarca (Colombia). Conocido gracias a su gran producción de carbón mineral de primera calidad y los abundantes hatos de ganado lechero, se ha dado a conocer como la "Ciudad Carbonífera y Lechera de Colombia".
Guachetá en lengua muisca significa "Labranza de nuestro cerro" o "Labranza del Mancebo"

3.2.2 Misión

Servir a la comunidad, promover la prosperidad general y garantizar la efectividad de los principios, derechos y deberes consagrados en la Constitución; facilitar la participación de todos en las decisiones que los afectan y en la vida económica, política, administrativa y cultural de la Nación; defender la independencia nacional, mantener la integridad territorial y asegurar la convivencia pacífica y la vigencia de un orden justo[46].

3.2.3 Visión

Guachetá en el 2019, será un municipio que crece en su economía siendo productivo, competitivo y sostenible; socialmente equitativo e incluyente; fraterno,

[46]ALCALDIA MUNICPAL. Misión Guachetá. Marzo 2017. Disponible en internet: http://www.guacheta-cundinamarca.gov.co/quienes_somos.shtml#mision

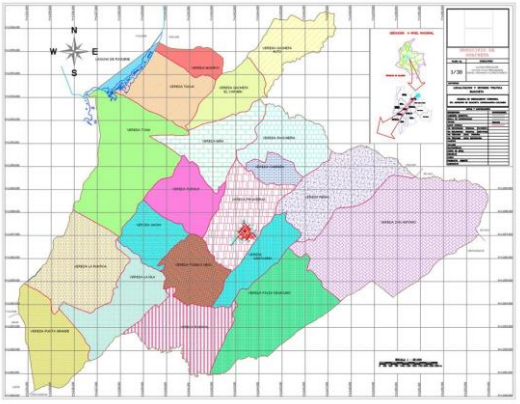
ordenado, protector de su medio ambiente. Un municipio para vivir bien, para visitar y disfrutar[47].

3.2.4 Ubicación Geográfica

Guachetá está ubicado en la Provincia de Ubaté, se encuentra a 118 km de Bogotá por vía terrestre, se comunica por carretera con los Municipios de Ubaté, Lenguazaqué, Samacá, Ráquira y Fúquene.

Su área total es de 177.45 Km2 (17.745 Ha) según el plano catastral escala 1:10000. Se encuentra entre los pisos térmicos frío y páramo cuya temperatura oscila entre los 12º y 13º y la precipitación se presenta entre 832 mm y 746.5 mm. La Cabecera Municipal se localiza a los 5º23”15´. De latitud Norte y a los 73º41”20´ de longitud al Oeste del Meridiano Greenwich y a una altitud de 2688 m.s.n.m. Dista de Santafé de Bogotá a 118 Km[48]. Las ilustración 7 y 8 permite observar la división política del municipio, y área Urbana.

Ilustración 7. Mapa municipio de Guachetá



Fuente. GUACHETA. Esquema ordenamiento territorial.2000.anexo

Ilustración 8. Ubicación geográfica área urbana

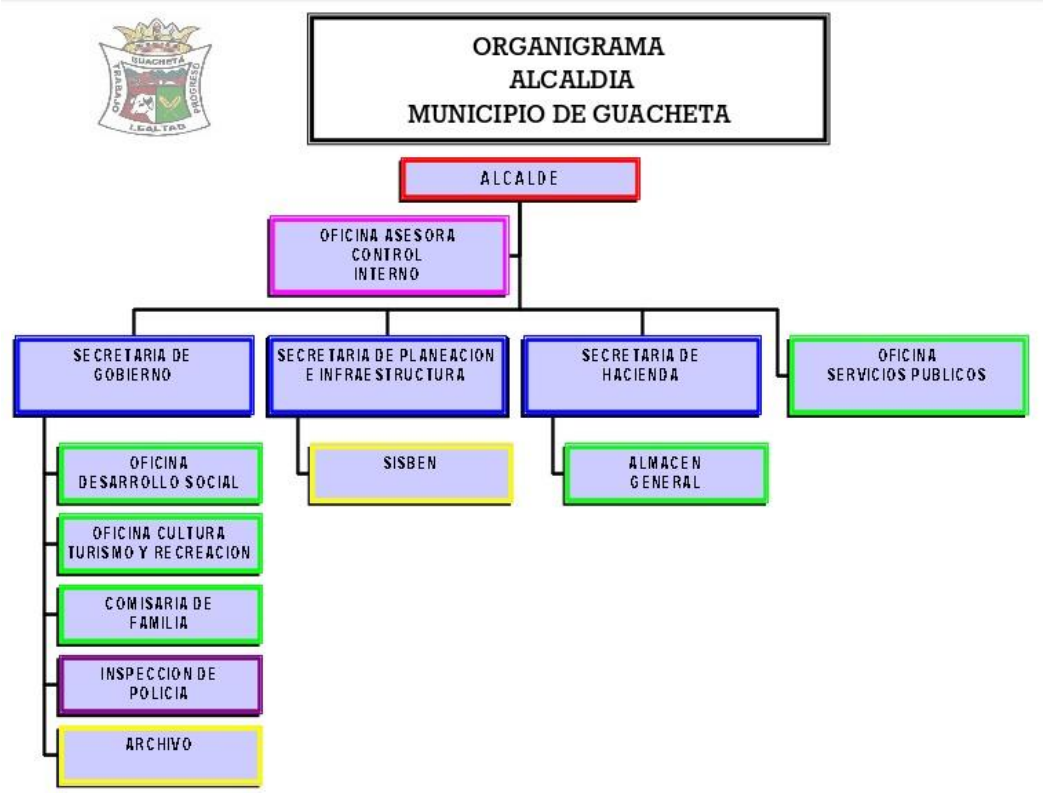
Fuente: google maps

[47] ALCALDIA MUNICPAL. Op.Cit. http://www.guacheta-cundinamarca.gov.co/quienes_somos.shtml#vision
[48]ALCALDIA MUNICPAL DE GUACHETA. Op. cit., http://www.guacheta-cundinamarca.gov.co/informacion_general.shtml#geografia

3.3 ESTRUCTURA ORGANIZACIONAL

La estructura organizacional de la alcaldía municipal está divida de acuerdo al organigrama. Se observa en la ilustración 9.

Ilustración 9. Organigrama Alcaldía Municipal De Guachetá



Fuente: COLOMBIA. Alcaldía municipal de Guachetá. Organigrama alcaldía municipal de Guachetá. Internet: http://guacheta-cundinamarca.gov.co/apc-aa-files/353035623266393663396661313038 64/organigrama.jpg

3.4 AREA DE SISTEMAS

3.4.1 Caracterización del área de sistemas

El área de sistemas de la alcaldía municipal de Guachetá no es identificable, para realizar la función de proteger la información de la entidad existe el contrato de un ingeniero de sistemas.

3.4.1.1 Objetivos

- Garantizar la seguridad de los activos informáticos de la alcaldía municipal de Guachetá
- Brindar orientación sobre la protección de la información de la entidad.

3.4.1.3 Descripción de cargos y funciones.

En el área de sistemas labora el ingeniero de sistemas, profesional quien actualiza los diferentes sistemas de información de acuerdo a las normas legales, publicación, actualización de los procesos de contratación en el portal SECOP y el mantenimiento preventivo de la granja de servidores de la administración municipal.

Funciones:

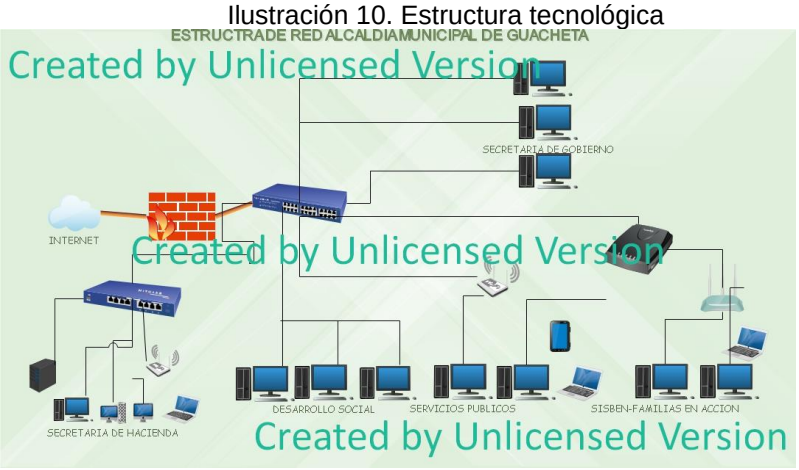
- Realizar la administración del sistema de información del municipio de Guachetá. Actualizar los sistemas de información, equipos de cómputo y demás equipos y elementos que hagan parte del inventario de la red de datos del municipio.
- Realizar la revisión técnica de cada uno de los equipos para establecer su estado actual. (Diagnostico).
- Realizar copias de seguridad o Backup como mínimo cada dos meses de los equipos de cómputo de todas las dependencias, inclusive la OMATAA.
- Prestar el apoyo necesario para garantizar el servicio de internet en cuanto a problemas generados en las redes y equipos internos.
- Prestar el apoyo necesario cuando se requieran traslados de redes de servicios de cómputo.
- Sugerir a través del supervisor del contrato la aplicación de cambios de tecnologías, programas etc., que conlleven a la optimización de los servicios.
- Realizar mantenimiento preventivo de los equipos de cómputo y de las redes de datos del municipio, según diagnóstico, en actividades como instalación, activación y actualización de antivirus, programas y aplicaciones, revisión del sistema del sistema operativo y limpieza de archivos temporales.
- Cargar la información a las diferentes entidades gubernamentales, entes de control y demás entidades que lo requieran, en especial dar cumplimiento a las fases del sistema de Gobierno en línea.
- Publicar los diferentes documentos, archivos y procedimientos de los diferentes procesos de selección de contratistas, conforme a lo señalado en la Ley 80 de 1993, Ley 1150 de 2007, Decreto 1082 de 2015, artículo 94 de la Ley 1474 de 2011, Decreto 019 de 2012 y demás normas que así lo contemplen, todo ello bajo la supervisión y dirección del responsable del proceso de contratación o de la información suministrada.
- Cargar la información que sea solicitada por las diferentes dependencias.
- Actualizar permanentemente la página web del municipio.
- Apoyar a la administración municipal en todas las actividades relacionadas con el objeto a contratar.
- Consolidar los informes de avance de la gestión para ser presentados al consejo de gobierno o informes al Honorable Concejo Municipal.
- Realizar brigadas de mantenimiento preventivo y correctivo de los computadores en las salas de sistemas de las instituciones educativas del municipio.

- Administrar las cuentas de correo electrónico institucional en aspectos como creación, restablecimiento de contraseñas, cierre de cuentas.
- Llevar el inventario de los equipos de cómputo de la alcaldía.
- Apoyar la actualización del Sistema de Información y Gestión del Empleo Público SIGEP.
- Presentar los informes requeridos por el supervisor en forma mensual sobre el estado de las actividades realizadas, anexando la relación pormenorizada de las mismas.

3.4.1.3 Infraestructura tecnológica

La red de la alcaldía municipal de Guachetá, está estructurada bajo la topología de estrella, la imagen 10. Infraestructura de red, permite observar la estructura.

Ilustración 10. Estructura tecnológica



Fuente: Propiedad del Autor, diseñado con el programa Edraw Max, versión prueba

3.4.1.4 Políticas de uso para la utilización de equipos de cómputo

- Realizar backup de los equipos de cómputo cada mes.
- Usar contraseñas seguras, de alto grado de complejidad.
- Apagar los equipos al terminar la jornada laboral.
- No instalar programas no autorizados
- Instalar en los equipos software antispyware.

3.4.1.5 Políticas de uso para la utilización del INTERNET

- El servicio de internet es de uso exclusivo para realizar funciones a cargo.
- Escribir la dirección web en la barra de navegador, no seguir enlaces.
- No suministrar información personal.
- No ingresar a YouTube, si no es necesario para cumplir las funciones a cargo.

3.5 SISTEMAS DE INFORMACION

En la alcaldía municipal de Guachetá siendo un ente territorial y público se manejan diferentes sistemas de información como:

- HASSQL: Software administrativo y financiero, donde se evidencia entradas, procesos y egresos de la entidad, está instalado en servicios públicos, secretaria de hacienda, almacén.

- SIFA: Sistema de información de Mas Familias En Acción, es una plataforma nacional, donde el municipio tiene acceso a través de usuario y clave, este sistema permite contiene toda la información de las familias que pertenecen al programa, en el municipio realizan novedades de los datos de las familias, ingresan datos, descargan reportes, y realizan consultas, instalada en el equipo de la oficina de Mas Familias En Acción.

- SICRESUB: Software local que contiene la información de los usuarios del régimen subsidiado del municipio, instalado en los equipos de la oficina de SISBEN y Aseguramiento.

- PLATAFORMA SISBEN LOCAL: Sistema de identificación de potenciales beneficiarios, es la plataforma municipal donde se ingresa los datos de los habitantes del municipio que solicitan la encuesta del SISBEN, para acceder subsidios, instalado en los equipos de la oficina de SISBEN y Aseguramiento.

- VIVANTO: Es la plataforma que permite realizar la consulta de la población víctima del conflicto armado, se puede consultar: historial grupo familiar y hecho victimizante, ayudas y beneficios, módulo de acreditación, ingreso y selección del servicio de novedades, novedades de actualización de datos, instalado en secretaria de Gobierno.

- SECOP: Sistema único de contratación pública, en esta plataforma la entidad realiza el cargue de la contratación para cada vigencia, plataforma nivel nacional, el usuario y clave es entregada a la secretaria de Gobierno.

- SIGEP: Sistema de información del empleo público al servicio de la administración pública y de los ciudadanos, contiene información, plataforma nivel nacional, el usuario y clave es entregada a la secretaria de Gobierno.

- SIA OBSERVA: Sistema información de auditoria, a través de este portal se realiza el cargue del rubro afectado para cada contrato realizado con la entidad, plataforma nivel nacional, el usuario y clave es entregada a la secretaria de Gobierno.

- SIRECI: Sistema de rendición electrónica de cuentas e informes, a través de esta plataforma local, control interno descarga los formatos de informes que debe entregar a la contraloría general de la nación, usuario y clave entregada a la oficina de control interno.

- MANGO: Monitoreo alimentario y nutricional gobernación de Cundinamarca, a través de este aplicativo se registra el estado nutricional de niñas y niños del municipio de acuerdo al reporte entregado por la ESE, usuario y clave entregado a la oficina de Desarrollo social, coordinación PIC (plan de intervenciones colectivas)

3.6 SERVICIOS QUE PRESTA

La administración pública es uno de los actores más importantes en el desarrollo de un país, es una interacción directa con los habitantes del territorio, es así que esta entidad brinda servicios a la comunidad de acuerdo a cada una de las áreas, y necesidades públicas, estas necesidades están vinculadas directamente al bienestar social, a las metas establecidas por la administración municipal, buscando prestar servicios de calidad.

3.6.1 Encuesta SISBEN: Ser encuestado para ingresar al SISBEN, cuando un hogar no ha sido encuestado por primera vez.

3.6.2 Actualización de datos ficha imagen del SISBEN: Obtener la corrección /actualización de la información que haya cambiado de uno o más miembros de las personas registradas en las bases de datos.

3.6.3 Factura impuesto predial unificado: Entrega de la factura

3.6.4 Vinculación EPS subsidiada**:** Aceptación de formularios para ingreso a una EPS subsidiada.

3.6.5 Actualización de datos y consulta: información beneficiarios Mas Familias en Acción.

3.6.6 Facturación acueducto y alcantarillado: ingreso de información de consumo de agua, cuota de alcantarillado y basura, entrega de factura.

3.6.7 Licencias de construcción: Expedición de licencias de construcción.
Pago de impuesto de rentas.

3.6.8 Paz y salvo industria y comercio.

3.6.9 Paz y salvo impuesto predial.

3.6.10 Certificado de estratificación**:** Certificar el estrato socio-económico de uno o varios inmuebles residencias del área urbana o rural que estén dentro del municipio.

3.6.11 Recepción de correspondencia.

3.6.12 Querellas.

3.6.13 Conciliaciones.

3.6.14 Extra juicios, Autenticación de documentos.

3.7 PROCEDIMIENTOS ACTUALES

A través de la gestión del ingeniero de sistemas se realiza la creación de correos electrónicos institucionales por medio de solicitud escrita al programa Gobierno en Línea.

3.8 INSPECCION VISUAL DE LOS ACTIVOS DE INFORMACION

3.8.1 Software y aplicaciones

Los equipos en su totalidad no cuentan con licencia del sistema operativo, no existe restricciones para la instalación de aplicaciones en los equipos, cuentas creadas con perfil de usuario, están creadas desde el administrador, el antivirus no está actualizado en todos los equipos, las bases de datos no tienen seguridad, puede acceder cualquier usuario, contraseñas de seguridad nula. Los equipos no cuentan con firewall activado.

3.8.2 Hardware

Se visualiza equipos Obsoletos para realizar ciertas tareas, problemas de procesador, memoria RAM, ocasionalmente se produce volcamiento de memoria RAM, los equipo se encuentran en el suelo sin soporte, puertos USB, deteriorados, memorias USB en cualquier lugar sin mayor cuidado, no existe seguridad de los equipos de cómputo, están bajo riesgo de humedad.

Mala distribución de los monitores, CPU´s, teclados, mouse y demás herramientas del Taller de Soporte correctivo. Este desorden facilitaría la perdida de información, equipos y herramientas necesarias para el adecuado desempeño de esta área.

3.8.3 Red

Los routers, switch, no están instalados en los mejores lugares, están al acceso de todo personal, contraseñas inseguras, configuración que permite el acceso de todos los equipos en el caso del WIFI.

3.8.4 Equipamiento auxiliar

Son muy pocos los equipos que tienen una UPS, esto hace que se presente perdida de información en el momento de bajonazos de luz inesperados y daños físicos a los equipos. Imagen [15].

- No se utilizan paneles de obturación para el cableado en la sala de servidores.
- No se encontró sistema de marquillas en los cables de datos y cables de energía.
- Los cables de datos se encuentran enredados con los cables de energía siendo esto uno de los generadores de ruido en el cableado de datos.
- Se observa que en la sala de servidores no se realiza una limpieza periódica en cuanto a contaminación por polvo y/o suciedad, que podría causar averías de origen físico o lógico en los servidores, UPS, evaporadora y demás.
- El sistema eléctrico de la unidad no cuenta con protección contra electrocución por contacto directo o indirecto en las áreas de trabajo.
- No están por separado los circuitos de la red regulada y normal.

3.8.5 Servicios

Se tiene acceso de conectividad a internet, algunos equipos el acceso a través de cable y otros a través de WIFI, se presentan intermitencias en el servicio, regularmente se hace mantenimiento.

3.8.6 Personal

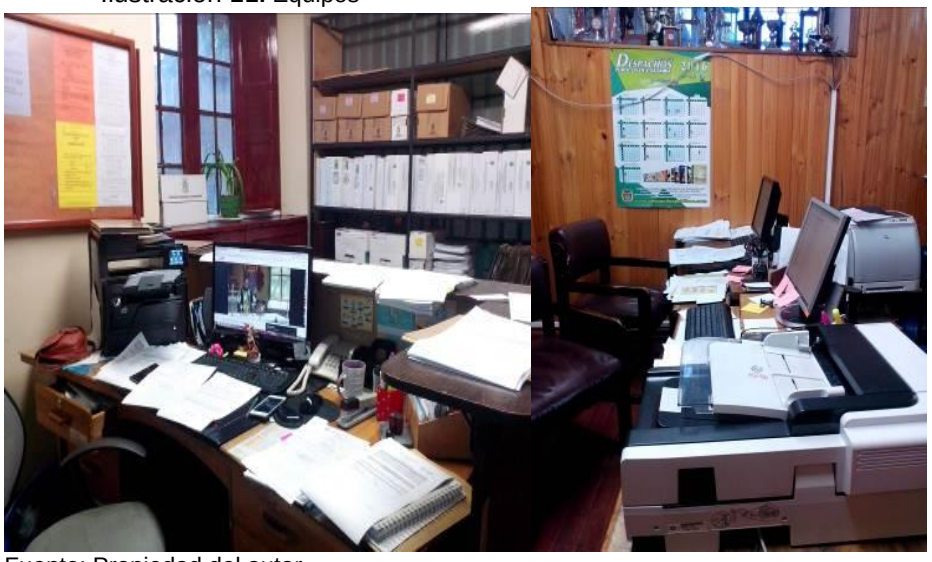
El personal no está capacitado en el tema de seguridad informática, desconocen la importancia y el valor de la información que a diario manejan, existe solo el ingeniero de sistemas encargado de toda la empresa en el tema de informática y seguridad. No existen políticas de seguridad informática.

3.8.7 Información

No se da buen manejo a la seguridad de la información, se evidencia documentos al acceso de todas las personas, con información valiosa en algunas oficinas, otras oficinas manejan adecuadamente el archivo, de forma digital y física.

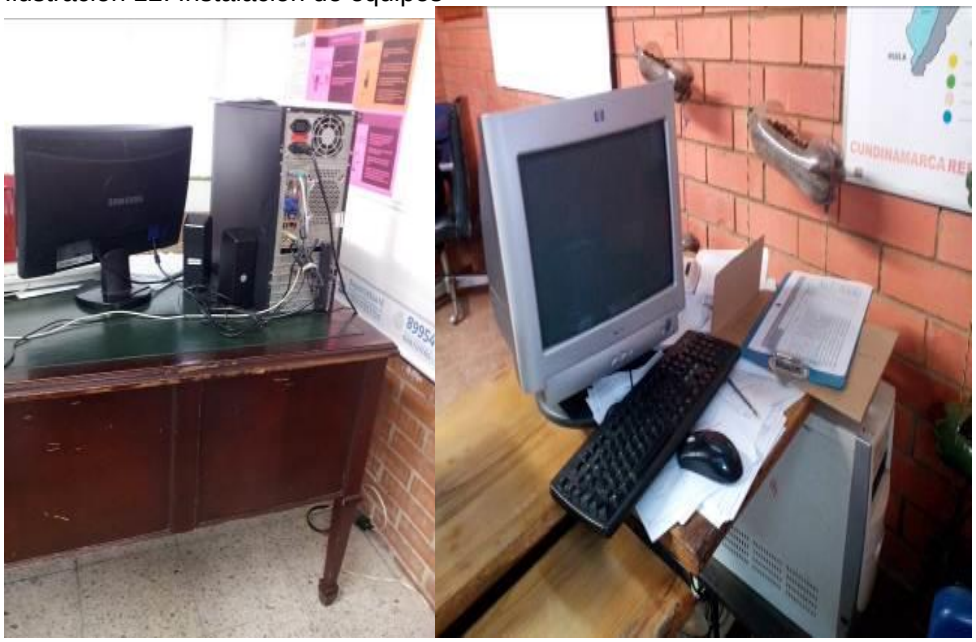
A continuación se realiza la descripción visual de los activos de la entidad, relacionados de la Ilustración 11 a la 15.

Ilustración 11. Equipos



Fuente: Propiedad del autor

Ilustración 12. Instalación de equipos



Fuente: Propiedad del autor

Ilustración 13. Instalación de Cableado

Fuente: Propiedad del autor

Ilustración 14. Instalación UPS

Fuente: Propiedad del autor

Ilustración 15. Organización de la informacion

Fuente: Propiedad del autor

4.LASIFICAR LOS ACTIVOS DE INFORMACIÓN CON QUE CUENTA LA ALCALDÍA MUNICIPAL DE GUACHETÁ, UTILIZANDO LA METODOLOGÍA MAGERIT V3

4.1 INTRODUCCION

La información es el activo más importante de las entidades, es así que la alcaldía municipal de Guachetá se rige bajo este principio, para proteger su información requiere de un sistema robusto que garantice que todos sus activos estén protegidos, seguros y salvaguardados.

Para el desarrollo del presente capitulo, se realiza la clasificación de los activos de información de la alcaldía municipal de Guachetá utilizando la metodología MAGERIT V3.

4.2 CALIFICACION DE LA INFORMACION

La información se consolida como uno de los activos más importantes para las organizaciones, convirtiéndose en el recurso vital para la gestión y la toma de decisiones.

Es preciso que todos los funcionarios y contratistas que se encuentran desarrollando alguna labor con la Entidad, comprendan el impacto que podría tener la pérdida y/o divulgación de la información considerada como clasificada o reservada que se encuentre a su cargo[49].

4.2.1 METODOLOGÍA DE LA CALIFICACIÓN DE LA INFORMACIÓN

La información debe ser protegida apropiadamente contra el acceso no autorizado, modificación, divulgación, pérdida o destrucción, sin importar la fuente en donde esté almacenada (computadores, librerías, portátiles, medios extraíbles como discos duros externos, USB, CD, DVD, Blu-Ray. Etc., contratos, documentos, comunicaciones verbales, etc.). Desde éste punto de vista, es importante determinar el papel que cumplen las entidades y funcionarios que por diversos motivos están involucrados en el tratamiento de la información[50].

Es de vital importancia que en la identificación de la calificación de la información, sea el jefe de la dependencia o del área responsable de la generación, posesión, control o custodia de la información, quien asuma la responsabilidad de definir y

[49] PRESIDENCIA DE LA REPUBLICA, Guía para la clasificación de la información de acuerdo con sus niveles de seguridad. Bogotá D. C. (Marzo de 2007). P3.Dispponible en internet: http://es.presidencia.gov.co/dapre/DocumentosSIGEPRE/G-GD-02-calificacion-informacion.pdf
[50] Ibíd., P8.

justificar los casos en que se debe restringir ya que de ésta manera se garantiza que la calificación sea razonable y proporcionada[51].

Pasos para realizar la clasificación de la información

4.2.1.1 Paso 1 identificar la información a cargo: Las tablas de retención documental son el insumo necesario para realizar la calificación de la información, de igual forma se debe realizar entrevistas con los productores documentales en las que es posible evaluar el tipo de información producida, los medios empleados para su almacenamiento y/o divulgación, los controles existentes y requeridos.

Al agrupar la información por categorías que faciliten la descripción, calificación, disponibilidad y controles de acceso estas son representadas como series y subseries de las Tablas de Retención Documental. Se debe tener en cuenta que la información se presenta en diferentes soportes y formatos:

Soporte

- Documentos en papel: cartas, informes, soportes contables, documentos legales, historias laborales, contratos etc.
- Discos compactos, discos duros, DVD, Blu-ray
- Correo electrónico, intranet, internet
- Rollos de microfilmación, casetes
- Mapas, planos, dibujos, fotografías
- Publicaciones, libros

Formato

- TEXTO: .doc .txt .rtf .pdf
- HOJA DE CÁLCULO: .xls .xlt .csv
- PRESENTACIONES: .ppt .pps
- DOCUMENTOS GRÁFICOS: .jpg .gif .png .tif .ttf
- BASES DE DATOS: .mdb .sql
- AUDIO: .wav .mid .mp3 .ogg
- VIDEO: .mpeg .avi .mov

4.2.1.2 Paso 2 Establecer la calificación de la información: La calificación de la información identificada corresponde directamente al jefe de la dependencia.

La calificación que se asigna a la categoría de información determinará los controles requeridos para su custodia, almacenamiento y acceso, además es importante asumir la calificación que manifieste su productor ya sea una persona, una empresa u otra entidad y debe contemplarse de acuerdo a:

[51]Ibíd., P8-9.

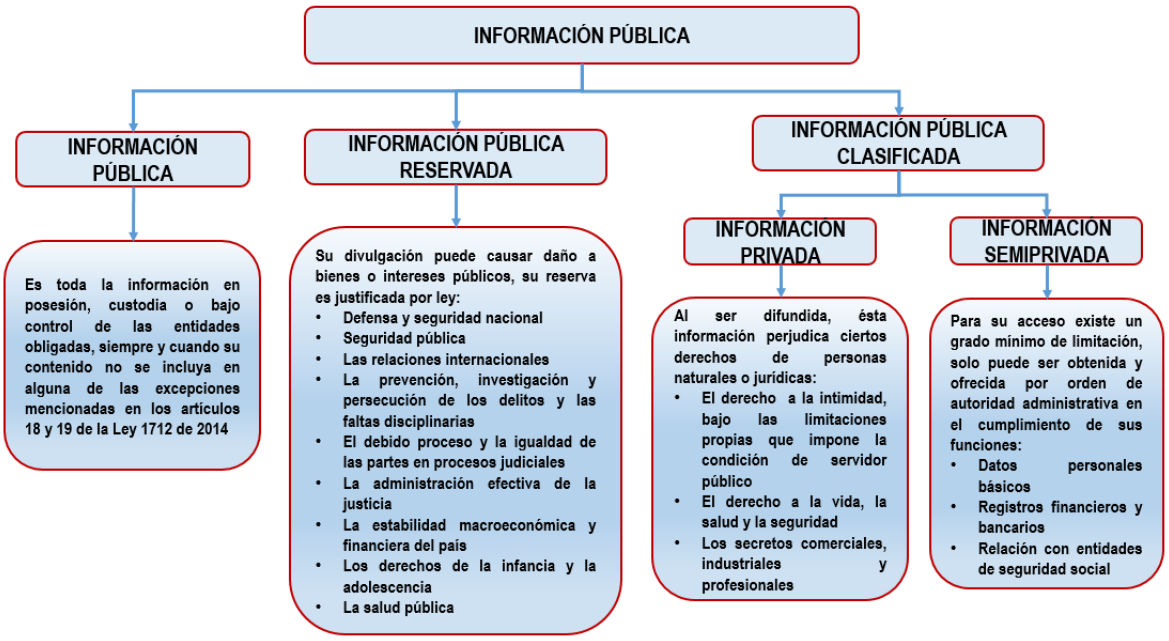
Información pública: Es toda información que un sujeto obligado genere, obtenga, adquiera, o controle en su calidad de tal. (Artículo 5 Ley 1712 de 2014).

Información clasificada: Es toda aquella que al ser divulgada puede llegar a causar daño a algunos derechos individuales de personas naturales o jurídicas por contener información relacionada con la intimidad y privacidad de éstas. (Artículo 18 Ley 1712 de 2014).

Información reservada**:** Su divulgación indebida puede afectar bienes o intereses públicos. (Artículo 19 Ley 1712 de 2014).

La ilustración 16 muestra permite observar la clasificación de la información.

Ilustración 16. Calificación de la información



Fuente: PRESIDENCIA DE LA REPUBLICA, Guía para la clasificación de la información de acuerdo con sus niveles de seguridad. Bogotá D. C. (Marzo de 2007). P12.Dispponible en internet: http://es.presidencia.gov.co/dapre/DocumentosSIGEPRE/G-GD-02-calificacion-informacion.pdf

4.2.1.3 Paso 3 Definir las medidas de protección para las clases de información: después de identificado y calificado la información se establecen los mecanismos de protección de la información, teniendo en cuenta su disposición final de acuerdo a la tabla de retención documental.

Para este proceso se debe tener en cuenta las políticas de seguridad de la información, estos controles pueden ser copias electrónicas, fotocopias (sin generar duplicidad de la información), controles de acceso, digitalización, controles biométricos, Los esquemas de protección del activo de información deben ser coordinados entre el propietario, el responsable de la información y el comité de

seguridad informática y deben ser consecuentes con la disposición final indicada en las Tablas de Retención Documental.

Algunas medidas recomendables para la protección de la información son:

Autenticación: El mecanismo más simple es usar clave para acceder a los datos, igualmente, huella digital, identificación biométrica entre otras, así se protege la confidencialidad.

Acceso basado en roles: otorgar acceso a las bases de datos si es necesario para que el funcionario cumpla sus funciones.

Cifrado de datos: mecanismo para prevenir acceso no autorizado a la información, en el caso de la información de acceso a las aplicaciones y transacciones financieras.

Controles administrativos: como procedimiento de segregación funciones, procedimiento de control de cambios, rotación de funciones, vacaciones obligatorias.

Aseguramiento: garantizar que los equipos estén protegidos, se puede llegar a realizar auditoria de sistemas, pruebas de intrusión, evaluación de desempeño de sistemas de información, supervisión administrativa, supervisión de acceso a datos.

4.2.1.4 Paso 4 registrar la información en la herramienta de calificación de la información: El jefe de cada dependencia (Área, Dirección, Consejería, Secretaría, etc.) como responsable de la información, deberá designar por medio de comunicación escrita dirigida a los jefes del Área Administrativa y del Área de Tecnología y Sistemas de Información, un funcionario responsable de registrar la información correspondiente a su dependencia, se sugiere asignar personal de alta confianza quien será habilitado por el Área de Tecnología y Sistemas de Información para ejecutar ésta tarea.

4.2.1.5 Paso 5 Validación de la información registrada en la herramienta para la calificación de la información: Después que cada dependencia realice el registro adecuado, a través de un comité y responsable del archivo deberán analizar los datos registrados por cada dependencia y validar las justificaciones para la calificación asignada, detectando posibles errores en el registro los cuales serán notificados formalmente al responsable de la información (jefe de dependencia) para que tome las medidas correctivas del caso.

El Área de Tecnología y Sistemas de Información y el Grupo de Gestión Documental del Área Administrativa, realizarán de manera semestral la validación de la información registrada en la herramienta de calificación de la información, de

ser necesario, solicitarán al responsable de la información (jefe de la dependencia) la actualización o ajustes necesarios que correspondan.

4.2.1.6 Paso 6 Implementación de controles: De acuerdo a los controles que se definan, se ejecutan las actividades necesarias para garantizar que los controles se realicen monitoreando continuamente su efectividad.

4.2.1.7 Paso 7 Consolidar inventario de activos de información de la entidad: El Área de Tecnología y Sistemas de Información realiza la compilación de todos los registros realizados por las dependencias obteniendo como resultado el Inventario de los Activos de Información[52].

4.3 ACTIVOS INFORMATICOS

Se realiza una descripción detallada de los activos informáticos, de acuerdo a lo que establece el libro II de MAGERIT V3.

Tabla 2. Activos

Tipo de activo MAGERIT	Código del activo	Activos más relevantes en la entidad
[esential] Activos esenciales	[adm] datos de interés para la administración publica	Convenios interadministrativos OPS Datos de proyectos terminados Proyectos en ejecución Egresos
	[vr] Datos vitales	Resoluciones Edictos
	[per] datos de carácter personal	Historia laboral personal de planta
[SW] Software Aplicaciones informáticas	[Office]	Microsoft Office 2010 Microsoft Office 2007
	[browser] Navegador web	Internet Explorer 11 Crome Mozilla
	[dbms] sistema de gestión de bases de datos	SICRESUB Gestor de bases de datos HASS SISBENet MFA MANGO VIVANTO SIA OBSERVA

[52]Ibíd., P12-18.

Tipo de activo MAGERIT	Código del activo	Activos más relevantes en la entidad
[SW] Software de aplicaciones	[av] Antivirus	Avanst
	[OS] Sistema operativo	Sistema Operativo Windows 8 (7 -Lic.) Sistema Operativo Windows 7 (17-Lic.) Sistema Operativo Windows XP (8 - Lic.)
	[backup] sistema de backup	Backup
[Aux] Equipamiento Auxiliar Instalaciones	[gen]generadores eléctricos	UPS_2
	[Supply]Suministros esenciales	papel, carpetas, catálogos, tinta tóner
	[cabling] cableado	Cableado Estructurado Cat. 5E Conectores RJ45 Jack RJ45 Canaleta
	[wire] cable eléctrico	Cableado eléctrico
	[furniture] mobiliario	Escritorios Archivadores Estantes
[L] Instalaciones	[building] edificio	Edificio
	[local] cuarto	Sala de sistemas
[P] Personal	[adm] Administrador de sistemas	Funcionarios de oficina área administrativa, sistemas
	[ue] Usuario externo	Jefe de aplicativos
	[ui] Usuario Interno	Funcionarios
[D] Datos/Información	[Int] Datos de gestión interna	Archivos de proyectos Archivos de interventorías Archivos de contratistas Archivos de proyectos Archivos de interventorías Acciones administrativas Acción de tutela Acción popular Actas Soportes de Recaudos Querellas Manuales de aplicativo Documentos legales Inventarios Licencias Denuncios Auditoria interna Tablas de retención documental

	[backup] copias de respaldo	Archivos de copias de seguridad de la información
	[conf] Datos de configuración	Datos de configuración de servidores
	[D_Gestión de proyectos]	Datos de gestión de proyecto de ejecución.
	[Password] credenciales	Contraseñas de acceso de usuarios del sistema
[K] Claves Criptográficas	[Sing] clave de firma	Firma digital Alcalde
[S] Servicios	[int] inteno	Servicio de internet de los funcionarios
	[Ext] usuarios externos	Soportes contratos Liquidaciones
	[pub] al publico	Extra juicios Autenticaciones Denuncios Facturas
	[E-mail] correo electrónico	Correos electrónicos
[HW] Equipamiento informático (hardware)	[Pc] Informática personal	Equipos Portátiles Equipos de Escritorio
	[mobile] informática móvil (4)	Celulares
	[Routers] encaminadores	Routers
	[Swicht] conmutadores	Swicht – 2
	[print] medios de impresión	Impresoras
	[scan] escáneres	Escáneres
	[Crypto] dispositivos criptográficos	Token
	[wap] punto de acceso inalámbrico	Antena inalámbrica
	[firewall] Cortafuegos	Firewall
[COM]Redes De Comunicación	[[LAN]) Red Local	Red Local
	[wifi] red inalámbrica	Wifi
	[Mobile] telefonía móvil	Red telefónica móvil
	[Internet]	Internet
[Media] Soporte De Información	[printed]	Soportes de los proyectos en ejecución. Soportes de Egresos Soportes de obligaciones financieras. Soportes Bases de Datos Soportes de Actas
	[disk] Discos	Almacenamiento disco duro externo
	[usb] usb	Almacenamiento memoria USB
	[vdisk] Discos virtuales	Almacenamiento disco duro virtuales
	[dvd] DVD	Almacenamiento de información DVD
	[cd] Cederrón (CD-ROM)	Almacenamiento de información CD

Fuente. Propiedad del autor

4.4 CLASIFIACION DE LOS ACTIVOS DE INFORMACION

Habiendo realizado la verificación de los activos, se procede a clasificar la información de acuerdo a lo establecido en la guía para la calificación de la información de acuerdo con sus niveles de seguridad.

Tabla 3. Clasificación activos de información

Tipo de activo MAGERIT	Código del activo	Nombre del activo	Clasificación de la información
[esential] Activos esenciales	[adm] datos de interés para la administración publica	Convenios interadministrativos OPS Datos de proyectos terminados Proyectos en ejecución Egresos	Información Pública
	[vr] Datos vitales	Resoluciones Edictos	Información Pública/Reservada
	[per] datos de carácter personal	Historia laboral personal de planta	información Privada
[sw] Software/aplicación	[backup] sistema de backup	Backup	Información Publica
[D] Datos/Información	[Int] Datos de gestión interna	Archivos de proyectos Archivos de interventorías Archivos de contratistas	Información semiprivada
		Archivos de proyectos Archivos de interventorías Acciones administrativas Acción de tutela Acción popular Actas Soportes de Recaudos Querellas Manuales de aplicativo Documentos legales Inventarios Licencias Denuncios Auditoria interna Tablas de retención documental	
	[backup] copias de respaldo	Archivos de copias de seguridad de la información	Información Privada
	[conf] Datos de configuración	Datos de configuración de servidores	

Tipo de activo MAGERIT	Código del activo	Nombre del activo	Clasificación de la información
[D] Datos/Información	[D_Gestión de proyectos]	Datos de gestión de proyecto de ejecución.	Información Privada
	[Password] credenciales	Contraseñas de acceso de usuarios del sistema	
[K] Claves Criptográficas	[Sing] clave de firma	Firma digital Alcalde	Información semiprivada
[S] Servicios	[Ext] usuarios externos	Soportes contratos Liquidaciones	
	[pub] al publico	Extra juicios Autenticaciones Denuncios Facturas	Información Privada
	[E-mail] correo electrónico	Correos electrónicos	
[Media] Soporte De Información	[printed]	Soportes de los proyectos en ejecución. Soportes de Egresos Soportes de obligaciones financieras. Soportes Bases de Datos Soportes de Actas	
	[disk] Discos	Almacenamiento disco duro externo	
	[usb] usb	Almacenamiento memoria USB	
	[vdisk] Discos virtuales	Almacenamiento disco duro virtuales	
	[dvd] DVD	Almacenamiento de información DVD	
	[cd] Cederrón (CD-ROM)	Almacenamiento de información CD	

Fuente: Propiedad del autor

4.5 DIMENSIONES DE VALORACION

Son las características o atributos que hacen valioso un activo. Una dimensión es una faceta o aspecto de un activo, independiente de otras facetas.

Las dimensiones se utilizan para valorar las consecuencias de la materialización de una amenaza.

La valoración que recibe un activo en una cierta dimensión es la medida del perjuicio para la organización si el activo se ve dañado en dicha dimensión[53].

4.5.1 De acuerdo a las dimensiones de seguridad

Las dimensiones a tener en cuenta son las establecidas en el numeral 4 del libro II MAGERIT, sobre criterios de valoración.

4.5.1.1 Criterios de valoración

[D] Disponibilidad: Tener la disponibilidad de los activos cuando se requiere.
[I] Integridad de los datos: El activo de información no debe ser alterado de forma inescrupulosa.
[C] Confidencialidad de la información: No se permite revelar la información a personas no autorizadas.
[A] Autenticidad: Garantizar la fuente que proporciona los datos.
[T] Trazabilidad: Las actuaciones de una entidad deben ser imputadas exclusivamente a esta.

4.5.1.2 Valoración de los activos. A continuación se muestra en la tabla 5 la valoración cualitativa de los activos, teniendo en cuenta las dimensiones de seguridad.

Tabla 4 Valoración Cualitativa De Activos

Tipo de activo MAGERIT	**Nombre de activos**	**Clasificación de la información**	**Valoración de los activos**					
			[D]	**[I]**	**[C]**	**[A]**	**[T]**	**Prom**
[esential] Activos esenciales	Convenios interadministrativos OPS Datos de proyectos terminados Proyectos en ejecución Egresos	Información Pública	7	7	7	7	6	6,8
	Resoluciones Edictos Historia laboral personal de planta	Información Pública/Reservada información Privada						

[53] ESPAÑA. Ministerio De Hacienda Y Administraciones Pública. MAGERIT Versión 3.0. Metodología de análisis y gestión de riesgos de los sistemas de información. Libro II. Madrid Octubre 2012. P.15. Disponible en internet: https://es.scribd.com/document/128378588/MAGERIT-III-Libro-II-Catalogo-de-Elementos

Tipo de activo MAGERIT	Nombre de activos	Clasificación de la información	Valoración de los activos					
			[D]	[I]	[C]	[A]	[T]	Prom
[sw] Software/aplicación	Backup	Información Publica						
[D] Datos/Información	Archivos de proyectos Archivos de interventorías Archivos de contratistas Archivos de proyectos Archivos de interventorías Acciones administrativas Acción de tutela Acción popular Actas Soportes de Recaudos Querellas Manuales de aplicativo Documentos legales Inventarios Licencias Denuncios Auditoria interna Tablas de retención documental	Información semiprivada	8	9	9	9	7	8,4
	Archivos de copias de seguridad de la información							
	Datos de configuración de servidores	información Privada						
	Datos de gestión de proyecto de ejecución.							

Tipo de activo MAGERIT	Nombre de activos	Clasificación de la información	Valoración de los activos					
			[D]	[I]	[C]	[A]	[T]	Prom
[K] Claves Criptográficas	Firma digital Alcalde Contraseñas	información Privada	6	7	7	6	6	6,2
[S] Servicios	Soportes contratos Liquidaciones	información Semiprivada	7	7	6	6	6	6,4
	Extra juicios Autenticaciones Denuncios Facturas	información Privada						
	Correos electrónicos							
[Media] Soporte De Información	Soportes de los proyectos en ejecución. Soportes de Egresos Soportes de obligaciones financieras. Soportes Bases de Datos Soportes de Actas		7	7	7	7	6	6.8
	Almacenamiento disco duro externo							
	Almacenamiento memoria USB							
	Almacenamiento disco duro virtuales							
	Almacenamiento de información DVD							
	Almacenamiento de información CD							

Fuente: Propiedad del autor

4.5.2 De acuerdo al impacto

Para valorar los activos vale, teóricamente cualquier escala de valores a efectos prácticos, es sin embargo es muy importante que:}
Se use una escala común para todas las dimensiones, permitiendo comparar riesgos.
Se use una escala logarítmica, centrada en diferencias relativas de valor, y no en diferencias absolutas

Se use un criterio homogéneo que permita comparar análisis realizados por separado[54].

4.5.2.1 Criterios de valoración

Se ha elegido una escala detallada de diez valores, dejando en valor 0 como determinante de lo que sería un valor despreciable (a efectos de riesgos)[55].

Tabla 5 Criterios de valoración de los activos

Valor		Criterio
10	Extremo	Daño Extremadamente grave a la organización
9	Muy alto	Daño Muy grave a la organización
6-8	Alto	Daño Grave a la organización
3-5	Medio	Daño importante a la organización
1-2	Bajo	Daño Menor
0	Despreciable	Irrelevante para la organización

Fuente: De acuerdo a MAGERIT V3 libro 2 Catalogo de elementos

Muy Alto (MA)
Alto (A)
Medio (M)
Bajo (b)
Muy bajo (MB)

4.5.1.2 Valoración de los activos. Se realiza de acuerdo a lo estipulado en el libro II MAGERIT, numeral 4.1.

[54] ESPAÑA. Ministerio De Hacienda Y Administraciones Pública. MAGERIT Versión 3.0. Metodología de análisis y gestión de riesgos de los sistemas de información. Libro II. Madrid Octubre 2012. P.19. Disponible en internet: https://es.scribd.com/document/128378588/MAGERIT-III-Libro-II-Catalogo-de-Elementos

[55] ESPAÑA. Ministerio De Hacienda Y Administraciones Pública. MAGERIT Versión 3.0. Metodología de análisis y gestión de riesgos de los sistemas de información. Libro II. Madrid Octubre 2012. P.19. Disponible en internet: https://es.scribd.com/document/128378588/MAGERIT-III-Libro-II-Catalogo-de-Elementos

Tabla 6 valoración de los activos Libro II MAGERIT

Tipo de activo MAGERIT	Código del activo	Activos más relevantes en la entidad	Impacto	Descripción
[esential] Activos esenciales	[adm] datos de interés para la administración publica	Convenios interadministrativos OPS Datos de proyectos terminados Proyectos en ejecución Egresos	3.adm	Probablemente impediría la operación efectiva de una parte de la organización. .
	[vr] Datos vitales	Resoluciones Edictos		
[D] Datos/Información	[D_Gestión de proyectos]	Datos de gestión de proyecto de ejecución.		
[esential] Activos esenciales	[per] datos de carácter personal	Historia laboral personal de planta	3.lro	Probablemente sea causa de incumplimiento leve o técnico de una ley o regulación.
[SW] Software Aplicaciones informáticas	[Office]	Microsoft Office 2010 Microsoft Office 2007	5.adm	Probablemente impedirá la operación efectiva de más de una parte de la organización.
[P] Personal	[adm] Administrador de sistemas	Funcionarios de oficina área administrativa, sistemas		
	[ue] Usuario externo	Jefe de aplicativos		
	[ui] Usuario Interno	Funcionarios		
[SW] Software Aplicaciones informáticas	[browser] Navegador web	Internet Explorer 11 Crome Mozilla		
	[dbms] sistema de gestión de bases de datos	SICRESUB Gestor de bases de datos HASS SISBENet MFA MANGO VIVANTO SIA OBSERVA	3.olm	Probablemente merme la eficacia y seguridad de la misión operativa o logística (área local)
	[av] Antivirus	Avanst		

[S] Servicios	[OS] Sistema operativo	Sistema Operativo Windows 8 (7 -Lic.) Sistema Operativo Windows 7 (17-Lic.) Sistema Operativo Windows XP (8 - Lic.)	3.olm	Probablemente merme la eficacia y seguridad de la misión operativa o logística (área local)
	[int] inteno	Servicio de internet de los funcionarios		
	[Ext] usuarios externos	Soportes contratos Liquidaciones		
	[pub] al publico	Extrajuicios Autenticaciones Denuncios Facturas		
[SW] Software Aplicaciones informáticas	[backup] sistema de backup	Backup	6.lbl	Difusión limitada
[Aux] Equipamiento Auxiliar Instalaciones	[gen]generadores eléctricos	UPS_2	1.da	Pudiera causar interrupción de actividades propias de la organización.
	[Supply]Suministros esenciales	papel, carpetas, catálogos, tinta tóner		
	[cabling] cableado	Cableado Estructurado Cat. 5E Conectores RJ45 Jack RJ45 Canaleta		
	[wire] cable eléctrico	Cableado eléctrico		
	[furniture] mobiliario	Escritorios Archivadores Estantes		
[D] Datos/Información	[Int] Datos de gestión interna	Archivos de proyectos interventorías contratistas interventorías Acciones administrativas Acción de tutela Acción popular Actas Soportes de Recaudos Querellas Manuales de aplicativo Documentos legales Inventarios Licencias Denuncios Auditoria interna Tablas de retención documental		

Tipo de activo MAGERIT	Código del activo	Activos más relevantes en la entidad	Impacto	Descripción
[L] Instalaciones	[building] edificio	Edificio	7.olm	Probablemente perjudique la eficacia o seguridad de la misión operativa o logística.
	[local] cuarto	Sala de sistemas		
[D] Datos/Información	[backup] copias de respaldo	Archivos de copias de seguridad de la información	7.si	Probablemente se causa de un grave incidente de seguridad o dificulte la investigación de incidentes graves.
[S] Servicios	[E-mail] correo electronico	Correos electrónicos		
[HW] Equipamiento informático (hadware)	[Pc] Informática personal	Equipos Portátiles Equipos de Escritorio		
[Media] Soporte De Información	[disk] Discos	Almacenamiento disco duro externo		
	[usb] usb	Almacenamiento memoria USB		
	[vdisk] Discos virtuales	Almacenamiento disco duro virtuales		
	[dvd] DVD	Almacenamiento de información DVD		
	[cd] Cederrón (CD-ROM)	Almacenamiento de información CD		
[D] Datos/Información	[conf] Datos de configuración	Datos de configuración de servidores	7.adm	Probablemente impediría la operación efectiva de la organización.
[D] Datos/Información	[Password] credenciales	Contraseñas de acceso de usuarios del sistema	10.lbl	Secreto
[K] Claves Criptográficas	[Sing] clave de firma	Firma digital Alcalde	7.lbl	Confidencial
[S] Servicios	[E-mail] correo electrónico	Correos electrónicos	7.si	Probablemente sea causa de un grave incidente de seguridad o dificulte la investigación de incidentes graves.

Tipo de activo MAGERIT	Código del activo	Activos más relevantes en la entidad	Impacto	Descripción
[HW] Equipamiento informático (hardware)	[mobile] informática móvil (4)	Celulares	3.da	Probablemente cause la interrupción de actividades propias de la organización.
	[Routers] encaminadores	Routers		
	[Swicht] conmutadores	Swicht – 2		
	[print] medios de impresión	Impresoras		
	[scan] escáneres	Escáneres		
	[Crypto] dispositivos criptográficos	Token		
	[wap] punto de acceso inalámbrico	Antena inalámbrica		
	[firewall] Cortafuegos	Firewall		
[COM]Redes De Comunicación	[[LAN]) Red Local [wifi] red inalámbrica	Red Local Wifi	3.da	Probablemente cause la interrupción de actividades propias de la organización.
	[Mobile] telefonía móvil	Red telefónica móvil		
	[Internet]	Internet	3.da	Probablemente cause la interrupción de actividades propias de la organización.
[Media] Soporte De Información	[printed]	Soportes de los proyectos en ejecución. Soportes de Egresos Soportes de obligaciones financieras. Soportes Bases de Datos Soportes de Actas	6.pi2	Probablemente quebrante seriamente la ley o algún reglamento de protección de información personal.

Fuente: Propiedad del autor

5.DETERMINAR LAS AMENAZAS Y RIESGOS A QUE ESTÁN EXPUESTOS LOS ACTIVOS DE INFORMACIÓN

El desarrollo del presente capitulo, muestra las amenazas posibles sobre los activos del sistema de información de la alcaldía municipal de Guachetá.

5.1 IDENTIFICACION Y VALORACION DE AMENAZAS

La identificación de las amenazas se realiza de acuerdo a la siguiente clasificación del numeral 5 del libro II de MAGERIT.

Tabla 7 Amenazas

Nomenclatura	Tipos de amenaza
[N] Desastres naturales	[N.1] Fuego [N.2] Daños por agua [N.*] Desastres naturales
[I] De origen industrial	[I.1] Fuego [I.2] Daños por agua [I*] Desastres industriales [I.3] Contaminación mecánica [I.4] Contaminación electromagnética [I.5] Avería de origen físico o lógico [I.6] Corte del suministro eléctrico [I.7] Condiciones inadecuadas de temperatura o humedad [I.8] Fallo de servicios de comunicaciones [I.9] Interrupción de otros servicios o suministros esenciales [I.10] Degradación de los soportes de almacenamiento de la información [I.11] Emanaciones electromagnéticas
[E] Errores y fallos no intencionados	[E.1] Errores de los usuarios [E.2] Errores del administrador [E.3] Errores de monitorización (log) [E.4] Errores de configuración [E.7] Deficiencias en la organización [E.8] Difusión de software dañino [E.9] Errores de [re-]encaminamiento [E.10] Errores de secuencia [E.14] Fugas de información [E.15] Alteración de la información [E.16] Introducción de falsa información

Nomenclatura	Tipos de amenaza
	[E.17] Degradación de la información [E.18] Destrucción de la información [E.19] Divulgación de información [E.20] Vulnerabilidades de los programas (software) [E.21] Errores de mantenimiento / actualización de programas (software) [E.23] Errores de mantenimiento / actualización de equipos (hardware) [E.24] Caída del sistema por agotamiento de recursos [E.25] Pérdida de equipos [E.28] Indisponibilidad del personal
[A] Ataques intencionados	A.4] Manipulación de la configuración [A.5] Suplantación de la identidad del usuario [A.6] Abuso de privilegios de acceso [A.7] Uso no previsto [A.8] Difusión de software dañino [A.9] [Re-] encaminamiento de mensajes [A.10] Alteración de secuencia [A.11] Acceso no autorizado [A.12] Análisis de tráfico [A.13] Repudio [A.14] Interceptación de información (escucha) [A.15] Modificación de información [A.16] Introducción de falsa información [A.17] Corrupción de la información [A.18] Destrucción de la información [A.19] Divulgación de información [A.22] Manipulación de programas [A.23] Manipulación de equipos [A.24] Denegación de servicio [A.25] Robo de equipos [A.26] Ataque destructivo [A.27] Ocupación enemiga [A.28] Indisponibilidad del personal [A.30]Ingeniería Social

Fuente: Propiedad del autor

La identificación de amenazas que se presenta en la tabla 8 se realiza de acuerdo a lo estipulado en el libro II de Magertit.

Tabla 8 Identificación de amenazas

Tipo de amenaza	Amenaza
[N.1] Fuego	Incendio
[N.2] Daños por el agua	Humedad, inundación
[N.*] Desastres naturales	Fenómeno sísmico Contaminación
[I.5] Avería de origen físico o lógico	Falla del funcionamiento del hardware.
[I.6] Corte del suministro eléctrico	Fallas en el suministro de energía.
[I.8] Fallo de servicios de comunicaciones	Perdida de los medios de telecomunicación.
[I.9] Interrupción de otros servicios o suministros esenciales	No suministro de papelería, tóner.
[I.10] Degradación de los soportes de almacenamiento de la información	Avería del hardware
[E.1] Errores de los usuarios	Perdida de contraseñas. Mal ingreso de la información bases de datos. Descuido en la custodia de la información.
[E.2] Errores del administrador	Entregar información privada. Error de configuración de los pc.
[E.7] Deficiencias en la organización	No existen funciones propias para la protección de los activos.
[E.8] Difusión de software dañino	Propagación inocente de virus, spyware.
[E.14] Escapes de información	Disponibilidad de la información a terceros.
[E.15] Alteración de la información	Accesos a los equipos sin control. Acceso a carpetas sin control.
[E.18] Destrucción de la información	Desconocimiento de procesos.
[E.19] Fugas de información	Revelación por indiscreción.
[E.20] Vulnerabilidades de los programas (software)	Actualizaciones de software sin permisos. Instalación de programas sin autorización.
[E.21] Errores de mantenimiento / actualización de programas (software)	Perjuicio a la mantenibilidad del sistema de información. Falla funcionamiento del software.
[E.23] Errores de mantenimiento / actualización de equipos (hardware)	Perjuicio a la mantenibilidad del sistema de información.

Tipo de amenaza	Amenaza
[E.24] Caída del sistema por agotamiento de recursos	Saturación del sistema informático.
[E.25] Pérdida de equipos	Falta de equipos para desarrollar las actividades. Fuga de información.
[E.28] Indisponibilidad del personal	Abandono puestos de trabajo. Falta de confidencialidad. Falta de custodia de la información.
A.4] Manipulación de la configuración	Cambios de configuración de los equipos por parte de los funcionarios.
[A.5] Suplantación de la identidad del usuario	Usurpación de derecho.
[A.6] Abuso de privilegios de acceso	Abuso de nivel de privilegios para realizar tareas que no son propias de sus funciones.
[A.7] Uso no previsto	Consultas personales de internet. Bases de datos personales Descargas de internet. Programas personales. Juegos. Almacenamiento de datos personales.
[A.8] Difusión de software dañino	Propagación intencionada de virus.
[A.11] Acceso no autorizado	Uso ilícito del hardware.
[A.113] Repudio	Negación de acciones.
[A.14] Interceptación de información (escucha)	Escucha pasiva
[A.15] Modificación de información	Alteración intencional de la información.
[A.18] Destrucción de la información	Eliminación de información con toda la intención, para obtener beneficio propio.
[A.19] Divulgación de información	Divulgación Copia ilegal de software.
[A.22] Manipulación de programas	Alteración de programas.
[A.23] Manipulación de equipos	Sabotaje de hardware.
[A.24] Denegación de servicio	Saturación del sistema informático
[A.25] Robo	Robo de hardware. Robo de documentos.
[A.26] Ataque destructivo	Destrucción de hardware o documentos.
[A.28] Indisponibilidad del personal	Daño a la disponibilidad del personal.
[A.30]Ingeniería Social	Abuso de la buena fe de las personas.

Fuente: Propiedad del autor

5.1.1 Criterios de evaluación

Se presenta la identificación y evaluación las amenazas que sufren los activos de información de la unidad. La identificación de amenazas está basada en la clasificación de MAGERIT:

Tabla 9. Escala de rango frecuencia de amenazas

	Criterio	
Valor	Frecuencia	Rango de frecuencia
100	Frecuencia muy alta	1 vez al día
70	Frecuencia alta	1 vez cada semana
50	Frecuencia media	1 vez cada 2 meses
10	Frecuencia baja	1 vez cada 6 meses
5	Frecuencia muy baja	vez al año

Fuente: Propiedad del autor

5.1.2 Evaluación de las amenazas a los activos

La evaluación de las amenazas permite conocer el riesgo al que está expuesto el activo informático, a continuación se describe la frecuencia de vulnerabilidades, dimensiones de seguridad, impacto de las amenazas causados en los activos.

Tabla 10. Dimensiones

Dimensiones de Seguridad	Identificación
Autenticidad	A
Confiabilidad	C
Integridad	I
Disponibilidad	D
Trazabilidad	T

Fuente: Propiedad del autor

Escala de rango porcentual de impactos en los activos para cada dimensión de seguridad.

Tabla 11. Impactos de activos

Impacto	Valor Cuantitativo
Muy Alto	100%
Alto	70%
Medio	50%
Bajo	10%
Muy bajo	5%

Fuente: Propiedad del Autor

A continuación se presenta la identificación de las amenazas para cada activo, teniendo presente la frecuencia en impacto en cada dimensión, teniendo en cuenta las tablas 8,9 y 10.

Tabla 12. Identificación de amenazas por activo identificando su frecuencia e impacto

Tipos de activo	**Nombre de activos**	**Amenaza**	**FRECUENCIA**	**[D]**	**[C]**	**[I]**	**[A]**	**[T]**
[Esential] Activos esenciales	Convenios interadministrativos OPS Datos de proyectos terminados Proyectos en ejecución Egresos	[E.14] Escapes de información	50		50%			
	Resoluciones Edictos							
	Historia laboral personal de planta							
[D] Datos/Información	Datos de gestión de proyecto de ejecución.							

Tipos de activo	Nombre de activos	Amenaza	FRECUENCIA	[D]	[C]	[I]	[A]	[T]
[SW] Software Aplicaciones informaticas	Microsoft Office 2010 Microsoft Office 2007 SICRESUB GB DAT HASS SISBENet MFA MANGO VIVANTO SIA OBSERVA	[E.21] Errores de mantenimiento / actualización de programas (software)	50	70%		70%		
	Avanst							
	Sistema Operativo Windows 8 (7 - Lic.) Sistema Operativo Windows 7 (17- Lic.) Sistema Operativo Windows XP (8 - Lic.)							
	Internet Explorer 11 Crome Mozilla	[A.8] Difusión de software dañino	50	50%	50%	50%		
	Backup	[A.25] Robo	10	10%	100%			
[Aux] Equipamiento Auxiliar Instalaciones	UPS_2	[I.6] Corte del suministro eléctrico	50	50%				
	papel, carpetas, catálogos, tinta tóner	[I.9] Interrupción de otros servicios o suministros esenciales	10	10%				

Tipos de activo	Nombre de activos	Amenaza	FRECUENCIA	[D]	[C]	[I]	[A]	[T]
[Aux] Equipamiento Auxiliar Instalaciones	Cableado Estructurado Cat. 5E Conectores RJ45 Jack RJ45 Canaleta	[E.23] Errores de mantenimiento / actualización de equipos (hardware)	50	50%				
	Cableado eléctrico	[N.2] Daños por el agua	10	10%				
	Escritorios Archivadores Estantes							
[L] Instalaciones	Edificio	[N.*] Desastres naturales	10	10%				
	Sala de sistemas	[N.2] Daños por el agua	50	50%				
[P] Personal	Funcionarios de oficina área administrativa, sistemas	[A.28] Indisponibilidad del personal	50	50%				
	Jefe de aplicativos							
	Funcionarios	[A.30] Ingeniería social	70	70%	70%	70%		

Tipos de activo	Nombre de activos	Amenaza	FRECUENCIA	[D]	[C]	[I]	[A]	[T]
[D] Datos/Información	Archivos de proyectos interventorías de contratistas de proyectos Acciones administrativas Acción de tutela Acción popular Actas y demás.	[E.19] Fugas de información	50	50%				
	Archivos de copias de seguridad de la información	[E.18] Destrucción de la información	10	10%				
	Datos de configuración de servidores	[E.2] Errores del administrador	50	50%	50%	70%		
	Contraseñas de acceso de usuarios del sistema	[E.1] Errores de los usuarios	50	50%	70%	70%		
[K] Claves Criptográficas	Firma digital Alcalde	[A.5] Suplantación de la identidad del usuario	50	50%	50%		50%	
[S] Servicios	Servicio de internet de los funcionarios	[A.19] Divulgación de información	50		100%			
	Soportes contratos Liquidaciones	[A.5] Suplantación de la identidad del usuario	10	10%	10%	10%		
	Correos electrónicos	[A.7] Uso no previsto	70	70%	70%	70%		

Tipos de activo	Nombre de activos	Amenaza	FRECUENCIA	[D]	[C]	[I]	[A]	[T]
[HW] Equipamiento informático (hadware)	Equipos Portátiles Equipos de Escritorio Impresoras Escáner Firewall	[E.23] Errores de mantenimiento / actualización de equipos (hardware)	70	70%				
	Celulares	[A.7] Uso no previsto	70	70%	70%	70%		
	Routers Swicht – 2	[A.6] Abuso de privilegios de acceso	50	50%	50%	50%		
	Token	[E.2] Errores del administrador	10	10%	10%	10%		
[COM]Redes De Comunicación	Red Local	A.24] Denegación de servicios	10	10%				
	Wifi	[E.9] Errores de [re-] encaminamiento	50	50%				
	Red telefónica móvil	A.24] Denegación de servicios	50	50%				
	Internet	[A.7] Uso no previsto	100	100 %	100%	100 %		
[Media] Soporte De Información	Soportes de los proyectos en ejecución. Soportes de Egresos Soportes de obligaciones financieras. Soportes Bases de Datos Soportes de Actas	[A.26] Ataque destructivo	10	10%				

	Almacenamiento disco duro externo	[A.15] Modificación de información	10			10%		
	Almacenamiento memoria USB Almacenamiento de información CD Almacenamiento de información DVD	[E.18] Destrucción de la información	5	5%				
	Almacenamiento disco duro virtuales	[A.30]Ingeniería Social	50	50%	50%	50%		

Fuente: propiedad del autor

5.2 RIESGO POTENCIAL

5.2.1 Criterios de evaluación

El análisis y la evaluación del riesgo se hace mediante la siguiente formula:

RIESGO=PROBABILIDAD*IMPACTO

Se desarrolla el análisis por cada una de las variables, teniendo en cuenta una escala de 1 a 5 de la probabilidad y el impacto de acuerdo a los indicadores establecidos anteriormente.

Tabla 13. Identificación Impacto

Escalas			
#	Impacto	probabilidad	Riesgo
5	Muy Alto	A la semana.	Muy extremo
4	Alto	Al mes.	Extremo
3	Medio	En 6 meses.	Intolerable
2	Bajo	Al año.	Tolerable
1	Muy bajo	Puede ocurrir una vez cada 2 años.	Aceptable

Fuente: Propiedad del Autor

La medición del Nivel de Riesgo obedece al Mapa de Riesgos, que se describe a continuación:

Tabla 14. Mapa de Riesgos

PROBABILIDAD						
	5	5	10	15	20	25
	4	4	8	12	16	20
	3	3	6	9	12	15
	2	2	4	6	8	10
	1	1	2	3	4	5
		1	2	3	4	5
		IMPACTO				

NIVEL DE RIESGO	
5	Muy extremo
4	Extremo
3	Intolerable
2	Tolerable
1	Aceptable

Fuente. Propiedad del autor

5.2.2. Evaluación del riesgo potencial a los activos

A través de la evaluación del riesgo se conoce los riesgos a los que están sometidos los activos, para el desarrollo de esta actividad se utilizó MAGERIT V3. La empresa debe conocer los riesgos a que están expuestos los activos de la información, para estar preparada y generar estrategias de mejora y protección.

Tabla 15. Matriz de Riesgo

Tipos de activo	Nombre de activos	Impacto	Probabilidad	Riesgo
[Esential] Activos esenciales	Convenios interadministrativos OPS Datos de proyectos terminados Proyectos en ejecución Egresos	3	3	9
	Resoluciones Edictos			
	Historia laboral personal de planta			

Tipos de activo	Nombre de activos	Impacto	Probabilidad	Riesgo
[SW] Software Aplicaciones informáticas	Microsoft Office 2010 Microsoft Office 2007	4	4	16
	Internet Explorer 11 Crome Mozilla			
	SICRESUB Gestor de bases de datos HASS SISBENet MFA MANGO VIVANTO SIA OBSERVA			
	Avanst			
	Sistema Operativo Windows 8 (7 -Lic.) Sistema Operativo Windows 7 (17-Lic.) Sistema Operativo Windows XP (8 - Lic.)			
	Backup			
[Aux] Equipamiento Auxiliar Instalaciones	UPS_2	3	3	9
	papel, carpetas, catálogos, tinta tóner			
	Cableado Estructurado Cat. 5E Conectores RJ45 Jack RJ45 Canaleta			
	Cableado eléctrico			
	Escritorios Archivadores Estantes			
[L] Instalaciones	Edificio	3	2	6
	Sala de sistemas			
[P] Personal	Funcionarios de oficina área administrativa, sistemas	4	3	12

Tipos de activo	Nombre de activos	Impacto	Probabilidad	Riesgo
[D] Datos/Información	Archivos de proyectos Archivos de interventorías Archivos de contratistas Archivos de proyectos Archivos de interventorías Y demás documentación	3	4	12
	Archivos de copias de seguridad de la información	2	1	2
	Datos de configuración de servidores	2	2	4
[D] Datos/Información	Datos de gestión de proyecto de ejecución.	3	2	6
	Contraseñas de acceso de usuarios del sistema	3	2	6
[K] Claves Criptográficas	Firma digital Alcalde	4	2	8
[S] Servicios	Servicio de internet de los funcionarios	5	3	15
	Soportes contratos Liquidaciones	2	1	2
	Correos electrónicos	5	4	20
[HW] Equipamiento informático (hadware)	Equipos Portátiles Equipos de Escritorio Escáneres Impresoras Firewall	4	4	16
	Celulares	4	4	16
	Routers Swicht – 2	3	3	9
	Token	2	1	2
[COM]Redes De Comunicación	Red Local	2	2	4
	Wifi	4	4	16
	Red telefónica móvil	3	3	9
	Internet	4	5	20
[Media] Soporte De Información	Soportes de los proyectos en ejecución, Egresos, obligaciones financieras, Bases de Datos y Actas	2	2	4

[Media] Soporte De Información	Almacenamiento disco duro externo DVD USB CD disco duro virtuales	2	2	4

Fuente: Propiedad del Autor

6.APLICAR CONTROLES DE LA NORMA ISO 27001:2013 A LOS ACTIVOS DE INFORMACIÓN

Los controles de seguridad para la alcaldía municipal de Guachetá, se aplicaran bajo los estándares de la norma ISO 27001:2013, se desarrollara los siguientes controles, los que aplican para la entidad de acuerdo al análisis realizado.

- Políticas de seguridad
- Aspectos organizativos de la seguridad de la información
- Seguridad ligada a los recursos humanos
- Gestión de activos
- Control de accesos
- Criptografía
- Seguridad física y ambiental
- Seguridad en la operativa
- Seguridad de las comunicaciones
- Adquisición y mantenimiento de sistemas

6.1 OBJETIVOS DE CONTROL Y CONTROLES

Tabla 16 Controles de la Norma ISO/IEC 27001:2013

<table>
<tr><td>A.5</td><td colspan="2">POLÍTICAS DE SEGURIDAD</td></tr>
<tr><td>A.5.1</td><td colspan="2">Directrices establecidas por la dirección para la seguridad de la información.</td></tr>
<tr><td colspan="3">Objetivo: Brindar apoyo y orientación a la dirección con respecto a la seguridad de la información, de acuerdo con los requisitos del negocio y los reglamentos y las leyes pertinentes.</td></tr>
<tr><td>A5.1.1</td><td>Políticas para la seguridad de la información.</td><td>Control: La dirección debe aprobar un documento de política de seguridad de la información y lo debe publicar y comunicar a todos los empleados y partes externas pertinentes.</td></tr>
<tr><td colspan="2">APLICA</td><td>CUMPLE</td></tr>
<tr><td>SI</td><td>NO</td><td>SI</td><td>NO</td></tr>
<tr><td colspan="2">Descripción: Los controles permiten salvaguardar la información y proteger la confidencialidad e integridad de la misma.</td><td colspan="2">Descripción: No existen políticas definidas para la seguridad de la información, se mantiene un control para salvaguardar la información.</td></tr>
<tr><td>A5.1.2</td><td>Revisión de las políticas para la seguridad de la información.</td><td colspan="2">Control: La política de seguridad de la información se debe revisar a intervalos planificados o cuando se producen cambios significativos, para garantizar que sigue siendo</td></tr>
</table>

		adecuada, suficiente y eficaz.
APLICA		**CUMPLE**	
SI	**NO**	**SI**	**NO**
Descripción: Con la política establecida se permitirá hacer seguimiento y auditorías al proceso de seguridad de la información.		Descripción No existe política establecida para este control.	

Tabla 17. Control Organización de la seguridad de la información

A.6	**ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACION**	
A.6.1	**Organización interna**	
Objetivo: Establecer un marco de referencia de gestión para iniciar y controlar la implementación y la operación de la seguridad de la información dentro de la organización.		
A.6.1.1	**Roles y responsabilidades para la seguridad de la información**.	**Control:** Se debería definir asignar todas las responsabilidades de la seguridad de la información.
APLICA		**CUMPLE**
SI	**NO**	**SI** / **NO**
Descripción: La dirección debe aprobar un documento de política de seguridad de la información y lo debe publicar y comunicar a todos los empleados y partes externas pertinentes.		Descripción: No existe política de seguridad sobre este control.
A.6.1.2	**Separación de deberes**	**Control:** Los deberes y áreas de responsabilidad en conflicto deberían separar para reducir las posibilidades de modificación no autorizada o no intencional, o el uso indebido de los activos de la organización.
APLICA		**CUMPLE**
SI	**NO**	**SI** / **NO**
Descripción: El control permitirá crear las responsabilidades de los funcionarios frente a la seguridad de la información.		Descripción No existe política para este control.
A.6.1.3	**Contacto con las autoridades**	**Control:** Se deberían mantener contactos apropiados con las autoridades pertinentes.

APLICA		CUMPLE	
SI	**NO**	**SI**	**NO**
Descripción: La política permite estipular el proceso a desarrollar al encontrar incidentes contra la seguridad de la información de la entidad.		Descripción: No existe política para este control.	
A.6.1.4	**Contacto con grupos de interés especial.**	**Control:** Es conveniente mantener los contactos apropiados con grupos de interés especiales, otros foros especializados en seguridad de la información, y asociaciones de profesionales.	
APLICA		**CUMPLE**	
SI	**NO**	**SI**	**NO**
Descripción: Permite estipular el contacto que se debe tener con otras entidades en tema de seguridad de la información.		Descripción: Se mantiene comunicación directa con los líderes de gobierno en línea.	
A.6.1.5	**Seguridad de la información en la gestión de proyectos.**	**Control:** La seguridad de la información se debería tratar en la gestión de proyectos, independientemente el tipo de proyecto.	
APLICA		**CUMPLE**	
SI	**NO**	**SI**	**NO**
Descripción: La política permite proteger la información de los proyectos en ejecución.		Descripción: No existe política definida para este control.	
A.6.2 Dispositivos para movilidad y teletrabajo.			
Objetivo: Garantizar la seguridad del teletrabajo y el uso de dispositivos móviles.			
A.6.2.1	**Política de uso de dispositivos móviles.**	**Control:** Se debería adoptar una política y unas medidas de seguridad de soporte, para gestionar los riesgos introducidos por el uso del dispositivo móvil.	
APLICA		**CUMPLE**	
SI	**NO**	**SI**	**NO**
Descripción: Se aplicara lineamientos del debido uso del celular corporativo.		Descripción: No existe política establecida para este control, realizan las recomendaciones básicas del buen uso del equipo de comunicación.	

Tabla 18. Control seguridad de los recursos humanos

A.7	SEGURIDAD DE LOS RECURSOS HUMANOS	
A.7.1	Antes de asumir el empleo	
Objetivo: Asegurar que lo empleados y contratistas comprenden sus responsabilidades y son idóneos en los roles para los que se consideran.		
A.7.1.1	**Selección**	**Control:** Las verificaciones de los antecedentes de todos los candidatos a un empleo se deberían llevar a cabo de acuerdo con las leyes, reglamentos y ética pertinentes, y deberían ser proporcionales a los requisitos de negocio, a la clasificación de la información a que se va a tener acceso, y a los riesgos percibidos.
APLICA		**CUMPLE**
SI / **NO**		**SI** / **NO**
Descripción: Al iniciar el proceso de contratación el personal encargado de esta área, solicita la documentación requerida para iniciar el proceso contractual.		Descripción: La entidad dentro del proceso de selección y contratación solicita documentos de antecedentes disciplinarios, fiscales, judiciales, certificación laboral, documentos soportes de hoja de vida, y demás documentos de acuerdo a lo estipulado por las leyes gubernamentales.
A.7.1.2	**Términos y condiciones del empleo**	**Control:** Los acuerdos contractuales con empleados y contratistas, deberían establecer sus responsabilidades y las de la organización en cuanto a la seguridad de la información.
APLICA		**CUMPLE**
SI / **NO**		**SI** / **NO**
Descripción: Existe un perfil estipulado para cada cargo.		Descripción: En las cláusulas del contrato se estipula la responsabilidad que asume el funcionario o contratista del cuidado y custodia de los elementos de trabajo y confidencialidad de la información.

A.7	SEGURIDAD DE LOS RECURSOS HUMANOS	
A.7.2	Durante la ejecución del empleo	
Objetivo: Asegurarse de que los empleados y contratistas tomen conciencia de sus responsabilidades de seguridad de la información y las cumplan.		
A.7.2.1	**Responsabilidades de la dirección**	**Control:** La dirección debería exigir a todos los empleados y contratistas la aplicación de la seguridad de la información de acuerdo con las políticas y procedimientos establecidos por la organización.
APLICA		**CUMPLE**
SI	**NO**	**SI** / **NO**
Descripción: El control de responsabilidades de la dirección, permite dejar estipulado los compromisos de la dirección frente a la seguridad de la información de la entidad.		Descripción: No existe política establecida para este control, se mantiene el control a través de auditoria por parte de la oficina de control interno.
A.7.2.2	**Toma de conciencia, educación y formación en la seguridad de la información.**	**Control:** Todos los empleados de la organización, y en donde sea pertinente, los contratistas, deberían recibir la educación y la formación en toma de conciencia apropiada, y actualizaciones regulares sobre las políticas y procedimientos pertinentes para su cargo.
APLICA		**CUMPLE**
SI	**NO**	**SI** / **NO**
Descripción: El control de conciencia, educación y formación permite, formar a los funcionarios, contratistas, de forma permanente sobre la importancia de la seguridad de la información.		Descripción: No existe política establecida para este control, no se realiza capacitación sobre seguridad informática.
A.7.2.3	**Proceso disciplinario.**	**Control:** Se debería contar con un proceso disciplinario formal el cual debería ser comunicado, para emprender acciones contra empleados que hayan cometido una violación a la seguridad de la información.
APLICA		**CUMPLE**

SI	NO	SI	NO
Descripción: El control permite crear los lineamientos para desarrollar el proceso disciplinario, al presentarse un delito o falta relacionada con la seguridad de la información.		Descripción: No existe política establecida para este control, pero existe mecanismos de llamado de atención a los funcionarios cuando un evento de esta clase se presente.	
A.7	**SEGURIDAD DE LOS RECURSOS HUMANOS**		
A.7.3	**Terminación o cambio de empleo**		
Objetivo: Proteger los intereses de la organización como parte del proceso de cambio o terminación del contrato.			
A.7.3.1	**Terminación o cambio de responsabilidades de empleo**	**Control:** Las responsabilidades y los deberes de seguridad de la información que permanecen validos después de la terminación o cambio de contrato se deberían definir, comunicar al empleado o contratista y se deberían hacer cumplir.	
APLICA		**CUMPLE**	
SI	**NO**	**SI**	**NO**
Descripción: El control de terminación o cambio de responsabilidades permite estipular el proceso a seguir, cuando el funcionario se retira de la entidad o cambia de responsabilidades en la misma.		Descripción: No existe política establecida para este control. Es deficiente el control frente a este tema.	

Tabla 19. Control Gestión de Activos

A.8	GESTION DE ACTIVOS	
A.8.1	Responsabilidad por los activos	
Objetivo: Identificar los activos organizacionales y definir las responsabilidades de protección apropiadas.		
A.8.1.1	**Inventario de activos**	Control: Se deberían identificar los activos asociados con la información y las instalaciones de procesamiento de información, y se debería elaborar y mantener un inventario de estos activos.
APLICA		**CUMPLE**
SI / **NO**		**SI** / **NO**
Descripción: El control de inventario de activos, permite reforzar el trabajo que ha desarrollado la entidad sobre el inventario de los activos hasta fecha.		Descripción: Existe inventario de activos, falta mayor estipulación.
A.8.1.2	**Propiedad de los activos**	**Control:** Los activos mantenidos en el inventario deberían tener un propietario.
APLICA		**CUMPLE**
SI / **NO**		**SI** / **NO**
Descripción: El control de propiedades de los activos permite estipular claramente, el propietario de la información.		Descripción: Se ha delegado la responsabilidad al funcionario jefe de dependencia.
A.8.1.3	**Uso aceptable de los activos**	**Control:** Se deberían identificar, documentar e implementar reglas para el uso aceptable de información y de activos asociados con información e instalaciones de procesamiento de información.
APLICA		**CUMPLE**
SI / **NO**		**SI** / **NO**
Descripción: El control permite realizar un adecuado control al uso de los activos de la entidad.		Descripción: No existe política establecida para este control.

A.8	GESTION DE ACTIVOS		
A.8.1	Responsabilidad por los activos		
A.8.1.4	Devolución de activos	**Control:** Todos los empleados y usuarios de partes externas deberían devolver todos los activos de la organización que se encuentren a su cargo, al terminar su empleo, contrato o acuerdo.	
APLICA		CUMPLE	
SI	NO	SI	NO
Descripción: El control de devolución de los activos, permite ejercer el debido control a la devolución de los activos de la entidad.		Descripción: No existe política establecida para este control. No se ejerce un mayor control.	
A.8.2	Clasificación de la información		
Objetivo: Asegurar que la información recibe un nivel apropiado de protección, de acuerdo con su importancia para la organización.			
A.8.2.1	Clasificación de la información	**Control:** La información se debería clasificar en función de los requisitos legales, valor, criticidad y susceptibilidad a divulgación o a modificación no autorizada.	
APLICA		CUMPLE	
SI	NO	SI	NO
Descripción: El control de clasificación de la información permitirá realizar el control del proceso de clasificación de la información en la entidad.		Descripción: No existe política establecida para este control.	
A.8.2.2	Etiquetado de la información	**Control:** Se debería desarrollar e implementar un conjunto adecuado de procedimientos para el etiquetado de la información, de acuerdo con el esquema de clasificación de información adoptado por la organización.	
APLICA		CUMPLE	
SI	NO	SI	NO
Descripción: El control de etiquetado de la información, permitirá realizar un mayor control de la información de la entidad.		Descripción: No existe política establecida para este control. Se realiza rotulación.	

A.8	GESTION DE ACTIVOS	
A.8.2	Clasificación de la información	
A.8.2.3	**Manejo de activos**	**Control:** Se deberían desarrollar e implementar procedimientos para el manejo de activos, de acuerdo con el esquema de clasificación de información adoptado por la organización.
APLICA		**CUMPLE**
SI / **NO**		**SI** / **NO**
Descripción: El control permite de manejo de activos permite realizar el adecuado manejo de activos de la entidad.		Descripción: No existe política establecida para este control.

A.8.3	Manejo de los soportes de almacenamiento	
Objetivo: se debería garantizar el adecuado manejo a los soportes de almacenamiento.		
A.8.3.1	**Gestión de medios removibles**	Control: Se deberían implementar procedimientos para la gestión de medios removibles, de acuerdo con el esquema de clasificación adoptado por la organización.
APLICA		**CUMPLE**
SI / **NO**		**SI** / **NO**
Descripción: El control de medios removibles, permitirá llevar un mayor control sobre los medios removibles de la información de la entidad.		Descripción: No existe política establecida para este control.
A.8.3.2	**Disposición de los medios**	**Control:** Se debería disponer en forma segura de los medios cuando ya no se requieran, utilizando procedimientos formales.
APLICA		**CUMPLE**
SI / **NO**		**SI** / **NO**
Descripción: El control de disposición de medios, permitirá realizar el control sobre los medios cuando ya no se requieran.		Descripción: No existe política establecida para este control.
A.8.3.3	**Transferencia de medios físico**	**Control:** Los medios que contienen información se deberían proteger contra acceso no autorizado, uso indebido o corrupción durante el transporte.

APLICA		CUMPLE	
SI	**NO**	**SI**	**NO**
Descripción: El control de transferencia de medios físicos, permite realizar un adecuado control sobre los medios que se deben transportar, para protegerlos de acceso no autorizado.		Descripción: No existe política establecida para este control.	

Tabla 20. Control de accesos

A.9	**CONTROL DE ACCESOS**	
A.9.1	**Requisitos del negocio para control de acceso**	
Objetivo: Limitar el acceso a información y a instalaciones de procesamiento de información.		
A.9.1.1	**Política de control de acceso**	**Control:** Se debería establecer, documentar y revisar una política de control de acceso con base en los requisitos del negocio y de seguridad de la información.
APLICA		**CUMPLE**
SI	**NO**	**SI** / **NO**
Descripción: El control de acceso físico y lógico permite tener un control sobre los riesgos de divulgación de la información o acceso físico a los activos a personal no autorizado.		Descripción: No existe política establecida para este control. Se ejerce un control físico y lógico.
A.9.1.2	**Política sobre el uso de los servicios de red**	**Control:** Solo se debería permitir acceso de los usuarios a la red y a los servicios de red para los que hayan sido autorizados específicamente.
APLICA		**CUMPLE**
SI	**NO**	**SI** / **NO**
Descripción: El control de política sobre el uso de los servicios de red, permitirá controlar el acceso no autorizado a la red.		Descripción: No existe política establecida para este control.
A.9.2	**Gestión de acceso usuarios**	
Objetivo: Asegurar el acceso de los usuarios autorizados y evitar el acceso no autorizado a sistemas y servicios.		
A.9.2.1	**Registro y cancelación del registro de usuarios**	**Control:** Se debería implementar un proceso formal de registro y de cancelación de registro de usuarios, para posibilitar la asignación de los

		derechos de acceso.
APLICA		**CUMPLE**
SI	**NO**	**SI** / **NO**
Descripción: El control de registro y cancelación de usuarios, permitirá realizar un control en el acceso y cambio de usuarios.		Descripción: No existe política establecida para este control.
A.9.3	**Responsabilidades de los usuarios**	
Objetivo: Hacer que los usuarios rindan cuentas por la salvaguarda de su información de autenticación.		
A.9.3.1	**Uso de la información de autenticación secreta**	**Control:** Se debería exigir a los usuarios que cumplan las prácticas de la organización para el uso de información de autenticación secreta.
APLICA		CUMPLE
SI	NO	SI / NO
Descripción: El uso del control del uso de la información permitirá exigir el cumplimiento de las prácticas de la organización para el uso de información de autenticación secreta.		Descripción: No existe política establecida para este control.
A.9.4	**Control de acceso a sistemas y aplicaciones**	
Objetivo: Evitar el acceso no autorizado a sistemas y aplicaciones.		
A.9.4.3	**Sistema de gestión de contraseñas**	**Control:** Los sistemas de gestión de contraseñas deberían ser interactivos y deberían asegurar la calidad de las contraseñas.
APLICA		**CUMPLE**
SI	**NO**	**SI** / **NO**
Descripción: El control de sistema de gestión de contraseñas permitirá controlar el adecuado uso de contraseñas y su calidad.		Descripción: No existe política establecida para este control, pero se maneja el uso de contraseñas.

Tabla 21. Control Criptografía

A.10	CRIPTOGRAFIA	
A.10.1	Controles criptográficos	
Objetivo: Asegurar el uso apropiado y eficaz de la criptografía para proteger la confidencialidad, la autenticidad y/o la integridad de la información.		
A.10.1.1	**Política sobre el uso de controles criptográficos**	**Control:** Se debería desarrollar e implementar una política sobre el uso de controles criptográficos para la protección de la información.
APLICA		**CUMPLE**
SI / **NO**		**SI** / **NO**
Descripción: El control permitirá llevar la revisión de los controles criptográficos que se realicen.		Descripción: No existe política establecida para este control.
A.10.1.2	**Gestión de llaves**	**Control:** Se debería desarrollar e implementar una política sobre el uso, protección y tiempo de vida de las llaves criptográficas durante todo su ciclo de vida.
APLICA		**CUMPLE**
SI / **NO**		**SI** / **NO**
Descripción: El control permite desarrollar la política sobre el uso y protección y tiempo de vida de las llaves criptográficas.		Descripción: No existe política establecida para este control.se realiza restricciones sobre su aplicación.

Tabla 22. Control seguridad física y del entorno

A.11	SEGURIDAD FÍSICA Y DEL ENTORNO	
A.11.1	Áreas seguras	
Objetivo: Prevenir el acceso físico no autorizado, el daño y la interferencia a la información y a las instalaciones de procesamiento de información de la organización.		
A.11.1.1	**Perímetro de seguridad física**	**Control:** Se deberían definir y usar perímetros de seguridad, y usarlos para proteger áreas que contengan información sensible o critica, e instalaciones de manejo de información.
APLICA		**CUMPLE**
SI / **NO**		**SI** / **NO**
Descripción: El control permite desarrollar una política que defina los perímetros de		Descripción: No existe política establecida para este control, sin

seguridad para las áreas que se maneje información sensible o critica.		embargo la entidad realiza asignaciones del cuidado y protección de la información.
A.11.1.2	**Controles físicos de entrada**	**Control:** Las áreas seguras se deberían proteger mediante controles de entrada apropiados para asegurar que solamente se permite el acceso a personal autorizado.
APLICA		**CUMPLE**
SI	**NO**	**SI** / **NO**
Descripción: El control permite el desarrollo de la política que permita generar las herramientas sólidas para asegurar el ingreso solo al personal autorizado, con el fin de proteger las áreas seguras.		Descripción: No existe política establecida para este control, para proteger estas áreas se realizan procesos básicos de protección.
A.11.1.3	**Seguridad de oficinas, recintos e instalaciones**	**Control:** Se debería diseñar y aplicar seguridad física a oficinas, recintos e instalaciones.
APLICA		**CUMPLE**
SI	**NO**	**SI** / **NO**
Descripción: El control permite general las estrategias para asegurar las áreas físicas, recintos e instalaciones de la entidad.		Descripción: No existe política establecida para este control.se manejan las normas básicas de seguridad.
A.11.1.4	**Protección contra amenazas externas y ambientales**	**Control:** Se debería diseñar y aplicar protección física contra desastres naturales, ataques maliciosos o accidentes.
APLICA		**CUMPLE**
SI	**NO**	**SI** / **NO**
Descripción: El control permite definir una política para diseñar la protección física contra desastres naturales, ataques maliciosos o accidentes a la entidad.		Descripción: No existe política establecida para este control, se maneja la protección básica, la entidad presenta grandes riesgos en las instalaciones a desastres naturales o accidentes.
A.11.1.5	**Trabajo en áreas seguras**	**Control:** Se deberían diseñar y aplicar procedimientos para trabajo en áreas seguras.
APLICA		**CUMPLE**
SI	**NO X**	**SI** / **NO**
Descripción: El control permite diseñar la política y aplicar procedimientos para trabajo		Descripción: No existe política establecida para este control, se

en áreas seguras.		realiza los controles normativos básicos.
A.11.2	**Equipos**	
Objetivo: Prevenir la perdida, daño, robo o compromiso de activos, y la interrupción de las operaciones de la organización.		
A.11.2.1	**Ubicación y protección de los equipos**	**Control:** Los equipos deberían estar ubicados y protegidos para reducir los riesgos de amenazas y peligros del entorno, y las oportunidades para acceso no autorizado.
APLICA		**CUMPLE**
SI	**NO**	**SI** / **NO**
Descripción: El control permite el diseño de políticas de ubicación y protección de los equipos para reducir amenazas y accesos no autorizados.		Descripción: No existe política establecida para este control, se trabaja bajo las normas básicas de protección.
A.11.2.2	**Servicios de suministro**	**Control:** Los equipos se deberían proteger contra fallas de energía y otras interrupciones causadas por fallas en los servicios de suministro.
APLICA		**CUMPLE**
SI	**NO**	**SI** / **NO**
Descripción: El control permite desarrollar la política que permita proteger a los equipos contra fallas de energía y demás interrupciones causadas por ausencia en los servicios de suministro.		Descripción: No existe política establecida para este control. Se aplica la norma básica del buen cuidado.
A.11.2.3	**Seguridad del cableado**	**Control:** El cableado de potencia y de telecomunicaciones que porta datos o soporta servicios de información debería estar protegido contra interceptación, interferencia o daño.
APLICA		**CUMPLE**
SI	**NO X**	**SI** / **NO**
Descripción: El control permite desarrollar políticas que permitan proteger el cableado de interceptaciones, interferencias o daños.		Descripción: No existe política establecida para este control, se realizan mantenimientos preventivos.
A.11.2.4	**Mantenimiento de equipos**	Control: Los equipos se deberían mantener correctamente para

		asegurar su disponibilidad e integridad continuas.
APLICA		**CUMPLE**
SI	**NO X**	**SI** / **NO**
Descripción: El control permite desarrollar una política que permita realizar el mantenimiento de los equipos de forma preventiva y asegurar su disponibilidad e integridad.		Descripción: No existe política establecida para este control, se realiza mantenimiento a los equipos de forma eventual o cuando surge alguna afectación.
A.11.2.5	**Retiro de activos**	**Control:** Los equipos, información o software no se deberían retirar de su sitio sin autorización previa.
APLICA		**CUMPLE**
SI	**NO**	**SI** / **NO**
Descripción: El control permite realizar la política que defina el proceso para el retiro de activos de la entidad.		Descripción: No existe política establecida para este control, se realiza un seguimiento básico al retiro de activos.
A.11.2.6	**Seguridad de equipos y activos fuera de las instalaciones**	**Control:** Se deberían aplicar medidas de seguridad a los activos que se encuentran fuera de las instalaciones de la organización, teniendo en cuenta los diferentes riesgos de trabajar fuera de dichas instalaciones.
APLICA		**CUMPLE**
SI	**NO**	**SI** / **NO**
Descripción: El control permite desarrollar la política para aplicar medidas de seguridad a los activos que se encuentren fuera de las instalaciones de la entidad.		Descripción: No existe política establecida para este control.
A.11.2.7	**Disposición segura o reutilización de equipos**	**Control:** Se deberían verificar todos los elementos de equipos que contengan medios de almacenamiento, para asegurar que cualquier dato sensible o software con licencia haya sido retirado o sobrescrito en forma segura antes de su disposición o reutilización.
APLICA		**CUMPLE**
SI	**NO**	**SI** / **NO**
Descripción: El control permite desarrollar la política para realizar la adecuada revisión de		Descripción: No existe política establecida para este control, sin

equipos que contengan medios de almacenamiento para asegurar que cualquier dato sensible o software con licencia haya sido retirado o sobrescrito en forma segura antes de su disposición o reutilización.		embargo se realiza verificación de la información del equipo.
A.11.2.8	**Equipos de usuario desatendidos**	**Control:** Los usuarios deberían asegurarse de que a los equipos desatendidos se les dé protección apropiada.
APLICA		**CUMPLE**
SI	**NO**	**SI** / **NO**
Descripción: El control permite el desarrollo de la política de protección para los equipos desatendidos.		Descripción: No existe política establecida para este control, sin embargo quedan bajo la protección del jefe de dependencia.
A.11.2.9	**Política de escritorio limpio y pantalla limpia**	**Control:** Se debería adoptar una política de escritorio limpio para los papeles y medios de almacenamiento removibles, y una política de pantalla limpia en las instalaciones de procesamiento de información.
APLICA		**CUMPLE**
SI	**NO**	**SI** / **NO**
Descripción: El control permite desarrollar la política de escritorio limpio y pantalla limpia para asegurar la organización y protección de la información.		Descripción: No existe política establecida para este control. Realizan recomendaciones de la organización en las oficinas.

Tabla 23. Control seguridad de las operaciones

A.12	**SEGURIDAD DE LAS OPERACIONES**	
A.12.1	**Procedimientos operacionales y responsabilidades**	
Objetivo: Asegurar las operaciones correctas y seguras de las instalaciones de procesamiento de información.		
A.12.1.1	**Procedimientos de operación documentados**	**Control:** Los procedimientos de operación se deberían documentar y poner a disposición de todos los usuarios que los necesiten.
APLICA		**CUMPLE**
SI	**NO**	**SI** / **NO**
Descripción: El control permite realizar la política para documentar el procedimiento y		Descripción: No existe política establecida para este control. Se

ponerlos a disposición de los usuarios que lo necesiten.		realiza documentación sobre algunos procesos.
A.12.1.2	**Gestión de cambios**	**Control:** Se deberían controlar los cambios en la organización, en los procesos de negocio, en las instalaciones y en los sistemas de procesamiento de información que afectan la seguridad de la información.
APLICA		**CUMPLE**
SI	**NO**	**SI** / **NO**
Descripción: El control permite desarrollar una política para generar lineamientos en los cambios que se realicen en las instalaciones y los sistemas de información que afecten la seguridad de la información de la entidad.		Descripción: No existe política establecida para este control. Sin embargo se maneja seguimiento básico a los cambios que se realizan en la entidad.
A.12.1.3	**Gestión de capacidad**	**Control:** Para asegurar el desempeño requerido del sistema se debería hacer seguimiento al uso de los recursos, hacer los ajustes, y hacer proyecciones de los requisitos sobre la capacidad futura.
APLICA		**CUMPLE**
SI	**NO**	**SI** / **NO**
Descripción: El control permite generar la política del buen uso de los recursos, para garantizar el buen desempeño de los sistemas.		Descripción: No existe política establecida para este control. Se realizan indicaciones verbales del buen uso de los recursos.
A.12.2	**Protección contra códigos maliciosos**	
Objetivo: Asegurarse de que la información y las instalaciones de procesamiento de información estén protegidas contra códigos maliciosos.		
A.12.2.1	**Controles contra códigos maliciosos**	**Control:** Se deberían implementar controles de detección, de prevención y de recuperación, combinados con la toma de conciencia apropiada de los usuarios, para proteger contra códigos maliciosos.
APLICA		**CUMPLE**
SI	**NO**	**SI** / **NO**
Descripción: El control permite desarrollar la		Descripción: No existe política

política para implementar la directriz para la prevención de códigos maliciosos y toma de conciencia por parte de los usuarios de la protección de la información.		establecida para este control. Realizan controles de instalación de antivirus, pero no realizan el seguimiento.
A.12.3	**Copias de respaldo**	
Objetivo: Proteger contra la perdida de datos.		
A.12.3.1	**Respaldo de información**	**Control:** Se deberían hacer copias de respaldo de la información, del software e imágenes de los sistemas, y ponerlas a prueba regularmente de acuerdo con una política de copias de respaldo aceptada.
APLICA		**CUMPLE**
SI	**NO**	**SI** / **NO**
Descripción: El control permite crear la política de respaldo de copias de seguridad de la información del software e imágenes de los sistemas.		Descripción: No existe política establecida para este control. Sin embargo realizan copias esporádicamente.
A.12.4	**Registro y seguimiento**	
Objetivo: Registrar eventos y generar evidencia.		
A.12.4.1	**Registro de eventos**	**Control:** Se deberían elaborar, conservar y revisar regularmente los registros acerca de actividades del usuario, excepciones, fallas y eventos de seguridad de la información.
APLICA		**CUMPLE**
SI	**NO**	**SI** / **NO**
Descripción: El control permite crear la política para crear directrices que permitan elaborar, conservar y revisar regularmente los registros de actividades de usuario, excepciones, fallas eventos de seguridad de la información.		Descripción: No existe política establecida para este control. En su totalidad de los sistemas de información se llevan registros de las actividades de los usuarios.
A.12.4.2	**Protección de la información de registro**	**Control:** Las instalaciones y la información de registro se deberían proteger contra alteración y acceso

		no autorizado.
APLICA		**CUMPLE**
SI	**NO**	**SI**	**NO**
Descripción: El control permite elaborar la política para proteger las instalaciones y la información de registros.		Descripción: No existe política establecida para este control.	

A.12.5	**Control de software operacional**	
Objetivo: Asegurar la integridad de los sistemas operacionales		
A.12.5.1	**Instalación de software en sistemas operativos**	**Control:** Se deberían implementar procedimientos para controlar la instalación de software en sistemas operativos.
APLICA		**CUMPLE**
SI	**NO**	**SI**	**NO**
Descripción: El control permite crear la política para estipular los procedimientos a realizar en la instalación de software en sistemas operativos.		Descripción: No existe política establecida para este control. Sin embargo se realizan las recomendaciones generales de control de software.	
A.12.6	**Gestión de la vulnerabilidad técnica**	
Objetivo: Prevenir el aprovechamiento de las vulnerabilidades técnicas.		
A.12.6.1	**Gestión de las vulnerabilidades técnicas**	**Control:** Se debería obtener oportunamente información acerca de las vulnerabilidades técnicas de los sistemas de información que se usen; evaluar la exposición de la organización a estas vulnerabilidades, y tomar las medidas apropiadas para tratar el riesgo asociado.
APLICA		**CUMPLE**
SI	**NO**	**SI**	**NO**
Descripción: El control permite crear la política para conocer oportunamente acerca de las vulnerabilidades técnicas de los sistemas y tomar medidas preventivas.		Descripción: No existe política establecida para este control.	
A.12.6.2	**Restricciones sobre la instalación de**	**Control:** Se deberían establecer e implementar las reglas para la instalación de software por parte

	software	de los usuarios.
APLICA		**CUMPLE**
SI	**NO**	**SI** / **NO**
Descripción: El control permite establecer reglas para la instalación de software por parte de los usuarios.		Descripción: No existe política establecida para este control. Sin embargo se realizan las recomendaciones generales de control de software.
A.12.7	**Consideraciones sobre auditorias de sistemas de información**	
Objetivo: Prevenir el aprovechamiento de las vulnerabilidades técnicas.		
A.12.7.1	**Información controles de auditoría de sistemas**	**Control:** Los requisitos y actividades de auditoría que involucran la verificación de los sistemas operativos se deberían planificar y acordar cuidadosamente para minimizar las interrupciones en los procesos del negocio.
APLICA		**CUMPLE**
SI	**NO**	**SI** / **NO**
Descripción: El control permite crear la política para realizar adecuadamente las auditorias de los sistemas operativos, sin realizar interrupción en los procesos operativos.		Descripción: No existe política estipulada para este control, las auditorias no se realizan.

Tabla 24. Control seguridad de las comunicaciones

A.13	**SEGURIDAD DE LAS COMUNICACIONES**	
A.13.1	**Gestión de la seguridad de las redes**	
Objetivo: Asegurar la protección de la información en las redes, y sus instalaciones de procesamiento de información de soporte.		
A.13.1.1	**Controles de redes**	**Control:** Las redes se deberían gestionar y controlar para proteger la información en sistemas y aplicaciones.
APLICA		**CUMPLE**
SI	**NO**	**SI** / **NO**
Descripción: El control permite crear la política para generar lineamientos de protección de la información en la red.		Descripción: No existe política establecida para este control. Se realiza los controles de protección básicos en la red.

A.13.1.2	**Seguridad de los servicios de red**	**Control:** Se deberían identificar los mecanismos de seguridad, los niveles de servicio y los requisitos de gestión de todos los servicios de red, e incluirlos en los acuerdos de servicios de red, ya sea que los servicios se presten internamente o se contraten externamente.
APLICA		**CUMPLE**
SI	**NO**	**SI** / **NO**
Descripción: El control permite crear la política para garantizar los mecanismos de seguridad de los servicios de red.		Descripción: No existe política establecida para este control.
A.13.1.3	**Separación en las redes**	**Control:** Los grupos de servicios de información, usuarios y sistemas de información se deberían separar en las redes.
APLICA		**CUMPLE**
SI	**NO**	**SI** / **NO**
Descripción: El control permite realizar la política para generar los lineamientos de separación en las redes de los servicios de información, usuarios y sistemas de información.		Descripción: No existe política establecida para este control.
A.13.2	**Transferencia de información**	
Objetivo: Mantener la seguridad de la información transferida dentro de una organización y con cualquier entidad externa.		
A.13.2.1	**Políticas y procedimientos de transferencia de información**	**Control:** Se debería contar con políticas, procedimientos y controles de transferencia formales para proteger la transferencia de información mediante el uso de todo tipo de instalaciones de comunicación.
APLICA		**CUMPLE**
SI	**NO**	**SI** / **NO**
Descripción: El control permite generar la política de transferencia de información garantizando la protección y seguridad de la misma.		Descripción: No existe política establecida para este control. Se realiza el proceso de transferencia con los cuidados básicos de protección.
A.13.2.2	**Acuerdos sobre**	**Control:** Los acuerdos deberían

	transferencia de información	tener en cuenta la transferencia segura de información del negocio entre la organización y las partes externas.
APLICA		**CUMPLE**
SI	**NO**	**SI** / **NO**
Descripción: El control permite crear la política de transferencia de información entre la entidad y partes externas.		Descripción: No existe política establecida para este control.
A.13.2.3	**Mensajería electrónica**	**Control:** Se debería proteger adecuadamente la información incluida en la mensajería electrónica.
APLICA		**CUMPLE**
SI	**NO**	**SI** / **NO**
Descripción: El control permite diseñar la política del buen uso y la protección de la información en la mensajería electrónica.		Descripción: No existe política establecida para este control. Se realiza las pautas de cuidado y protección de forma verbal.
A.13.2.4	**Acuerdos de confidencialidad o de no divulgación**	**Control:** Se deberían identificar, revisar regularmente y documentar los requisitos para los acuerdos de confidencialidad o no divulgación que reflejen las necesidades de la organización para la protección de la información.
APLICA		**CUMPLE**
SI	**NO**	**SI** / **NO**
Descripción: El control permite crear la política del diseño, uso del acuerdo de confidencialidad, para la protección de la información.		Descripción: No existe política establecida para este control. Se está implementado una clausula en los contratos de prestación de servicios, donde se estipula la confidencialidad de los datos suministrados para el desarrollo de las funciones.

Tabla 25. Control adquisición, desarrollo y mantenimiento de sistemas

<table>
<tr><td>A.14</td><td colspan="3">ADQUISICIÓN, DESARROLLO Y MANTENIMIENTOS DE SISTEMAS</td></tr>
<tr><td>A.14.1</td><td colspan="3">Requisitos de seguridad de los sistemas de información</td></tr>
<tr><td colspan="4">Objetivo: Asegurar que la seguridad de la información sea una parte integral de los sistemas de información durante todo el ciclo de vida. Esto incluye también los requisitos para sistemas de información que prestan servicios en redes públicas.</td></tr>
<tr><td>A.14.1.1</td><td>Análisis y especificación de requisitos de seguridad de la información</td><td colspan="2">Control: Los requisitos relacionados con seguridad de la información se deberían incluir en los requisitos para nuevos sistemas de información o para mejoras a los sistemas de información existentes.</td></tr>
<tr><td colspan="2">APLICA</td><td colspan="2">CUMPLE</td></tr>
<tr><td>SI</td><td>NO</td><td>SI</td><td>NO</td></tr>
<tr><td colspan="2">Descripción: El control permite crear la política para estipular las especificaciones y requisitos de la seguridad de la información, en los sistemas de información existentes o nuevos sistemas.</td><td colspan="2">Descripción: No existe política establecida para este control.</td></tr>
<tr><td>A.14.1.3</td><td>Protección de transacciones de los servicios de las aplicaciones</td><td colspan="2">Control: La información involucrada en las transacciones de los servicios de las aplicaciones se debería proteger para evitar la transmisión incompleta, el enrutamiento errado, la alteración no autorizada de mensajes, la divulgación no autorizada, y la duplicación o reproducción de mensajes no autorizada</td></tr>
<tr><td colspan="2">APLICA</td><td colspan="2">CUMPLE</td></tr>
<tr><td>SI</td><td>NO</td><td>SI</td><td>NO</td></tr>
<tr><td colspan="2">Descripción: El control permite crear la política para proteger la información involucrada en las transacciones de los servicios de aplicaciones y evitar transmisión incompleta.</td><td colspan="2">Descripción: No existe política establecida para este control.</td></tr>
</table>

Tabla 26. Gestión de incidentes de seguridad de la información

<table>
<tr><td>A.16</td><td colspan="3">GESTION DE INCIDENTES DE SEGURIDAD DE LA INFORMACION</td></tr>
<tr><td>A.16.1</td><td colspan="3">Gestión de incidentes y mejoras en la seguridad de la información</td></tr>
<tr><td colspan="4">Objetivo: Asegurar un enfoque coherente y eficaz para la gestión de incidentes de seguridad de la información, incluida la comunicación sobre eventos de seguridad y debilidades.</td></tr>
<tr><td>A.16.1.1</td><td>Gestión de incidentes y mejoras en la seguridad de la información.</td><td colspan="2">Control: Se deberían establecer las responsabilidades y procedimientos de gestión para asegurar, una respuesta rápida, eficaz y ordenada a los incidentes de seguridad de la información.</td></tr>
<tr><td colspan="2">APLICA</td><td colspan="2">CUMPLE</td></tr>
<tr><td>SI</td><td>NO</td><td>SI</td><td>NO</td></tr>
<tr><td colspan="2">Descripción: El control permite crear la política para establecer las responsabilidades y procedimientos de gestión para asegurar, una respuesta rápida, eficaz y ordenada a los incidentes de seguridad de la información.</td><td colspan="2">Descripción: No existe política establecida para este control.</td></tr>
</table>

Fuente: Propiedad del autor

7.PROPONER LAS POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN BASADAS EN LA NORMA ISO 27001:2013

Se propone crear las políticas y controles de seguridad informática en la alcaldía municipal de Guachetá, con el fin de salvaguardar los activos de información de la entidad.

La seguridad informática es el proceso donde se permite evaluar y administrar los riesgos apoyados en políticas y estándares que cubran las necesidades de la alcaldía municipal.

Dentro de los criterios a tener en cuenta son los siguientes:

Seguridad institucional
Seguridad física
Administración de centros de cómputo

7.1 POLÍTICAS DE SEGURIDAD DE LA INFORMACION

7.1.1 Políticas generales de la seguridad informática

Siendo la información un componente indispensable para el cumplimiento de los objetivos de la entidad, se hace necesario la creación de las políticas de seguridad de la información, para que esta sea protegida de forma independiente en el momento de ser manejada, almacenada, procesada, y/o transportada.

La política de seguridad de la información surge como herramienta institucional, para concientizar a cada uno de los directivos, funcionarios, contratistas y terceros que presten sus servicios o tengan algún tipo de relación con la empresa, sobre la importancia y sensibilización de la información y servicios críticos, de tal forma que permita desarrollar adecuadamente sus labores y cumplir con su propósito misional.

Objetivo

Definir las pautas de propósito general, concisa, y fácil de leer e interpretar, para asegurar una adecuada protección de la información de la empresa.

Aplicabilidad

Las políticas son aplicables a Gerencia, subgerencia, jefes de dependencias, funcionarios, contratistas, y en general a todos los usuarios de la información que cumplan con los propósitos generales de organización.

Directrices

- Mantener el inventario actualizado de sus activos de información bajo la responsabilidad de cada propietario de información y centralizado por el área de archivo y sistemas.

- Los directivos, funcionarios, contratistas y terceros que presten sus servicios o tengan algún tipo de relación con la empresa son responsables de la información que manejan para protegerla, evitando robos, suplantaciones, accesos no autorizados, utilización impropia de la misma.

- La administración municipal debe garantizar la protección de la información de la entidad.
- Verificar que se definan, implementen, revisen y actualicen las políticas de seguridad de la información.

7.2 POLITICAS PARA LA ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACION

7.2.1 Políticas generales para la organización interna

La política para la organización de la seguridad interna, surge con el fin de estipular parámetros de protección de la información, para que funcionarios, servidores y contratistas quienes tienen relación directa con la información general de la entidad, conozcan el valor de la información para su empresa y desarrollen las actividades de forma responsable e idónea.

Objetivo

Crear pautas de gestión para controlar e implementar la seguridad de la información dentro de la entidad.

Aplicabilidad

Las políticas son aplicables a Gerencia, subgerencia, jefes de dependencias, funcionarios, contratistas, que tienen relación directa con la entidad.

Directrices

- El área de comunicaciones y de sistemas en conjunto deben implementar estrategias, programas de socialización y divulgación, para sensibilizar a los

usuarios, que la seguridad informática es un tema de todos y no solo del área de sistemas.

- La información interna de la entidad no debe ser alterada, transferida, intercambiada, transferida con terceros bajo ningún propósito.

- Se implementara la clasificación de la información de acuerdo a los parámetros establecidos como primaria, (fuentes externas), secundaria (producida por la entidad), confidencial, privada, reserva, publica.

- La información de la entidad física o en medio virtual, debe ser codificada, archivada y salvaguardada, de acuerdo a los parámetros establecidos por la oficina de archivo.

- La información debe ser protegida, salvaguardada y utilizada únicamente para los fines administrativos de la alcaldía municipal de Guachetá.

- El uso de dispositivos móviles entregados por la entidad debe ser exclusivamente para el cumplimiento de las funciones estipuladas para cada funcionario, su uso no debe ser personal.

- Los funcionarios, servidores y contratistas deben cumplir con las políticas y estándares de seguridad informática establecidos por la entidad.

7.3 POLITICAS PARA LA SEGURIDAD DE LOS RECURSOS HUMANOS

7.3.1 Políticas generales para la seguridad de los recursos humanos

Las políticas para la seguridad de los recursos humanos es la herramienta que permite generar pautas para asegurar la capacidad de preservar la integridad, disponibilidad, confidencialidad y accesibilidad de la información por parte de uno de los elementos importantes de la seguridad de la informática, como es el recurso humano. Es fundamental educar al personal desde su ingreso y permanencia, sin importar la vinculación laboral las medidas de protección de la información para minimizar el riesgo.

Objetivo

Asegurar que los empleados y contratistas comprendan la importancia de la seguridad de la información, sus responsabilidades con la entidad y el compromiso que adquieren al ingresar a la misma.

Aplicabilidad

Las políticas son aplicables a Gerencia, subgerencia, jefes de dependencias, funcionarios, contratistas, que tienen relación directa con la entidad

Directrices

- Realizar controles previos de verificación del personal que se incorporara a la entidad.

- Al ingresar un empleado a la alcaldía de Guachetá Cundinamarca a manejar equipos de cómputo, procesar información, y hacer uso de equipos informáticos, debe aceptar las condiciones de confidencialidad, buen uso y manejo de los equipos, cumplir con las políticas y estándares fijados para la seguridad informática de la entidad.

- Al ingresar los usuarios nuevos se deben reportar con el ingeniero de sistemas para que este, sea quien realice inducción y configure los permisos de cada usuario.

- Se realizaran periódicamente capacitación a todos los servidores públicos de la alcaldía municipal de Guachetá, sobre las políticas y estándares de seguridad informática, prevención de amenazas vulnerabilidades, manual de usuarios, donde se debe dar a conocer las obligaciones y responsabilidades de cada funcionario y sanciones que pueden llegar a incurrir.

- De acuerdo a la legislación colombiana se aplicaran las sanciones que sean necesarias, en el momento que se presente robo, alteración de información, divulgación de información confidencial, o declaración de cualquier delito informático.

- El personal de la alcaldía municipal de Guachetá será responsable del reporte de incidentes y debilidades de seguridad que se detecten.

- El responsable de la contratación debe informar al funcionario o contratista y dejar por escrito, la responsabilidad y los deberes de seguridad de la información que permanecen validos después de la terminación o cambio de contrato y hacerlos cumplir.

7.4 POLITICAS PARA LA GESTION DE ACTIVOS

7.4.1 Políticas generales para la gestión de activos

Las políticas generales para la gestión de activos surgen con el fin de crear patrones para la protección de los activos de la entidad, concientizando a funcionarios, servidores públicos, contratistas de la importancia, cuidado y protección de todos los activos de la entidad.

Objetivo

Asegurar que los activos de la entidad reciban un nivel apropiado de protección, de acuerdo con su importancia para la entidad.

Aplicabilidad

Las políticas son aplicables a Gerencia, subgerencia, jefes de dependencias, funcionarios, contratistas, y en general a todos los usuarios de la información que cumplan con los propósitos generales de organización.

Directrices

- Mantener el inventario actualizado de sus activos de información bajo la responsabilidad de cada propietario de información y centralizado por el área de archivo y sistemas.

- Identificar, documentar e implementar reglas para el uso aceptable de información y de activos asociados con información e instalaciones de procesamiento de información.

- Los funcionarios públicos deben conservar los registros de información activa y aquellos que se han declarado confidenciales.

- Toda la información que sea manejada por los funcionarios públicos estará sujeta a auditoria.

- Se debe tener claro el uso de USB designadas para el trabajo y el uso de USB personales, informar al área de sistemas, ser responsables de un buen manejo de los discos extraíbles y evitar fugas y pérdida de información.

- Todos los empleados y usuarios deben devolver todos los activos de la organización que se encuentren a su cargo, al terminar empleo, contrato o acuerdo.

- Crear los procedimientos para la administración de medios informáticos, de almacenamiento, como discos externos, USBs, celulares, información impresa y la eliminación segura de la misma.

- Se implementara el plan de manejo de activos, de acuerdo al esquema de clasificación adoptada por la entidad.

- Realizar adecuada disposición de los activos de almacenamiento, cuando ya no se requieran, utilizando los procedimientos formales.

- Es responsabilidad de los funcionarios, contratistas, servidores públicos, proteger contra acceso no autorizado, uso indebido o corrupción durante el transporte los medios físicos de transferencia física de información.

- Todo funcionario, contratista, servidor público tiene responsabilidad de velar por la integridad, confidencialidad, disponibilidad, confiabilidad, accesibilidad de la información que maneje.

7.5 POLITICA PARA EL CONTROL DE ACCESO

7.5.1 Políticas generales de control de acceso

Las políticas para el control de acceso, son el medio para crear un sistema de restricciones y protección de la información, evitando el acceso no autorizado a los sistemas de información, a través de la política se implementa procedimientos formales para controlar el acceso a los sistemas de información, servicios de información, bases de datos, los funcionarios, servidores públicos, contratistas y demás personal con vinculación permanente a la entidad, deben ser responsables del control de acceso eficaces, especialmente quienes dentro del desarrollo de sus funciones tienen a su cargo el manejo de contraseñas y protección de la seguridad de los recursos informáticos.

Objetivo

Limitar el acceso no autorizado a los sistemas de información y a instalaciones de procesamiento de la información.

Aplicabilidad

Las políticas son aplicables administrador de sistemas, Administrador de servidores.

Directrices

- La oficina de sistemas creara políticas y procedimiento para regular el acceso a las áreas restringidas por parte de funcionarios no autorizados.

- Solo el personal autorizado tendrá acceso a los equipos de cómputo, para que alguien pueda utilizarlo, todo se hará a través de previa autorización de la oficina de sistemas.

- La oficina de sistemas será la encargada de implementar un proceso formal de registros y cancelación de registros de usuarios, para posibilitar la creación los derechos de acceso, asignarlos o revocarlos según sea el caso.

- Los funcionarios, servidores públicos, contratistas, deben proteger la información que se utiliza en la alcaldía municipal de Guachetá, su confidencialidad e integridad, que debe ser archivada por motivos institucionales ya sea dentro del área interna o externa de la entidad o internet.

- Los funcionarios, servidores públicos, contratistas, deben conocer la importancia de la protección de los equipos con software de protección como antivirus, firewall.
- En el momento de realizar mantenimiento de un equipo de área restringida, avisar con tiempo a los servidores públicos que dependan de estos equipos para evitar pérdidas de información y alteración en su trabajo.

- Los funcionarios, contratistas cuando terminen las sesiones activas, se deben asegurar con mecanismos de bloqueo.

- Definir los perfiles de acceso de cada usuario.

- Utilizar contraseñas con un alto grado de complejidad, no utilizar palabras comunes, información personal, no publicarlas en papeles pegadas a los equipos de oficina, deben conservarse de forma segura.

- El área de sistemas es la encargada de la instalación de software o hardware en los equipos.

7.6 POLITICA CRIPTOGRAFIA

7.6.1 Políticas generales de criptografía

Las políticas de criptografía son herramientas que permite definir las técnicas, para asegurar el uso apropiado de la criptografía, protegiendo la confidencialidad, integridad y/o autenticidad de la información.

Objetivo

Asegurar el uso apropiado de la criptografía para proteger la confidencialidad, autenticidad, y/o integridad de la información.

Aplicabilidad

Las políticas son aplicables jefe de sistemas.

Directrices

- Implementar un sistema de administración de claves criptográficas, para preservar la utilización por parte de la alcaldía municipal de Guachetá.

- Cambiar o actualizar las claves cuando se requieran, estipulando las reglas del porque se realiza el cambio y como debe cambiarse las claves.

- La firma digital del alcalde no debe ser utilizada para fines ajenos a los que corresponda al desarrollo de actividades de la entidad.

- Generar de forma segura certificados de clave pública.

7.7 POLITICA PARA LA SEGURIDAD FISICA Y DEL ENTORNO

7.7.1 Políticas generales de la seguridad física y Del entorno

Las políticas de seguridad física y del entorno, son las pautas que permite evitar e impedir el acceso no autorizado, daños e interferencias a las estaciones de información, cuidado de equipos de la alcaldía municipal de Guachetá.

Objetivo

Prevenir el acceso físico no autorizado, el daño de interferencia a la información y a las instalaciones de procesamiento de la información, evitando el daño, robo,

compromisos de activos que comprometan el desarrollo de las actividades de la entidad.

Aplicabilidad

Las políticas son aplicables a todos los recursos físicos de los sistemas de información de la entidad: estructura de cableado, archivos, medios de almacenamiento, instalaciones, etc.

Directrices

- El acceso a la información clasificada y a las zonas de procesamiento de información es solo para el personal autorizado.

- Realizar supervisión de la entrada de visitantes a la alcaldía municipal de Guachetá, llevando registro de fecha, hora de ingreso y egreso, se permitirá el acceso donde exista justificación y propósitos específicos, se explicara los requerimientos de seguridad del área.

- Los funcionarios, contratistas deben portar el carnet que los identifica como funcionarios de la entidad, de lo contrario, no pueden tener acceso a las áreas protegidas.

- El área de sistemas diseñara el manual de derechos para el ingreso a las áreas protegidas, que deberá ser socializado con los funcionarios, firmado el acuerdo, actualizando el proceso cada 6 meses.

- Realizar seguimiento de parte de la oficina de control interno a las visitas realizadas a las áreas protegidas.

- Las oficinas donde se realicen las actividades de proceso de información deben estar protegidas con un sistema de seguridad especial, contar con la señalización requerida.

- Las oficinas deben estar cerradas y aseguradas cuando se encuentren solas.

- Ubicar los equipos de cómputo, impresoras, escáneres, adecuadamente dentro del área protegida, evitando acceso no autorizados, ataques maliciosos o accidentes que pueden afectar la información.

- Es responsabilidad de los funcionarios, servidores públicos, contratistas evitar fuga de la información de la entidad almacenada en los equipos de cómputo asignados.

- Los funcionarios, servidores públicos, contratistas no deben instalar, reubicar equipos, sin la autorización de la oficina de sistemas.

- El área de almacén y sistemas será la encargada de realizar seguimiento a los equipos asignados, retiro de equipos y verificar el estado del mismo.

- El equipo asignado deberá ser de uso exclusivo solo para las actividades contratadas.

- Desarrollar capacitaciones para sensibilizar a los funcionarios, servidores públicos, contratistas, sobre la seguridad de la información, protección de los datos, controles de acceso al sistema, y administración de cambios.

- Es responsabilidad de cada los funcionarios, servidores públicos, contratistas almacenar la información en el equipo de cómputo de forma segura.

- No ingerir alimentos, bebidas mientras se utiliza el equipo de cómputo.

- Evitar exponer el equipo a humedad, mantenerlo limpio.

- No se permite el destapar los equipos, nadie diferente a la oficina de sistemas.

- El equipo asignado deberá ser de uso exclusivo solo para las actividades contratadas.

- El mantenimiento de los equipos estará a cargo del personal autorizado de la oficina de sistemas, se realizara el mantenimiento preventivo asegurando su disponibilidad e integridad

- Es responsable el servidor público de la custodia del equipo de cómputo asignado, de lo contrario responderá de acuerdo a la normatividad vigente, sobre robo, daño, se abrirán las sanciones disciplinarias que vengan al caso.

- El préstamo de los equipos, daño de los mismos se deben reportar a la oficina de sistemas

- Contar con suministro de energía interrumpido (UPS), un apagado adecuado de los equipos, evitar perdida de información.

- Proteger el cableado contra interceptación, daño o interrupción, mediante controles como: evitando trayectos de áreas visibles o áreas públicas, utilizar conductos.

- Mantener escritorios limpios, medios de almacenamiento removible asegurados y pantalla limpia en los equipos.

- Retirar y guardar la información confidencial inmediatamente impresa.

- Desconectar de la red sistemas, servicios de computadores personales, terminales e impresoras cuando no están en uso, los equipos deben estar protegidos con contraseñas de alta complejidad, configurar protectores de equipo, y bloqueo de equipos que no estén bajo actividad.

- Guardar bajo llave la información sensible de la alcaldía municipal de Guachetá.

7.8 POLITICA PARA LA SEGURIDAD DE LAS OPERACIONES

7.8.1 Políticas generales de la seguridad de las operaciones

Las políticas generales de la seguridad de las operaciones son un instrumento para que funcionarios, servidores públicos, contratistas protejan los servicios internos y externos que ofrece la entidad, así mismo cumplir con las metas establecidas en el plan de desarrollo.

Objetivo

Asegurar el adecuado desarrollo de los procesos de información de la alcaldía municipal de Guachetá.

Aplicabilidad

Las políticas son aplicables de manera transversal a todos los procesos de la entidad.

Directrices

- Realizar El documento de los procedimientos de cambios en los procesos operativos, los sistemas e instalaciones del proceso de información, verificando su cumplimiento.

- Definir los controles necesarios para el acceso no autorizado, protección de software malicioso, para garantizar la seguridad de los datos y los servicios de red de la alcaldía municipal de Guachetá.

- Se debe mantener actualizado el antivirus en todos los equipos de la alcaldía municipal de Guachetá, bajo la supervisión de la oficina de sistemas.

- El área de sistemas realizara copias de respaldo de la información, del software e imágenes de los sistemas y ponerlas a prueba regularmente.

- El área de sistemas elaborara y conservara, revisara regularmente los registros acerca de las actividades de usuario, fallas, excepciones y eventos de seguridad de la información para resolver los inconvenientes que se lleguen a presentar.

- El área de sistemas debe ejercer el control en los cambios en la entidad, en los procesos, en las instalaciones y en los sistemas de información.

- El área de sistemas generara control en la debida utilización de los recursos para garantizar el desempeño del sistema.

- El área de sistemas es la encargada de realizar instalación se software y aplicaciones en los equipos, si se requiere de una instalación especial, de igual forma se debe contar con el aval y permiso de esta oficina.

- El área de sistemas establecerá e implementara las reglas para la instalación de software por parte de los usuarios, teniendo en cuenta los derechos de autor y propiedad intelectual.

- Los funcionarios, contratistas deben informar al área de sistemas cualquier vulnerabilidad técnica que se presente a los sistemas de información, para que esta área evalué y tome las medidas pertinentes para tratar el riesgo asociado.

- Sincronizar los relojes de los sistemas de procesamiento de información, para que se refleje solo una fuente de referencia de tiempo.

- Realizar auditoria a los equipos de procesamiento de información, agendándola con anterioridad, evitando interrupción en el desarrollo del proceso de la organización.

- Planificar adecuadamente las visitas de auditoria de sistemas, con el fin de evitar interrupciones en los proceso de la entidad.

7.9 POLITICA PARA LA SEGURIDAD DE LAS COMUNICACIONES

7.9.1 Políticas generales para la seguridad de las comunicaciones

La seguridad de la información es un compromiso de funcionarios, servidores públicos, y ante la proliferación de amenazas que están latentes, como software malicioso, virus, troyanos, etc. se hace necesario la creación de las políticas para la seguridad de las comunicaciones, estableciendo criterios de protección de la información garantizando la confidencialidad, integridad, disponibilidad, y accesibilidad de la información que se emite o se recibe por los diferentes canales.

Objetivo

Asegurar y mantener la protección de la información bajo el correcto funcionamiento de las instalaciones de procesamiento de la información y comunicaciones, estableciendo responsabilidades y procedimientos para la gestión y operación.

Aplicabilidad

Las políticas son aplicables a sistemas de redes, sistemas de comunicación, sistemas de procesamiento y transmisión de informacion, área de sistemas.

Directrices

Pertenece al personal encargado del área de sistemas:

- Crear los controles especiales para salvaguardar la confidencialidad e integridad del procedimiento de los datos que pasan a través de las redes públicas, y proteger los sistemas conectados.

- Implementar los controles especiales que garantice la disponibilidad y accesibilidad de los servicios de red y equipos conectados.

- Se debe reporta a la oficina de sistemas cualquier anomalía, amenaza en la red.

- Realizar separación en las redes de los grupos de servicios información, usuarios y sistemas de información.

- Se debe evitar navegar por páginas no seguras, ingresar a sitios web que permitan explotar vulnerabilidades.

- Al realizar la transferencia de información se debe garantizar la protección de la información, de forma física y/o digital.

- El uso del correo electrónico debe ser solo exclusivo para fines de trabajo, no personal ya que este correo electrónico esta monitoreado por el programa gobierno en línea, del ministerio de las TIC´S.

- Definir la norma de regulación del uso del correo electrónico en la alcaldía municipal de Guachetá.

- El uso de internet debe ser exclusivo para cumplir las actividades relacionadas con el trabajo y funciones a desempeñar.}

- Instalar y actualizar periódicamente software para detección y prevención de software malicioso.

- El responsable de la contratación de la entidad creara el compromiso de confidencialidad a firmar por los funcionarios, servidores públicos, contratistas y terceros que desarrollen funciones en la entidad, y realizara asesoramiento sobre las sanciones que incurren al incumplir el acuerdo.

7.10 POLITICA PARA LA ADQUISICION, DESARROLLO Y MANTENIMIENTO DE SISTEMAS

7.10.1 Políticas generales para la adquisición, desarrollo y mantenimiento de sistemas

Las políticas generales para la adquisición, desarrollo y mantenimiento de sistemas, es la herramienta que permite crear los parámetros que permitan garantizar la seguridad de la información durante el procesamiento de la interno y salida de datos durante todo el ciclo de vida.

Objetivo

Asegurar los controles de seguridad para la información, a través de la documentación de normas y procedimientos que se aplicaran durante todo el ciclo de vida

Aplicabilidad

Las políticas son aplicables área de sistemas.

Directrices

- Definir el procedimiento de la administración de claves.

- Definir el procedimiento de cambios en los sistemas, seguridad en las plataformas de la entidad, control de código malicioso.

- Garantizar el cumplimiento de la seguridad para el software.

7.11 POLITICA PARA LA GESTION DE INCIDENTES DE SEGURIDAD DE LA INFORMACION

7.11.1 Políticas generales para la gestión de incidentes de seguridad de la información

Las políticas generales para la gestión de incidentes de seguridad de la información permiten generar el enfoque coherente, eficaz, transparente para gestión de los incidentes de la seguridad de la información en la entidad.

Objetivo

Generar un enfoque coherente y eficaz para la gestión de incidentes de la seguridad de la información, incluida sobre la comunicación sobre eventos de seguridad y debilidades.

Aplicabilidad

Las políticas son aplicables área de sistemas, procesos de la entidad.

Directrices

- Comunicar los incidentes de seguridad al área de sistemas a través de los canales asignados por la entidad, dentro del menor tiempo posible.

- Implementar controles detallados de acuerdo al incidente presentado, generar recuperación de la información de acuerdo a la violación de seguridad, realizar las correcciones necesarias.

8.RECOMENDACIONES

- El estudio realizado deja ver que los activos de información de la alcaldía municipal de Guachetá, presentan un riesgo intolerable, la recomendación es aplicar las políticas de seguridad desarrolladas para cada control.

- Aplicar un sistema de seguridad de la información para la alcaldía municipal de Guachetá.

- Se debe realizar la clasificación de la información de acuerdo a lo indicado en el manual de clasificación de la información de presidencia de la república.

- Aplicar los controles del estándar ISO/IEC 27001:2013, que de acuerdo al análisis realizado a la entidad se determina presenta mayor importancia.

- Generar conciencia de la importancia de la seguridad de la información en los funcionarios, contratistas y demás usuarios que tienen acceso directo a la información, ya que estos representan una de las mayores amenazas para los activos de información.

9.CONCLUSIONES

- La alcaldía municipal de Guachetá presenta un nivel intolerable de riesgo de los activos informáticos, dejando fallas visibles que se deben controlar y generar el plan de acción de mejora, para garantizar la seguridad de la información.

- Los funcionarios, servidores públicos, contratistas por falta de capacitación, de prevención, en su mayoría son causantes de las amenazas a las que está expuesta los activos informáticos de la alcaldía municipal de Guachetá.

- Las instalaciones de la alcaldía municipal de Guachetá están en un riesgo alto, es fuente importante para no garantizar completamente la protección de los activos informáticos.

- Se realiza la aplicación de los controles del estándar ISO/IEC 27001:2013, de acuerdo a lo requerido por la entidad, después de realizar el análisis de riesgo.

- A través de la aplicación de las políticas de seguridad de la información, con compromiso y disciplina se lograra estructurar el sistema de gestión de seguridad de la información para la al alcaldía municipal de Guachetá, garantizando la integridad, confidencialidad, disponibilidad, accesibilidad, legalidad, confiabilidad, No repudio de la información.

BIBLIOGRAFÍA

AMAYA TARAZONA. Carlos. Sistema de gestión de la seguridad de la información. UNAD. 2013. Bogotá.

COLLAZOS BALAGUER. M. La nueva version ISO 27001:2013. Peru. Un cambio de integracion de los sistemas de gestion.p.17.

COLOMBIA. MINISTERIO DE TECNOLOGIAS D-E LA INFORMACION Y LAS COMUNICACIONES. Decreto Número 2573 De 2014: (12, Diciembre, 2014). Por el cual se establecen los lineamientos generales de la Estrategia de Gobierno en línea, se reglamenta parcialmente la Ley 1341 de 2009 y se dictan otras disposiciones. Bogotá D. C., El Ministerio 2014. 9p.

GUZMAN SILVA. Carlos. Alberto. Diseño de un sistema de gestión de seguridad de la información para una entidad financiera de segundo piso. Institución Universitaria POLITÉCNICO GRANA COLOMBIANO. Bogotá D. C. 2015. P13-17. Disponible en internet: http://repository.poligran.edu.co/bitstream/handle/10823/654/Proyecto%20de%20Grado%20SGSI%20-%20IGM-%20CarlosGuzman%20%28FINAL%29.pdf?sequence=1&isAllowed=y

COLOMBIA. CONGRESO DE LA REPUBLICA. Ley 527 de 1999. Bogotá. (Agosto 21 de 1999).Diario oficial N°43.673 de 21 de Agosto de 1999.

COLOMBIA. CONGRESO DE LA REPUBLICA. Ley 1341 de 2009. Bogotá. (30 de Julio de 2009). Diario oficial N| 47.426 de 30 de Julio de 2009.

COLOMBIA. CONGRESO DE LA REPUBLICA. DECRETO 2578 de 2012**.** Bogotá. (13 de Diciembre de 2012). Diario Oficial N° 48.648 del 13 de Diciembre de 2012.

COLOMBIA. CONGRESO DE LA REPUBLICA. Decreto 2573 De 2014. Bogotá. (12 de Diciembre de 2014). Diario oficial N° 49.523 del 12 de Diciembre de 2012

COLOMBIA. CONGRESO REPUBLICA DE COLOMBIA. ley 1273 de 2009. (Enero 5 2009).Diario oficial N° 47.223 del 5 de Enero de 2009.

COLOMBIA. CONGRESO DE LA REPUBLICA. Ley 1341 de 2009. Bogotá. (30 de Julio de 2009).Diario oficial 47.426 de 30 de Julio de 2009.

COLOMBIA. CONGRESO DE LA REPUBLICA. Ley 1150 DE 2007. Bogotá. (Septiembre 20 de 2007). Diario oficial N| 46.757 de 20 de Septiembre 2007.

COLOMBIA. CONGRESO REPUBLICA DE COLOMBIA. Ley 599 DE 2000. (24 de Julio de 2000). Diario oficial N° 44.097 del 24 de Julio de 2000.

COLOMBIA.CONGRESO DE LA REPUBLICA. Ley 1712 2014.Bogota. (6 Marzo 2014). Diario Oficial N° 49.084 de 6 de Marzo de 2014.

ESPAÑA. PORTAL DE ADMINISTRACION ELECTRONICA. MAGERIT v.3: Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Libro 1. 2012.

HURTADO DE BECERRA, Jacqueline. Metodología de la investigación holística. Caracas Venezuela, Edit. Sypal. 2000. Pág 38-39.

NORMA TÉCNICA NTC-ISO/IEC COLOMBIANA 27001. Tecnología de la información. Técnicas de seguridad. Sistemas de gestión de la seguridad de la información (SGSI). Requisitos. NTC - ISO/IEC 27001.Bogotá, D. C.INCONTEC. 2006-03-22. 45p.

RAMÍREZ VILLEGAS. Gabriel. CONSTAIN MORENO. Gustavo. modelos y estándares de seguridad informática: ISO 2705, Zona centro sur: Cead Palmira. Cead Popayán.UNAD.2012.25-34p.

UNIVERSIDAD PEDAGOGICA EXPERIMENTAL LIBERTADOR, 2006 FEDUPEL, Manual de trabajos de grado de especialización y maestría y tesis Doctorado.pag.13.

WEBGRAFIA

_____.ALEGSA. Diccionario informático. Definición de sistema informático. Disponible en internet: http://www.alegsa.com.ar/Dic/sistema_informatico.php.

_____Blog especializado en sistemas de gestión de seguridad de la información. ISO 27001: los activos de información. Disponible en internet: http://www.pmg-ssi.com/2015/03/iso-27001-los-activos-de-i

_____Blog especializado en sistemas de gestión de seguridad de la información. iso 27001:Los activos de información. 30 de Marzo 2015. Disponible en internet: http://www.pmg-ssi.com/2015/03/iso-27001-los-activos-de-i

_____GUZMAN SILVA.C.A. Institución Universitaria Politécnico Grana Colombiano.2015. P13-17. Disponible en internet: http://repository.poligran.edu.co/bitstream/handle/10823/654/Proyecto%20de%20Grado%20SGSI%20-%20IGM-%20CarlosGuzman%20%28FINAL%29.pdf?sequence=1&isAllowed=y

_____. DUANY DANGEL. Armando. Sistemas de Información.2010. Disponible en internet. http://www.econlink.com.ar/sistemas-informacion/definicion.

_____."El control Interno": Evaluación de riesgos". Internet: (http://datateca.unad.edu.co/contenidos/233004/CONTROL_INTERNO_Y_AUDITORIA.pdf.)

_____."El control Interno": actividades de control". Internet: (http: //datateca.unad.edu.co/contenidos/233004/CONTROL_INTERNO_Y_AUDITORIA.pdf.).

_____.EL PORTAL DE ISO 27002 EN ESPAÑOL. ISO 27002.ES. "Portal de soluciones técnicas y organizativas de referencia a los CONTROLES DE ISO/IEC 27002", Internet: (http://www.iso27000.es/iso27002.html).

_____. ESPAÑA, GOBIERNO DE EDUCACION CULTURA Y DEPORTE, Monográfico Introducción a la seguridad informática/seguridad de la información, 2012.P2. Disponible en internet: http://recursostic.educacion.es/observatorio/web/ca/software/software-general/1040-introduccion-a-la-seguridad-informatica?start=1

_____."Investigación descriptiva (s/f). [Documento en línea]". Internet: (http://www.mistareas.com.ve/investigacion-descriptiva.htm [Consulta: 2010, Mayo 18])

_____.ORGANIGRAMA. "¿Cómo estamos organizados? Internet: organigrama alcaldia municipal de Guacheta. Internet: http://guacheta-cundinamarca.gov.co/apc-aa files/353035623266393663396661313038 64/organigrama.jpg

_____.PACHECO. Federico. Welivesecurity. s.f. Disponible en internet: https://www.welivesecurity.com/la-es/2010/09/10/la-importancia-de-un-sgsi/

_____.PRESIDENCIA DE LA REPUBLICA, Guía para la clasificación de la información de acuerdo con sus niveles de seguridad. Bogotá D. C. (Marzo de 2007). P3-18.Dispponible en internet: http://es.presidencia.gov.co/dapre/DocumentosSIGEPRE/G-GD-02-calificacion-informacion.pdf

_____"¿Qué significa vulnerabilidad?". Internet: (http://www.unisdr.org/2004/campaign/booklet-spa/page8-spa.pdf).

COLOMBIA. ALCALDIA MUNICIPAL DE GUACHETA. "Generalidades". Internet: http://guacheta-cundinamarca.gov.co/informacion_general.shtml.

_____.RCN RADIO. Ataque cibernético en Colombia ha afectado a unas 11 empresas privadas. (Mayo 2015).Disponible en internet: http://www.rcnradio.com/nacional/ataque-cibernetico-en-colombia-ha-afectado-a-unas-11-em

_____."Salud y Seguridad. ISO 27001:2013. Sistemas de gestión de seguridad de la información". Disponible en internet: http://www.sgs.co/es-ES/Health-Safety/Quality-Health-Safety-and-Environment/Risk-Assessment-and-Management/Security-Management/ISO-27001-2013-Information-Security-Management-Systems.aspx

_____. UNAD. Grupo de investigación ECBTI.Bogota.2016. Disponible en internet: https://academia.unad.edu.co/ecbti/investigacion-y-productividad/grup

_____.UNISDR. ¿Qué significa vulnerabilidad? Disponible en internet: http://www.unisdr.org/2004/campaign/booklet-spa/page8-spa.pdf

_____."Vulnerabilidad". Disponible en internet: https://es.scribd.com/document/323783504/Que-Significa-Vulnerabilidad.

ANEXOS

Anexo A. Declaración de Aplicabilidad SOA

Tabla 27. Declaración de Aplicabilidad SOA

		Objetivo de control	Aplica SI/NO	Justificación	Cumple SI/NO	Justificación
A.5 POLÍTICAS DE SEGURIDAD						
Objetivo del Control	**A. 5.1 Directrices establecidas por la dirección para la seguridad de la información.**					
Control	**A. 5.1.1 Políticas para la seguridad de la información.**	La dirección debe aprobar un documento de política de seguridad de la información y lo debe publicar y comunicar a todos los empleados y partes externas pertinentes.	SI	Los controles permiten salvaguardar la información y proteger la confidencialidad e integridad de la misma.	NO	No existen políticas definidas para la seguridad de la información, se mantiene un control para salvaguardar la información.
Control	**A. 5.1.2 Revisión de las políticas para la seguridad de la información.**	La política de seguridad de la información se debe revisar a intervalos planificados o cuando se producen cambios significativos, para garantizar que sigue siendo adecuada, suficiente y eficaz.	SI	Con la política establecida se permitirá hacer seguimiento y auditorías al proceso de seguridad de la información.	NO	No existe política establecida para este control.

Continuidad (Tabla 27)

		Objetivo de control	Aplica SI/NO	Justificación	Cumple SI/NO	Justificación
A.6 ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACION						
Objetivo del Control	**A.6.1 Organización interna**					
Control	**A.6.1.1 Roles y responsabilidades para la seguridad de la información**	La dirección debe aprobar un documento de política de seguridad de la información y lo debe publicar y comunicar a todos los empleados y partes externas pertinentes.	SI	La dirección debe aprobar un documento de política de seguridad de la información y lo debe publicar y comunicar a todos los empleados y partes externas pertinentes.	NO	No existe política de seguridad sobre este control.
Control	**A.6.1.2 Separación de deberes**	Los deberes y áreas de responsabilidad en conflicto deberían separar para reducir las posibilidades de modificación no autorizada o no intencional, o el uso indebido de los activos de la organización.	SI	El control permitirá crear las responsabilidades de los funcionarios frente a la seguridad de la información.	NO	No existe política establecida para este control.
Control	**A.6.1.3 Contacto con las autoridades**	Se deberían mantener contactos apropiados con las	SI	La política permite estipular el proceso a desarrollar al	NO	No existe política para este control.

		autoridades pertinentes.		encontrar incidentes contra la seguridad de la información de la entidad.		
Control	**A.6.1.4 Contacto con grupos de interés especial.**	Es conveniente mantener los contactos apropiados con grupos de interés especiales, otros foros especializados en seguridad de la información, y asociaciones de profesionales.	SI	Permite estipular el contacto que se debe tener con otras entidades en tema de seguridad de la información.	SI	Se mantiene comunicación directa con los líderes de gobierno en línea.
Control	**A.6.1.5 Seguridad de la información en la gestión de proyectos.**	La seguridad de la información se debería tratar en la gestión de proyectos, independientemente el tipo de proyecto.	SI	La política permite proteger la información de los proyectos en ejecución.	NO	No existe política definida para este control.
Objetivo del Control	**A.6.2 Dispositivos para movilidad y teletrabajo.**					
Control	**A.6.2.1 Política de uso de dispositivos móviles.**	Se debería adoptar una política y unas medidas de seguridad de soporte, para gestionar los riesgos introducidos por el uso del dispositivo móvil.	SI	Se aplicara lineamientos del debido uso del celular corporativo.	NO	No existe política de seguridad sobre este control.

Continuidad (Tabla 27)

		Objetivo de control	Aplica SI/NO	Justificación	Cumple SI/NO	Justificación
A.7 SEGURIDAD DE LOS RECURSOS HUMANOS						
Objetivo del Control	**A.7.1 Antes de asumir el empleo**					
Control	**A.7.1.1 Selección**	Las verificaciones de los antecedentes de todos los candidatos a un empleo se deberían llevar a cabo de acuerdo con las leyes, reglamentos y ética pertinentes, y deberían ser proporcionales a los requisitos de negocio, a la clasificación de la información a que se va a tener acceso, y a los riesgos percibidos.	Si	Al iniciar el proceso de contratación el personal encargado de esta área, solicita la documentación requerida para iniciar el proceso contractual.	SI	La entidad dentro del proceso de selección y contratación solicita documentos de antecedentes disciplinarios, fiscales, judiciales, certificación laboral, documentos soportes de hoja de vida, y demás documentos de acuerdo a lo estipulado por las leyes gubernamentales.
Control	**A.7.1.2 Términos y condiciones del empleo**	Los acuerdos contractuales con empleados y contratistas, deberían establecer sus responsabilidades y las de la	SI	Existe un perfil estipulado para cada cargo	SI	En las cláusulas del contrato se estipula la responsabilidad que asume el funcionario o contratista del cuidado y custodia de los elementos de trabajo y confidencialidad de la

		organización en cuanto a la seguridad de la información.				información.
Objetivo del Control	**A.7.2 Durante la ejecución del empleo**					
Control	**A.7.2.1 Responsabilidades de la dirección**	La dirección debería exigir a todos los empleados y contratistas la aplicación de la seguridad de la información de acuerdo con las políticas y procedimientos establecidos por la organización.	Si	El control de responsabilidades de la dirección, permite dejar estipulado los compromisos de la dirección frente a la seguridad de la información de la entidad.	NO	No existe política establecida para este control, se mantiene el control a través de auditoria por parte de la oficina de control interno.
Control	**A.7.2.2 Toma de conciencia, educación y formación en la seguridad de la información.**	Todos los empleados de la organización, y en donde sea pertinente, los contratistas, deberían recibir la educación y la formación en toma de conciencia apropiada, y actualizaciones regulares sobre las políticas y procedimientos pertinentes para su cargo.	SI	El control de conciencia, educación y formación permite, formar a los funcionarios, contratistas, de forma permanente sobre la importancia de la seguridad de la información.	NO	No existe política establecida para este control, no se realiza capacitación sobre seguridad informática.

Control	**A.7.2.3 Proceso disciplinario.**	Se debería contar con un proceso disciplinario formal el cual debería ser comunicado, para emprender acciones contra empleados que hayan cometido una violación a la seguridad de la información.	SI	El control permite crear los lineamientos para desarrollar el proceso disciplinario, al presentarse un delito o falta relacionada con la seguridad de la información.	NO	No existe política establecida para este control, pero existe mecanismos de llamado de atención a los funcionarios cuando un evento de esta clase se presente.
Objetivo del Control	**A.7.3 Terminación o cambio de empleo**					
Control	**A.7.3.1 Terminación o cambio de responsabilidades de empleo**	Las responsabilidades y los deberes de seguridad de la información que permanecen validos después de la terminación o cambio de contrato se deberían definir, comunicar al empleado o contratista y se deberían hacer cumplir.	Si	El control de terminación o cambio de responsabilidades permite estipular el proceso a seguir, cuando el funcionario se retira de la entidad o cambia de responsabilidades en la misma.	NO	No existe política establecida para este control. Es deficiente el control frente a este tema.

Continuidad (Tabla 27)

		Objetivo de control	Aplica SI/NO	Justificación	Cumple SI/NO	Justificación
A.8 GESTION DE ACTIVOS						
Objetivo del Control	**A.8.1 Responsabilidad por los activos**					
Control	**A.8.1.1 Inventario de activos**	Se deberían identificar los activos asociados con la información y las instalaciones de procesamiento de información, y se debería elaborar y mantener un inventario de estos activos.	Si	El control de inventario de activos, permite reforzar el trabajo que ha desarrollado la entidad sobre el inventario de los activos hasta fecha.	SI	Existe inventario de activos, falta mayor estipulación.
Control	**A.8.1.2 Términos y condiciones del empleo**	Los activos mantenidos en el inventario deberían tener un propietario.	SI	El control de propiedades de los activos permite estipular claramente, el propietario de la información.	SI	Se ha delegado la responsabilidad al funcionario jefe de dependencia.
Control	**A.8.1.3 Uso aceptable de los activos**	Se deberían identificar, documentar e implementar reglas para el uso aceptable de información y de activos asociados con información e	SI	El control permite realizar un adecuado control al uso de los activos de la entidad.	NO	No existe política establecida para este control.

		instalaciones de procesamiento de información.				
Control	**A.8.1.4 Devolución de activos**	Todos los empleados y usuarios de partes externas deberían devolver todos los activos de la organización que se encuentren a su cargo, al terminar su empleo, contrato o acuerdo.	SI	El control de devolución de los activos, permite ejercer el debido control a la devolución de los activos de la entidad.	NO	No existe política establecida para este control. No se ejerce un mayor control.
Objetivo del Control	**A.8.2 Clasificación de la información**					
Control	**A.8.2.1 Clasificación de la información**	La información se debería clasificar en función de los requisitos legales, valor, criticidad y susceptibilidad a divulgación o a modificación no autorizada.	SI	El control de clasificación de la información permitirá realizar el control del proceso de clasificación de la información en la entidad.	NO	No existe política establecida para este control.
Control	**A.8.2.2 Etiquetado de la información**	Se debería desarrollar e implementar un conjunto adecuado de procedimientos para el etiquetado de la información, de acuerdo con el	SI	El control de etiquetado de la información, permitirá realizar un mayor control de la información de	NO	No existe política establecida para este control. Se realiza rotulación.

		esquema de clasificación de información adoptado por la organización.		la entidad.		
Control	**A.8.2.3 Manejo de activos**	Se deberían desarrollar e implementar procedimientos para el manejo de activos, de acuerdo con el esquema de clasificación de información adoptado por la organización.	SI	El control permite de manejo de activos permite realizar el adecuado manejo de activos de la entidad.	NO	No existe política establecida para este control.
Objetivo del Control	**A.8.3 Manejo de los soportes de almacenamiento**					
Control	**A.8.3.1 Gestión de medios removibles de empleo**	Se deberían implementar procedimientos para la gestión de medios removibles, de acuerdo con el esquema de clasificación adoptado por la organización.	SI	El control de medios removibles, permitirá llevar un mayor control sobre los medios removibles de la información de la entidad.	NO	No existe política establecida para este control.
Control	**A.8.3.2 Disposición de los medios**	Se debería disponer en forma segura de los medios cuando ya no se requieran, utilizando procedimientos	SI	El control de disposición de medios, permitirá realizar el control sobre	NO	No existe política establecida para este control.

		formales.		los medios cuando ya no se requieran.		
Control	**A.8.3.3 Transferencia de medios físico**	Los medios que contienen información se deberían proteger contra acceso no autorizado, uso indebido o corrupción durante el transporte.	SI	El control de transferencia de medios físicos, permite realizar un adecuado control sobre los medios que se deben transportar, para protegerlos de acceso no autorizado.	NO	No existe política establecida para este control.

Continuidad (Tabla 27)

	Objetivo de control	**Aplica SI/NO**	**Justificación**	**Cumple SI/NO**	**Justificación**
A.9 CONTROL DE ACCESOS					
Objetivo del Control	**A.9.1 Requisitos del negocio para control de acceso**				
Control	**A.9.1.1 Política de control de acceso**	El control de acceso físico y lógico permite tener un control sobre los riesgos de divulgación de la información o acceso físico a los activos a personal no autorizado.	SI	El control de inventario de activos, permite reforzar el trabajo que ha desarrollado la entidad sobre el inventario de los activos hasta fecha.	NO	No existe política establecida para este control. Se ejerce un control físico y lógico.
Control	**A.9.1.2 Política sobre el uso de**	Solo se debería permitir acceso de	SI	El control de política sobre el	NO	No existe política establecida para este control.

	los servicios de red	los usuarios a la red y a los servicios de red para los que hayan sido autorizados específicamente..		uso de los servicios de red, permitirá controlar el acceso no autorizado a la red.		
Objetivo del Control	**A.9.2 Gestión de acceso usuarios**					
Control	**A.9.2.1 Registro y cancelación del registro de usuarios**	Se debería implementar un proceso formal de registro y de cancelación de registro de usuarios, para posibilitar la asignación de los derechos de acceso.	SI	El control de registro y cancelación de usuarios, permitirá realizar un control en el acceso y cambio de usuarios.	NO	No existe política establecida para este control.
Objetivo del Control	**A.9.3 Responsabilidades de los usuarios**					
Control	**A.9.3.1 Uso de la información de autenticación secreta**	Se debería exigir a los usuarios que cumplan las prácticas de la organización para el uso de información de autenticación secreta.	SI	El uso del control del uso de la información permitirá exigir el cumplimiento de las prácticas de la organización para el uso de información de autenticación secreta.	NO	No existe política establecida para este control.

Objetivo del Control	A.9.4 Control de acceso a sistemas y aplicaciones Responsabilidades de los usuarios					
Control	**A.9.4.3 Sistema de gestión de contraseñas**	Los sistemas de gestión de contraseñas deberían ser interactivos y deberían asegurar la calidad de las contraseñas.	SI	El control de sistema de gestión de contraseñas permitirá controlar el adecuado uso de contraseñas y su calidad.	NO	No existe política establecida para este control, pero se maneja el uso de contraseñas.

Continuidad (Tabla 27)

	Objetivo de control	Aplica SI/NO	Justificación	Cumple SI/NO	Justificación
A.10 CRIPTOGRAFIA					
Objetivo del Control	**A.10.1 Controles criptográficos**				
Control	**A.10.1.1 Política sobre el uso de controles criptográficos**	Se debería desarrollar e implementar una política sobre el uso de controles criptográficos para la protección de la información.	SI	El control permitirá llevar la revisión de los controles criptográficos que se realicen.	NO	No existe política establecida para este control.
Control	**A.10.1.2 Gestión de llaves**	Se debería desarrollar e implementar una política sobre el uso, protección y tiempo de vida de las llaves criptográficas durante todo su ciclo de vida.	SI	El control permite desarrollar la política sobre el uso y protección y tiempo de vida de las llaves criptográficas.	NO	No existe política establecida para este control.

Continuidad (Tabla 27)

		Objetivo de control	Aplica SI/NO	Justificación	Cumple SI/NO	Justificación
A.11 SEGURIDAD FÍSICA Y DEL ENTORNO						
Objetivo del Control	**A.11.1 Áreas seguras**					
Control	**A.11.1.1 Perímetro de seguridad física**	Se deberían definir y usar perímetros de seguridad, y usarlos para proteger áreas que contengan información sensible o crítica, e instalaciones de manejo de información.	SI	Descripción: El control permite desarrollar una política que defina los perímetros de seguridad para las áreas que se maneje información sensible o critica.	NO	No existe política establecida para este control, sin embargo la entidad realiza asignaciones del cuidado y protección de la información.
Control	**A.11.1.2 Controles físicos de entrada**	Las áreas seguras se deberían proteger mediante controles de entrada apropiados para asegurar que solamente se permite el acceso a personal autorizado.	SI	El control permite el desarrollo de la política que permita generar las herramientas sólidas para asegurar el ingreso solo al personal autorizado, con el fin de proteger las áreas seguras.	NO	No existe política establecida para este control, para proteger estas áreas se realizan procesos básicos de protección.
Control	**A.11.1.3**	Se debería diseñar y	SI	El control	NO	No existe política establecida

	Seguridad de oficinas, recintos e instalaciones	aplicar seguridad física a oficinas, recintos e instalaciones.		permite general las estrategias para asegurar las áreas físicas, recintos e instalaciones de la entidad.		para este control.se manejan las normas básicas de seguridad.
Control	**A.11.1.4 Protección contra amenazas externas y ambientales**	Se debería diseñar y aplicar protección física contra desastres naturales, ataques maliciosos o accidentes.	SI	El control permite definir una política para diseñar la protección física contra desastres naturales, ataques maliciosos o accidentes a la entidad.	NO	No existe política establecida para este control, se maneja la protección básica, la entidad presenta grandes riesgos en las instalaciones a desastres naturales o accidentes.
Control	**A.11.1.5 Trabajo en áreas seguras**	Se deberían diseñar y aplicar procedimientos para trabajo en áreas seguras.	SI	El control permite diseñar la política y aplicar procedimientos para trabajo en áreas seguras.	NO	No existe política establecida para este control, se realiza los controles normativos básicos.
Objetivo del Control	**A.11.2 Equipos**					
Control	**A.11.2.1 Ubicación y protección de los equipos**	Los equipos deberían estar ubicados y protegidos para reducir los riesgos de amenazas y	SI	El control permite el diseño de políticas de ubicación y protección de	NO	No existe política establecida para este control, se trabaja bajo las normas básicas de protección.

		peligros del entorno, y las oportunidades para acceso no autorizado.		los equipos para reducir amenazas y accesos no autorizados.		
Control	**A.11.2.2 Servicios de suministro**	Los equipos se deberían proteger contra fallas de energía y otras interrupciones causadas por fallas en los servicios de suministro.	SI	El control permite desarrollar la política que permita proteger a los equipos contra fallas de energía y demás interrupciones causadas por ausencia en los servicios de suministro.	NO	No existe política establecida para este control. Se aplica la norma básica del buen cuidado.
Control	**A.11.2.3 Seguridad del cableado**	El cableado de potencia y de telecomunicaciones que porta datos o soporta servicios de información debería estar protegido contra interceptación, interferencia o daño.	SI	El control permite desarrollar políticas que permitan proteger el cableado de interceptacione s, interferencias o daños.	NO	No existe política establecida para este control, se realizan mantenimientos preventivos.
Control	**A.11.2.4 Mantenimiento de equipos**	Los equipos se deberían mantener correctamente para asegurar su	SI	El control permite desarrollar una política que	NO	No existe política establecida para este control, se realiza mantenimiento a los equipos de forma eventual o cuando

		disponibilidad e integridad continuas.		permita realizar el mantenimiento de los equipos de forma preventiva y asegurar su disponibilidad e integridad.		surge alguna afectación.
Control	**A.11.2.5 Retiro de activos**	El control permite realizar la política que defina el proceso para el retiro de activos de la entidad.	SI	No existe política establecida para este control, se realiza un seguimiento básico al retiro de activos.	NO	No existe política establecida para este control, se realiza un seguimiento básico al retiro de activos.
Control	**A.11.2.6 Seguridad de equipos y activos fuera de las instalaciones**	e deberían aplicar medidas de seguridad a los activos que se encuentran fuera de las instalaciones de la organización, teniendo en cuenta los diferentes riesgos de trabajar fuera de dichas instalaciones.	SI	El control permite desarrollar la política para aplicar medidas de seguridad a los activos que se encuentren fuera de las instalaciones de la entidad.	NO	No existe política establecida para este control.
Control	**A.11.2.7 Disposición segura o reutilización de**	Se deberían verificar todos los elementos de equipos que contengan medios	SI	El control permite desarrollar la política para	NO	No existe política establecida para este control, sin embargo se realiza verificación de la información

	equipos	de almacenamiento, para asegurar que cualquier dato sensible o software con licencia haya sido retirado o sobrescrito en forma segura antes de su disposición o reutilización.		realizar la adecuada revisión de equipos que contengan medios de almacenamient o para asegurar que cualquier dato sensible o software con licencia haya sido retirado o sobrescrito en forma segura antes de su disposición o reutilización.		del equipo.
Control	**A.11.2.8 Equipos de usuario desatendidos**	Los usuarios deberían asegurarse de que a los equipos desatendidos se les dé protección apropiada.	SI	El control permite el desarrollo de la política de protección para los equipos desatendidos.	NO	No existe política establecida para este control, sin embargo quedan bajo la protección del jefe de dependencia.
Control	**A.11.2.9 Política de escritorio limpio y pantalla limpia**	Se debería adoptar una política de escritorio limpio para los papeles y medios de almacenamiento removibles, y una política de pantalla limpia en las	SI	El control permite desarrollar la política de escritorio limpio y pantalla limpia para asegurar la organización y	NO	No existe política establecida para este control. Realizan recomendaciones de la organización en las oficinas.

		instalaciones de procesamiento de información.		protección de la información.		

Continuidad (Tabla 27)

		Objetivo de control	Aplica SI/NO	Justificación	Cumple SI/NO	Justificación
A.12 SEGURIDAD DE LAS OPERACIONES						
Objetivo del Control	**A.12.1 Procedimientos operacionales y responsabilidades**					
Control	**A.12.1.1 Procedimientos de operación documentados**	Los procedimientos de operación se deberían documentar y poner a disposición de todos los usuarios que los necesiten.	Si	El control permite realizar la política para documentar el procedimiento y ponerlos a disposición de los usuarios que lo necesiten.	NO	No existe política establecida para este control. Se realiza documentación sobre algunos procesos.
Control	**A.12.1.2 Gestión de cambios**	Se deberían controlar los cambios en la organización, en los procesos de negocio, en las instalaciones y en los sistemas de procesamiento de información que afectan la seguridad de la información.	SI	El control permite desarrollar una política para generar lineamientos en los cambios que se realicen en las instalaciones y los sistemas de información que afecten la seguridad de la información de la entidad.	NO	No existe política establecida para este control. Sin embargo se maneja seguimiento básico a los cambios que se realizan en la entidad.
Control	**A.12.1.3 Gestión de capacidad**	Para asegurar el desempeño	SI	El control permite generar la	NO	No existe política establecida para este control. Se

		requerido del sistema se debería hacer seguimiento al uso de los recursos, hacer los ajustes, y hacer proyecciones de los requisitos sobre la capacidad futura.		política del buen uso de los recursos, para garantizar el buen desempeño de los sistemas.		realizan indicaciones verbales del buen uso de los recursos.
Objetivo del Control	**A.12.2 Protección contra códigos maliciosos**					
Control	**A.12.2.1 Protección contra amenazas externas y ambientales**	Se deberían implementar controles de detección, de prevención y de recuperación, combinados con la toma de conciencia apropiada de los usuarios, para proteger contra códigos maliciosos.	SI	El control permite desarrollar la política para implementar la directriz para la prevención de códigos maliciosos y toma de conciencia por parte de los usuarios de la protección de la información.	NO	No existe política establecida para este control. Realizan controles de instalación de antivirus, pero no realizan el seguimiento.
Objetivo del Control	**A.12.3 Copias de respaldo**					
Control	**A.12.3.1 Respaldo de**	Se deberían hacer copias de respaldo	SI	El control permite crear la política	NO	No existe política establecida para este control. Sin

	información	de la información, del software e imágenes de los sistemas, y ponerlas a prueba regularmente de acuerdo con una política de copias de respaldo aceptada.		de respaldo de copias de seguridad de la información del software e imágenes de los sistemas.		embargo realizan copias esporádicamente.
Objetivo del Control	**A.12.4 Registro y seguimiento**					
Control	**A.12.4.1 Registro de eventos**	Se deberían elaborar, conservar y revisar regularmente los registros acerca de actividades del usuario, excepciones, fallas y eventos de seguridad de la información.	SI	El control permite crear la política para crear directrices que permitan elaborar, conservar y revisar regularmente los registros de actividades de usuario, excepciones, fallas eventos de seguridad de la información.	NO	No existe política establecida para este control. En su totalidad de los sistemas de información se llevan registros de las actividades de los usuarios.
Control	**A.12.4.2 Protección de la información de registro**	Las instalaciones y la información de registro se deberían proteger contra alteración y	SI	El control permite elaborar la política para proteger las instalaciones y la	NO	No existe política establecida para este control.

		acceso no autorizado.		información de registros.		
Objetivo del Control	**A.12.5 Control de software operacional**					
Control	**A.12.5.1 Instalación de software en sistemas operativos**	Se deberían implementar procedimientos para controlar la instalación de software en sistemas operativos.	SI	El control permite crear la política para estipular los procedimientos a realizar en la instalación de software en sistemas operativos.	NO	No existe política establecida para este control. Sin embargo se realizan las recomendaciones generales de control de software.
Objetivo del Control	**A.12.6 Gestión de la vulnerabilidad técnica**					
Control	**A.12.6.1 Gestión de las vulnerabilidades técnicas**	Se debería obtener oportunamente información acerca de las vulnerabilidades técnicas de los sistemas de información que se usen; evaluar la exposición de la organización a estas vulnerabilidades, y tomar las medidas apropiadas para tratar el riesgo asociado..	SI	El control permite crear la política para conocer oportunamente acerca de las vulnerabilidades técnicas de los sistemas y tomar medidas preventivas.	NO	No existe política establecida para este control.

Control	**A.12.6.2 Restricciones sobre la instalación de software**	Se deberían establecer e implementar las reglas para la instalación de software por parte de los usuarios.	SI	El control permite establecer reglas para la instalación de software por parte de los usuarios.	NO	No existe política establecida para este control. Sin embargo se realizan las recomendaciones generales de control de software.
Objetivo del Control	**A.12.7 Consideraciones sobre auditorias de sistemas de información**					
Control	**A.12.7.1 Información controles de auditoría de sistemas**	Los requisitos y actividades de auditoría que involucran la verificación de los sistemas operativos se deberían planificar y acordar cuidadosamente para minimizar las interrupciones en los procesos del negocio.	SI	El control permite crear la política para realizar adecuadamente las auditorias de los sistemas operativos, sin realizar interrupción en los procesos operativos.	NO	No existe política estipulada para este control, las auditorias no se realizan.

Continuidad (Tabla 27)

	Objetivo de control	**Aplica SI/NO**	**Justificación**	**Cumple SI/NO**	**Justificación**
A.13 SEGURIDAD DE LAS COMUNICACIONES					
Objetivo del Control	**A.13.1 Gestión de la seguridad de las redes**				
Control	**A.13.1.1** Las redes se	Si	El control	NO	No existe política establecida

	Controles de redes	deberían gestionar y controlar para proteger la información en sistemas y aplicaciones.		permite crear la política para generar lineamientos de protección de la información en la red.		para este control. Se realiza los controles de protección básicos en la red.
Control	**A.13.1.2 Seguridad de los servicios de red**	Se deberían identificar los mecanismos de seguridad, los niveles de servicio y los requisitos de gestión de todos los servicios de red, e incluirlos en los acuerdos de servicios de red, ya sea que los servicios se presten internamente o se contraten externamente.	SI	El control permite crear la política para garantizar los mecanismos de seguridad de los servicios de red.	NO	No existe política establecida para este control.
Control	**A.13.1.3 Separación en las redes**	Los grupos de servicios de información, usuarios y sistemas de información se deberían separar en las redes.	SI	El control permite realizar la política para generar los lineamientos de separación en las redes de los servicios de información, usuarios y sistemas de	NO	No existe política establecida para este control.

				información.		
Objetivo del Control	**A.13.2 Transferencia de información**					
Control	**A.13.2.1 Políticas y procedimientos de transferencia de información**	Se debería contar con políticas, procedimientos y controles de transferencia formales para proteger la transferencia de información mediante el uso de todo tipo de instalaciones de comunicación.	SI	El control permite generar la política de transferencia de información garantizando la protección y seguridad de la misma.	NO	No existe política establecida para este control. Se realiza el proceso de transferencia con los cuidados básicos de protección.
Control	**A.13.2.2 Acuerdos sobre transferencia de información**	Los acuerdos deberían tener en cuenta la transferencia segura de información del negocio entre la organización y las partes externas.	SI	El control permite crear la política de transferencia de información entre la entidad y partes externas.	NO	No existe política establecida para este control.
Control	**A.13.2.3 Mensajería electrónica**	Se debería proteger adecuadamente la información incluida en la mensajería electrónica.	SI	El control permite diseñar la política del buen uso y la protección de la información en la mensajería electrónica.	NO	Descripción: No existe política establecida para este control. Se realiza las pautas de cuidado y protección de forma verbal.
Control	**A.13.2.4 Acuerdos de**	Se deberían identificar, revisar	SI	El control permite crear la	SI	No existe política establecida para este control. Se está

	confidencialidad o de no divulgación	regularmente y documentar los requisitos para los acuerdos de confidencialidad o no divulgación que reflejen las necesidades de la organización para la protección de la información.		política del diseño, uso del acuerdo de confidencialidad, para la protección de la información.		implementado una clausula en los contratos de prestación de servicios, donde se estipula la confidencialidad de los datos suministrados para el desarrollo de las funciones.

Continuidad (Tabla 27)

		Objetivo de control	Aplica SI/NO	Justificación	Cumple SI/NO	Justificación
A.14 ADQUISICIÓN, DESARROLLO Y MANTENIMIENTOS DE SISTEMAS						
Objetivo del Control	**A.14.1 Requisitos de seguridad de los sistemas de información**					
Control	**A.14.1.1 Análisis y especificación de requisitos de seguridad de la información**	Los requisitos relacionados con seguridad de la información se deberían incluir en los requisitos para nuevos sistemas de información o para mejoras a los sistemas de información existentes.	Si	El control permite crear la política para estipular las especificaciones y requisitos de la seguridad de la información, en los sistemas de información existentes o nuevos sistemas.	NO	No existe política establecida para este control.
Control	**A.14.1.3 Protección de transacciones**	La información involucrada en las transacciones de los	SI	El control permite crear la política para	NO	No existe política establecida para este control.

	de los servicios de las aplicaciones	servicios de las aplicaciones se debería proteger para evitar la transmisión incompleta, el enrutamiento errado, la alteración no autorizada de mensajes, la divulgación no autorizada, y la duplicación o reproducción de mensajes no autorizada		proteger la información involucrada en las transacciones de los servicios de aplicaciones y evitar transmisión incompleta.		

Continuidad (Tabla 27)

		Objetivo de control	Aplica SI/NO	Justificación	Cumple SI/NO	Justificación
A.16 GESTION DE INCIDENTES DE SEGURIDAD DE LA INFORMACION						
Objetivo del Control	**A.16.1 Gestión de incidentes y mejoras en la seguridad de la información**					
Control	**A.16.1.1 Gestión de incidentes y mejoras en la seguridad de la información.**	Se deberían establecer las responsabilidades y procedimientos de gestión para asegurar, una respuesta rápida, eficaz y ordenada a los incidentes de seguridad de la información.	Si	El control permite crear la política para establecer las responsabilidades y procedimientos de gestión para asegurar, una respuesta rápida, eficaz y	NO	Descripción: No existe política establecida para este control.

				ordenada a los incidentes de seguridad de la información.		

Fuente: Propiedad del autor

ANEXO B. Resumen Analítico RAE

RESUMEN ANÁLITICO RAE.

Título de Documento.	Propuesta de un sistema de gestión de seguridad de la información para la alcaldía municipal de Guachetá Cundinamarca, basado en la norma ISO/IEC 27001:2013
Autor	LOPEZ CRISTANCHO Fanny Esperanza
Palabras Claves	Amenazas, vulnerabilidades, riesgo, ISO/IEC 27001:2013, seguridad, controles, información, ataques, contingencia.
Descripción El desarrollo de la monografía es una propuesta de un sistema de seguridad de la información para la alcaldía municipal de Guachetá, con el fin de proteger los activos de la información de la entidad.	
Fuentes Bibliográficas	AMAYA TARAZONA. Carlos. Sistema de gestión de la seguridad de la información. UNAD. 2013. Bogotá. COLLAZOS BALAGUER. M. La nueva version ISO 27001:2013. Peru. Un cambio de integracion de los sistemas de gestion.p.17. COLOMBIA. MINISTERIO DE TECNOLOGIAS D-E LA INFORMACION Y LAS COMUNICACIONES. Decreto Número 2573 De 2014: (12, Diciembre, 2014). Por el cual se establecen los lineamientos generales de la Estrategia de Gobierno en línea, se reglamenta parcialmente la Ley 1341 de 2009 y se dictan otras disposiciones. Bogotá D. C., El Ministerio 2014. 9p. GUZMAN SILVA. Carlos. Alberto. Diseño de un sistema de gestión de seguridad de la información para una entidad financiera de segundo piso. Institución Universitaria POLITÉCNICO GRANA COLOMBIANO. Bogotá D. C. 2015. P13-17. Disponible en internet: http://repository.poligran.edu.co/bitstream/handle/10823/654/Proyecto%20de%20Grado%20SGSI%20-%20IGM-

%20CarlosGuzman%20%28FINAL%29.pdf?sequence=1&isAllowed=y

COLOMBIA. CONGRESO DE LA REPUBLICA. Ley 527 de 1999. Bogotá. (Agosto 21 de 1999).Diario oficial N°43.673 de 21 de Agosto de 1999.

COLOMBIA. CONGRESO DE LA REPUBLICA. Ley 1341 de 2009. Bogotá. (30 de Julio de 2009). Diario oficial N| 47.426 de 30 de Julio de 2009.

COLOMBIA. CONGRESO DE LA REPUBLICA. DECRETO 2578 de 2012**.** Bogotá. (13 de Diciembre de 2012). Diario Oficial N° 48.648 del 13 de Diciembre de 2012.

COLOMBIA. CONGRESO DE LA REPUBLICA. Decreto 2573 De 2014. Bogotá. (12 de Diciembre de 2014). Diario oficial N° 49.523 del 12 de Diciembre de 2012

COLOMBIA. CONGRESO REPUBLICA DE COLOMBIA. ley 1273 de 2009. (Enero 5 2009).Diario oficial N° 47.223 del 5 de Enero de 2009.

COLOMBIA. CONGRESO DE LA REPUBLICA. Ley 1341 de 2009. Bogotá. (30 de Julio de 2009).Diario oficial 47.426 de 30 de Julio de 2009.

COLOMBIA. CONGRESO DE LA REPUBLICA. Ley 1150 DE 2007. Bogotá. (Septiembre 20 de 2007). Diario oficial N| 46.757 de 20 de Septiembre 2007.

COLOMBIA. CONGRESO REPUBLICA DE COLOMBIA. Ley 599 DE 2000. (24 de Julio de 2000). Diario oficial N° 44.097 del 24 de Julio de 2000.

COLOMBIA.CONGRESO DE LA REPUBLICA. Ley 1712 2014.Bogota. (6 Marzo 2014). Diario Oficial N° 49.084 de 6 de Marzo de 2014.

ESPAÑA. PORTAL DE ADMINISTRACION ELECTRONICA. MAGERIT v.3: Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Libro 1. 2012.

	HURTADO DE BECERRA, Jacqueline. Metodología de la investigación holística. Caracas Venezuela, Edit. Sypal. 2000. Pág 38-39. NORMA TÉCNICA NTC-ISO/IEC COLOMBIANA 27001. Tecnología de la información. Técnicas de seguridad. Sistemas de gestión de la seguridad de la información (SGSI). Requisitos. NTC -ISO/IEC 27001.Bogotá, D. C.INCONTEC. 2006-03-22. 45p. RAMÍREZ VILLEGAS. Gabriel. CONSTAIN MORENO. Gustavo. modelos y estándares de seguridad informática: ISO 2705, Zona centro sur: Cead Palmira. Cead Popayán.UNAD.2012.25-34p. UNIVERSIDAD PEDAGOGICA EXPERIMENTAL LIBERTADOR, 2006 FEDUPEL, Manual de trabajos de grado de especialización y maestría y tesis Doctorado.pag.13.

Contenido: El objetivo general del proyecto:

Proponer el sistema de gestión de seguridad de la información para la alcaldía municipal de Guachetá-Cundinamarca, basado en la norma ISO/IEC 27001:2013, utilizando como metodología de análisis de riesgo MAGERIT V3.

Objetivos Específicos

Revisar el estado actual de la seguridad de la información en la alcaldía municipal de Guachetá.

Clasificar los activos de información con que cuenta la alcaldía municipal de Guachetá, utilizando la metodología MAGERIT V3.

Determinar las amenazas y riesgos a que están expuestos los activos de información.

Aplicar controles de la norma ISO 27001:2013 a los activos de información.

Proponer las políticas de seguridad de la información basadas en la norma ISO 27001:2013

En el desarrollo del proyecto se realizó identificación de los activos de la entidad, amenazas y valoración de riesgo en el que se encontraban, aplicar los controles de seguridad de la norma ISO 27001:2013 a los activos de información, y proponer las políticas de seguridad que brinden protección a los activos informáticos.

Metodología El método holístico se utilizara para construir la propuesta del sistema de gestión de seguridad de la información para la alcaldía municipal de Guachetá-Cundinamarca, bajó la norma ISO 27001:2013, es una propuesta integrativa de la investigación y de la metodología.

Tipos de investigación:
La investigación exploratoria: observación, lectura y registro.
La investigación descriptiva: características de la descripción de los hechos.
La investigación comparativa: antecedentes, diferencias y semejanzas

Línea de investigación: La línea de investigación para el desarrollo de la propuesta es la de Gestión de sistemas de información, teniendo como precedente las líneas de investigación de la Escuela de ciencias básicas tecnología e ingeniería, cadena de sistemas, de la Universidad Nacional Abierta y a Distancia.

Etapas de la investigación:
Diagnóstico, planteamiento y fundamentación de la propuesta.
Procedimiento metodológico
Recursos necesarios para la ejecución
Análisis y conclusiones

Instrumentos de recolección de datos de la investigación:
Encuestas
Observaciones
Entrevista con los funcionarios de la entidad.
Entrevista con los funcionarios del área de sistemas.
Documentos gubernamentales relacionados con el tema de seguridad informática.
Libros, artículos de internet, revistas, normas, leyes, entre otros de forma física o electrónica.

Fases Metodológicas:
Fase I: Recolección y análisis de datos
Fase II: Seleccionar y evaluar alternativas, seleccionar y evaluar alternativas de solución de los antecedentes encontrados
Fase III: Construcción

Conclusiones
La alcaldía municipal de Guachetá presenta un nivel intolerable de riesgo de los activos informáticos, dejando fallas visibles que se deben controlar y generar el

plan de acción de mejora, para garantizar la seguridad de la información.

Los funcionarios, servidores públicos, contratistas por falta de capacitación, de prevención, en su mayoría son causantes de las amenazas a las que está expuesta los activos informáticos de la alcaldía municipal de Guachetá.

Las instalaciones de la alcaldía municipal de Guachetá están en un riesgo alto, es fuente importante para no garantizar completamente la protección de los activos informáticos.

Se realiza la aplicación de los controles del estándar ISO/IEC 27001:2013, de acuerdo a lo requerido por la entidad, después de realizar el análisis de riesgo.

A través de la aplicación de las políticas de seguridad de la información, con compromiso y disciplina se lograra estructurar el sistema de gestión de seguridad de la información para la al alcaldía municipal de Guachetá, garantizando la integridad, confidencialidad, disponibilidad, accesibilidad, legalidad, confiabilidad, No repudio de la información.

Recomendaciones.

El estudio realizado deja ver que los activos de información de la alcaldía municipal de Guachetá, presentan un riesgo intolerable, la recomendación es aplicar las políticas de seguridad desarrolladas para cada control.

Aplicar un sistema de seguridad de la información para la alcaldía municipal de Guachetá.

Se debe realizar la clasificación de la información de acuerdo a lo indicado en el manual de clasificación de la información de presidencia de la república.

Aplicar los controles del estándar ISO/IEC 27001:2013, que de acuerdo al análisis realizado a la entidad se determina presenta mayor importancia.

Generar conciencia de la importancia de la seguridad de la información en los funcionarios, contratistas y demás usuarios que tienen acceso directo a la información, ya que estos representan una de las mayores amenazas para los activos de información.

Fuente: Propiedad del autor

ANEXO C. Entrevista a Funcionarios

ALCALDIA MUNICIPAL DE GUACHETA

ENTREVISTA ABIERTA PARA FUNCIONARIOS

¿Conoce usted que es seguridad informática?
¿Sabe el valor cuantitativo y cualitativo de la información que está bajo su custodia?
¿Sabe cómo proteger la información física y digital?
¿Los equipos a su cargo tienen instalado algún antivirus?
¿considera que el área de trabajo es apropiada para el desempeño de la labor asignada?
¿Cuándo navega en internet conoce normas de seguridad para proteger la información?
¿Ha sido capacitado sobre el tema de seguridad de la información y activos de la empresa?

ANEXO D. Entrevista Encargado Área de Sistemas

ALCALDIA MUNICIPAL DE GUACHETA

ENTREVISTA ABIERTA ENCARGADO AREA DE SISTEMAS

¿Los funcionarios han recibido capacitación sobre el tema de seguridad informática?
¿Las instalaciones de cableado en la entidad cumplen con las normas establecidas?
¿Existen políticas de seguridad informática en la alcaldía municipal de Guachetá?
¿Cómo protegen los activos de información de la alcaldía de Guachetá?
¿Los equipos cuentan con software licenciado?
¿Los equipos cuentan con antivirus actualizado?
¿Con que periodicidad se realizan copias de seguridad?
¿Los funcionarios conocen las normas establecidas para los equipos de cómputo?
¿Se realiza de forma permanente mantenimiento de los equipos de cómputo?
¿las áreas de cómputo están libres de material combustible, como suministro de papel en exceso de las necesidades inmediatas?
¿Las áreas cuentan con un respectivo plan de contingencias?