DISEÑO DE POLÍTICAS PARA LA GESTIÓN DE LA INFORMACIÓN DE LA ALCALDÍA DE MONTECRISTO BOLÍVAR.

JESUS DAVID DIAZ QUICENO

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA UNAD
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA
ESPECIALIZACION EN SEGURIDAD INFORMATICA
MONTECRISTO
2018.

DISEÑO DE POLÍTICAS PARA LA GESTIÓN DE LA INFORMACIÓN DE LA ALCALDÍA DE MONTECRISTO BOLÍVAR.

JESUS DAVID DIAZ QUICENO

Proyecto de grado para optar el título de Especialista en Seguridad Informática.

Asesor
Esp. Ing. Christian Reynaldo Angulo.

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA UNAD
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA
ESPECIALIZACION EN SEGURIDAD INFORMATICA
MONTECRISTO.
2018.

Nota de aceptación:

_____

_____

_____

_____

_____

_____

_____

Firma del presidente del jurado.

_____

Firma del jurado

_____

Firma del jurado

Montecristo, Septiembre 19 de 2018

DEDICATORIA

Todos los esfuerzos que me han llevado a conseguir la victoria es gracias a Dios, el me dio la fuerza para lograr este sueño, de titularme como especialista en Seguridad Informática. Gracias al apoyo incondicional que me han brindado mis padres y las personas que han estado cerca de mí que han visto el sacrificio que yo he realizado para sacar adelante mi carrera profesional, a ellos dedico este triunfo.

AGRADECIMIENTOS.

Quiero exaltar el agradecimiento a Dios por darme la oportunidad de permitirme haber consagrado esta etapa de mi vida profesional, por haberme dado las fuerzas necesarias para cursar esta especialidad en Seguridad Informática a pesar de todos los impases presentados en este proceso.

Agradecer a mis padres por demostrarme sus muestras de cariño y apoyo incondicional en todos mis procesos formativos en el cual siempre han estado acompañándome con total disponibilidad.

Al ingeniero Christian Reynaldo Angulo quien fue mi guía en la preparación de este proyecto, agradezco su inmensa colaboración y a todo el cuerpo de docentes de la universidad que lograron formarme y compartirme el conocimiento para hoy lograr llegar a ser un especialista en Seguridad Informática.

Por último, agradecer a la UNAD por ser un pilar fundamental en la formación profesional y a la cual escogí para lograr cumplir esta meta. Con su ayuda logran crear un mejor país y con mejores oportunidades.

TABLA DE CONTENIDO Pág.

LISTA DE TABLAS.

Pág.

LISTA DE FIGURAS.

Pág.

LISTA DE FORMULAS.

Pág.

LISTA DE ANEXOS.

Pág.

GLOSARIO.

Activos: Son los datos relacionados con el sistema de información[1].

Adware: Software de publicidad creado para visualizar anuncios en un ordenador, abre ventanas emergentes generalmente mostradas en un explorador de internet. Con el tiempo puede llegar a ser molesto.

Antivirus: Programa diseñado para el descubrimiento de software con código malicioso o dañino que afecta el rendimiento de un equipo informático.

Ataque Web: Acción que se materializa, logrando afectar la integridad, disponibilidad y confidencialidad de un sistema de información.

BCP: Plan de continuidad del negocio. [2]

Confidencialidad: Evitar que personas no autorizadas puedan acceder a la información.

Delito Informático: Comportamientos ilícitos[3] que se llevan a cabo mediante herramientas electrónicas para atacar contra la seguridad de los datos informáticos.

Disponibilidad: La información y los recursos relacionados estén disponibles para el personal autorizado.

DLP: Data Leakage Protection - Protección de fuga de datos: Son aquellos parámetros que establecen lineamientos de seguridad, con el objetivo de controlar

[1] ROMERO, Luis Alonso. conceptos generales de SI. [online]. [Investigado: 22 de noviembre de 2018]. Consulta en Internet: Seguridad Informática, Conceptos generales. [http://cort.as/-RaSd]
[2] BCP: Plan de continuidad del negocio [online]. [Investigado 15 de septiembre de 2018]. publicado en Internet: [http://cort.as/-RaSo]
[3] Delito Informático: aquella acción antijurídica que tiene como objetivo destruir y dañar activos [online]. [Consultado 14 de febrero de 2019]. Publicado en Internet: [http://cort.as/-GfuJ]

la información, a fin de evitar que esta sea robada y llevada hacia otros sistemas de información de otras organizaciones.

Firewall: Llamado también “Cortafuegos”, se trata de un sistema el cual permite brindar protección a una computadora o una red de computadoras, de posibles amenazas provenientes de una red de terceros. Este mismo permite la filtración de paquetes de los datos que rondan en la red. En la mayoría de ocasiones es importante contar con un firewall en nuestra computadora o red de computadoras, para mantener la seguridad de nuestros sistemas.

Gusano Informático: Tiene la capacidad de replicarse a sí mismo para extenderse por las redes a las que se encuentra conectado un dispositivo.

Hacking: “hacking” [4] en términos informáticos se refiere a la conducta de entrar a un sistema de información de forma violenta y sin autorización, es decir vulnerando las barreras de protección establecidas para tal fin.

Impacto: Es la acción que genera una consecuencia negativa sobre cualquier activo de información, generando una amenaza de seguridad crítica.

Incidente: Todo tipo de amenaza materializada capaz de afectar los principios de seguridad de una organización. Es ocasionado mediante técnicas utilizadas para el robo de información y perdida de los datos.

Ingeniería Social: Es el uso de acciones estudiadas que permite obtener información confidencial de otras personas sin que estas se den cuenta de que la están revelando. Los hackers utilizan diferentes técnicas psicológicas y habilidades sociales y formas de ataque como los ataque por teléfono, ataque vía Internet,

[4] REYES PLATA, Alejandro. Ethical Hacking [online]. [Consultado: 22 de mayo de 2019]. Publicado en Internet: [http://cort.as/-RaTk]

Phishing, ataque vía SMS, Vishing, ataque vía correo electrónico, ataque cara a cara entre otros.

Integridad: Guardar la totalidad de la información, cuyo contenido debe permanecer inalterado a menos que sea modificado por personal autorizado.

Keylogger: Tipo de programa desarrollado que se encarga de capturar información por medio de pulsaciones del teclado o mouse, con el objetivo de enviar información a usuarios que buscan fines maliciosos.

Malware: Software malicioso que se encarga ejecutar scripts con el fin de cumplir un objetivo ya sea robo de información o daño a una computadora.

Phishing: Método de captura de información por medio de sitios web falsos[5].

Probabilidad: Es un suceso de que una ocurrencia pueda suceder o no.

Ransomware: Secuestra los datos de un ordenador pidiendo dinero por el rescate a cambio de liberarla. [6]

Riesgos: Es una amenaza que tiene la probabilidad de materializarse y puede ser controlada para que no cause impacto en una organización.

Troyano: Semejante a los virus informáticos, [7] pero el funcionamiento no suele ser destruido.

[5] RIVERO, Marcelo. Que es el Phishing [Consultado: 29 de mayo de 2019]. Publicado en Internet: [http://cort.as/-A5L8]

[6] PASTOR, Javier. Wanna Decryptor: así funciona el Ransomware que se ha usado en el ciberataque a Telefónica [online]. [Consultado: 18 de mayo de 2019]. Publicado en Internet: [http://cort.as/-RaVH]

[7]VIRUS TROYANO [online]. [Investigado: 29 de mayo de 2019]. Publicado en dirección: [http://cort.as/-RaVR]

Virus Informático: Son totalmente transparentes, suelen viajar dentro de archivos ejecutables[8], al ser instalados ejecutan acciones dentro de los ordenadores con el objetivo de perturbar el correcto funcionamiento.

Vulnerabilidad: Son debilidades en el software o hardware, que pueden ser aprovechados por un malware para afectar su información.

SI: Seguridad de la información.

:

[8] RIVERO, Marcelo. Que es el Phishing online Microsoft MVP Enterprise Security - Founder & CEO to Foro Spyware & Info Spyware. [Consultado: 29 de mayo de 2019]. Publicado en Internet: [http://cort.as/-RaVs].

RESUMEN.

Desde muchos años las organizaciones han hecho esfuerzos por dotarse de sistemas informáticos que permitan el manejo de la información para lograr aumentar su productividad, sin tener en cuenta que muchas de estas adoptan poco presupuesto económico en el campo de la seguridad informática.

La seguridad informática se convirtió en algo fundamental para las organizaciones, muchas se han preparado para proteger sus activos de información con la intención de mantener los principios de Seguridad de la información (SI).

Ha pasado mucho tiempo desde que se introdujo el término de Seguridad informática, y desde hace poco las organizaciones han tenido la necesidad de protegerse debido a la cantidad de amenazas que se encuentran en el ciberespacio por el desarrollo acelerado de la tecnología.

Actualmente existen muchas técnicas de intrusiones realizadas por distintos criminales informáticos que buscan realizar secuestros, robos de información y pérdida de datos. A medida que va avanzando la tecnología, el tema de la Ciberseguridad se ha vuelto más importante en el mundo y ha ocupado en los últimos años un gran perfil en Latinoamérica.

En Colombia se han generado grandes pérdidas económicas por descuido en la seguridad informática. Con el avance continuo de la internet son muchas las razones por la cuales se desconfía del manejo de información en sistemas, a diario muchos delincuentes informáticos buscan la manera de adentrar a los sistemas de información con el fin de dañar y violentar cualquier infraestructura tecnológica.

Por ello, es que se relaciona el caso de seguridad a la alcaldía municipal de Montecristo Bolívar. Esta entidad carece de sistemas que permitan el manejo óptimo de la información, y ante todo esto, mirando todas esas dificultades que se

presentan y que a simple vista se pueden visualizar en la organización del cual se está trabajando, se ven fallas con el control interno de la información. Por esto, es que en el siguiente proyecto se opta y se sustentaran los pasos para la realización de un proyecto aplicado que busque solucionar todos estos problemas y que buscan beneficiar a la administración municipal, que como propósito fundamental se busque realizar un diseño de políticas de seguridad al departamento de informática, que busque detectar e identificar vulnerabilidades y amenazas que se presenten en la entidad pública, con el fin de medir los riesgos y así definir los procesos y procedimientos de seguridad que se deben implementar para resguardar los valores de dicha organización.

Para todo este proceso se recogerá información de la alcaldía municipal a través de la observación, técnicas de encuestas y pruebas, con la idea de tener una visión general y mostrarles a los entes de control interno los problemas y fallas que se observan con el manejo la información.

ABSTRACT

For many years, organizations have made efforts to cope with computer systems that require information management to increase their productivity, without taking into account that many of these adopt little economic budget in the field of computer security.

Computer security has become essential for organizations, many have prepared to protect their information assets with the intention of maintaining the confidentiality, availability and integrity of information in computer systems.

It has been a long time since the term Computer Security was introduced, and organizations have recently had the need to protect themselves due to the number of threats found in cyberspace due to the accelerated development of technology.

There are currently many intrusion techniques carried out by different computer criminals who seek to kidnap, steal information and data loss. As technology

advances, the issue of cybersecurity has become more important in the world and has in recent years occupied a great profile in Latin America.

In Colombia, large economic losses have been generated due to carelessness in computer security.

With the continuous advancement of the internet, there are many reasons why information management in systems is distrustful, every day many computer criminals look for ways to get into information systems in order to damage and violate any technological infrastructure.

Therefore, the security case is related to the municipal mayor of Montecristo Bolívar. This entity lacks systems that allow the optimal management of information, and above all this, looking at all those difficulties that arise and that at first glance can be visualized in the organization of which you are working, failures are seen with internal control of the information. For this reason, it is that in the following project the steps for the realization of an applied project that seeks to solve all these problems and that seek to benefit the municipal administration are chosen and supported, which as a fundamental purpose is to design a management system for the information to the IT department, which seeks to detect and identify vulnerabilities and threats that occur in the public entity, in order to measure the risks and thus define the controls and security mechanisms that must be implemented to safeguard the information assets of that organization.

For all this process, information from the municipal mayor's office will be collected through observation, survey techniques and network traffic tests with the idea of having an overview and showing internal control entities the problems and failures of managing the security of the information.

INTRODUCCIÓN.

La seguridad de la información se convirtió en un factor importante en el progreso de una organización. Todas las entidades que procesen altos volúmenes de información están en la necesidad de protegerlas debido a la cantidad de peligros y amenazas que se han venido desarrollando a través de los años.

En la actualidad la tecnología en el mundo está en un crecimiento exponencial y a su vez están apareciendo nuevas amenazas que están afectando la seguridad de todas las plataformas tecnológicas, por eso la importancia de estar evolucionando constantemente con diferentes métodos implementados de (hardware y software) para contrarrestar las brechas de seguridad.

La gran preocupación de las organizaciones hoy en día es lograr cuidar los pilares de la SI. Por este motivo es que se han adoptado diferentes procedimientos de seguridad que permitan reducir los riesgos, con la intención de protegerse de los diferentes tipos de ataques.

Ninguna organización está totalmente protegida de los riesgos que existen, todas son susceptibles, por eso se han creado Normas internacionales de seguridad que explican la manera de cómo se deben proteger las organizaciones, y como aplicar las buenas prácticas de SI, se hace referencia al estándar ISO 27001 (SGSI).

La creación de un gobierno de Seguridad de la información permite a una organización tener los activos seguros y en este proyecto se busca que la información de la alcaldía de Montecristo Bolívar, este orientada por las normas que se encuentran establecidas en el estándar ISO 27001, teniendo en cuenta que este sistema puede ser adoptado a cualquier organización, sin importar su tamaño y/o actividad económica. Poner en marcha este sistema mejora la productividad de la empresa y reduce los niveles de riesgos presentes en todas las organizaciones.

1 DEFINICIÓN DEL PROBLEMA

1.1 PLANTEAMIENTO DEL PROBLEMA.

Desde que Montecristo se convirtió en un municipio, fueron los distintos programas sociales creados por el gobierno nacional que llegaron a esa población, lográndose situar en el palacio municipal. Debido a estos programas se logró que la alcaldía del municipio ofreciera todos estos servicios a la comunidad en general, e hizo que con el pasar del tiempo se preparara mejor en infraestructura física como en infraestructura tecnológica para lograr optimizar todos los procesos, y brindarle todos los servicios a la comunidad de la mejor manera. Esto permitió que en la actualidad todos los programas estén operando desde dichas instalaciones, y que hoy día se encuentran en total operación.

La Alcaldía municipal de Montecristo desde sus inicios siempre ha manejado grandes volúmenes de información, por los diversos proyectos y programas que se manejan. Con base en esto fue necesario crear una infraestructura tecnológica, que permitiera agilizar los procesos de forma sistematizada, lográndose instalar diversos aplicativos con diferentes funciones dentro de la organización y a raíz de esto permitió la instalación de servidores y equipos que ayudaran a mantener la operatividad de todos los procesos. Teniendo en cuenta visita técnica realizada al área de seguridad informática es evidente que en la actualidad la alcaldía municipal no tiene diseñados procedimientos de SI. En múltiples ocasiones se ha presentado pérdida y fuga de datos confidenciales por realizar malas prácticas de seguridad, lo que ha generado atrasos en los procedimientos internos. (GTIC-MCR009 Plan De Tratamiento De Riesgos De Seguridad Y Privacidad De La Información).

Tal como se ha mencionado anteriormente, se ha presentado desde meses anteriores perdida de información de manera inexplicable, el tráfico de información que se maneja en una de las dependencias de la misma ha generado pérdidas que han ocasionado grandes atrasos en los procedimientos internos de la alcaldía, del

mismo modo muchos equipos que se encuentran conectados a la red de internet de la alcaldía municipal, han perdido información del cual no se ha tenido certeza del porque no aparecen, equipos que de alguna forma se han ejecutado programas internos y han hecho que toda la información sea pérdida.

En visita técnica se encontró que el departamento administrativo de informática presenta una infraestructura de red propensa al secuestro de información, pues carece de medidas de seguridad, políticas que permitan prevenir ataques externos, entiéndase, acceso y robo de información en los sistemas.

El Avance acelerado del internet ha hecho que muchos delincuentes informáticos vulneren la SI de las empresas, existen indicios que existan ataques externos a la infraestructura tecnológica de la alcaldía municipal, esta por ser una entidad pública, el grado de exposición y daño al que este expuesto cada día es mayor.

En la Alcaldía Municipal de Montecristo se ha propuesto la creación de un gobierno de SI que estimule buenas prácticas en el manejo de la información y permita solucionar los problemas internos relacionados con el control al tráfico de datos en la red interna de la organización. La medida evitaría ataques cibernéticos y otro tipo de delito informático existente en la actualidad.

El problema descrito requiere fortalecer la infraestructura tecnológica con procedimientos, políticas, estándares de seguridad informática y/o de la información, adaptando medidas tales como el diseño de **UTM**, **DMZ**, **IDS**, **IPS**, **antimalware**, **Firewall** y otros elementos de Ciberseguridad que se constituyan en un valor agregado para superarlo. Se pretende la elaboración de políticas de SI que brinden soluciones optimas y eficaces, a fin de proteger la información interna de la alcaldía municipal, alcanzando a dar la certeza que la información y demás que se manejen a nivel interno en ellas sea totalmente confiable y estén totalmente protegidas.

1.2. FORMULACIÓN DEL PROBLEMA

¿Qué beneficios trae a la organización la implementación del diseño de políticas de gestión de SI, y de qué manera ayuda a reducir los eventos o incidentes que se presentan en la alcaldía Municipal de Montecristo?

2 JUSTIFICACIÓN

El proyecto pretende diseñar políticas de SI para la alcaldía municipal de Montecristo que solucionen la problemática planteada[9]. La idea es proponer en una primera parte un informe en el cual se exprese y se concientice a la parte interna de la administración, sobre cuáles son los peligros que tiene la alcaldía en cuestiones de SI, los diferentes modelos de ataques cibernéticos que existen y las metodologías que se utilizan para el robo de información, y demostrar que el departamento de sistemas adolece de las falencias y debilidades relacionadas con los procesos de control, de los peligros asociados con cibercriminalidad, delito informático y todas aquellas prácticas generadoras de vulnerabilidades a todo sistema de información.

A fin de plantear esto, llevar a una segunda parte el diseño del Gobierno de SI, que dé efectividad a la protección y preservación de la información, para que los riesgos presentes logren ser controlados con el fin de que no se materialicen y se pueda tener en todo momento la preservación de los principios de SI. La idea es incluir en este proyecto un desarrollo completo de políticas relacionadas a la seguridad informática.

Se ha tomado la decisión de realizar un gobierno de gestión de SI, con la finalidad de brindar condiciones confiables que propicien seguridad y tranquilidad en el buen manejo de la información a cada uno de los que hacen parte del área operativa de la administración municipal.

Este proyecto será muy importante para el desarrollo de la alcaldía, con esto se busca mejorar las adecuaciones tecnológicas y la infraestructura, para que se ajusten los procesos del manejo de la información, y logra así brindar a cada una de las dependencias el autocontrol y la suficiencia necesaria con la búsqueda de la

[9] VILLAR, Edson. Avance de la Ciberseguridad y SI, [online]. 1 ed. [Consultado: 6 de Mayo de 2018]. Publicado en Internet: Ciber-Riesgo y SI. [http://cort.as/-RaWO].

misma.

El trabajo estará desarrollado como un proyecto aplicado, que evalúe el cumplimiento actual de las normas colombianas enfocadas a la SI, y que contribuya de manera innovadora a la solución de los problemas internos de la Alcaldía.
El diseño que se desea realizar contribuye al desarrollo de la entidad, Se pretende realizar con la intención de que esté a la par de todas las organizaciones que ya tienen implementado su propio Gobierno de Seguridad.

3 OBJETIVOS

3.1 Objetivo General.

Diseñar un gobierno de SI, en la alcaldía Municipal de Montecristo, bajo el estándar ISO-IEC 27001, que permita identificar los peligros y controlar los riesgos que existen en el manejo de la información.

3.2 Objetivos Específicos.

- ✓ Realizar informe para el levantamiento de información que permita hacer análisis de los riesgos que están presentes en la infraestructura tecnológica de la alcaldía municipal.
- ✓ Definir los parámetros y políticas de seguridad que ayuden a disminuir los riesgos presentes en la infraestructura tecnológica de la organización.
- ✓ Proponer la implementación de procesos de control que pretendan minimizar y reducir los tipos de ataques que existen en la actualidad.
- ✓ Plantear un gobierno de gestión de SI, para toda la organización que permita conservar los pilares de la SI, de todos los activos de información.
- ✓ Diseñar el gobierno de SI para toda la infraestructura municipal que garantice la protección y conservación de los activos de información más valiosos de la entidad.

4. ALCANCE Y DELIMITACIÓN DEL PROYECTO.

El desarrollo del buen gobierno de SI, aplica a todos los funcionarios, procesos o terceros de la Alcaldía Municipal de Montecristo, que tengan contacto con los diferentes estados de la información propia o bajo su custodia.

Será desarrollado en la alcaldía municipal del Municipio de Montecristo, entre el año 2017 y 2018.

5 MARCO REFERENCIAL

5.1 ANTECEDENTES

Para la realización de este proyecto, se hizo una revisión bibliográfica relacionada en proyectos de la misma temática a la que aquí se sustenta, con el objetivo de abordar toda la temática referente a la SI, y no dejar excluida ninguna conceptualización de gran importancia en el campo que se está estudiando. Tomado cada proyecto se puede referenciar algunos más importantes relacionados al proyecto, los cuales son:

Nombre del proyecto “Cloud Computing”, [10] presentado por Luis Felipe González Hernández, a la (UNAD). Este proyecto quedo diseñado con el fin de crear prácticas de SI, para la protección de información almacenada en la nube.

“Protección de los sistemas de información - Empresa sitiosdima.net” [11], desarrollado por Javier Humberto Robayo López – Richard Mauricio Rodríguez, UNAD - Colombia, este proyecto está desarrollado para establecer prácticas de “Endurecimiento” a los sistemas informáticos por medio del método “Hardening”.

Proyecto denominado “Plan estratégico de SI, para empresa del sector asegurador”, [12] Presentado por Marisol Lozano Olave, en la Institución universitaria Politécnico Gran colombiano, el cual trata del desarrollo de estrategias para que los riesgos de información sean apropiadamente administrados, por intermedio de políticas de Gestión de Incidentes, eventos y control de cambios.

---

[10] GONZALEZ HERNANDEZ, Luis Felipe. Seguridad Informática Cloud Computing [online]. 2016. [Consultado 11 de abril de 2019]. Publicado en Internet: [http://cort.as/-RaWy].

[11] MARTINEZ, Pablo. ¿Qué es el HARDENING? Muy interesante [online]. Blogs Soporte TI. [Consultado: 21 de Marzo de 2019]. Publicado en Internet: [http://cort.as/-RaX6].

[12] LOZANO OLAVE, Marisol. proyecto plan estratégico SI. (PESI) para empresa del sector asegurador [online]. [Consultado: 6 de diciembre de 2018]. Publicado en Internet: [http://cort.as/-RaXD].

5.2 MARCO CONCEPTUAL.

Se relacionan algunos conceptos importantes relacionados al Gobierno de SI[13]:

- ✓ **Activo de información:** información que, por su importancia, son de gran utilidad para las actividades de una organización.
- ✓ **Amenazas:** Cualquier evento accidental o con intención que puede ocasionar algún daño a los sistemas informáticos, provocando pérdidas materiales, financieras o de algún otro tipo a la organización[14].
- ✓ **Amenazas Naturales:** Son las que se pueden presentar por Inundación, incendio, tormentas, Tsunamis, fallos eléctricos, explosiones, etc.
- ✓ **Amenazas De Agentes Externos:** Son amenazas presentadas por el envío masivo de correos que contienen virus informáticos (malware), ataques ocasionados por cibercriminales, sabotajes terroristas, intrusiones, robos o estafa.
- ✓ **Amenazas De Robos Internos:** Amenazas generadas por los mismos empleados, ocasionados por el descontento e inconformismo en contra de la organización.
- ✓ **Aceptación Del Riesgo:** es el momento en el que se admite la pérdida o ganancia que proviene de un riesgo particular.
- ✓ **Confidencialidad:** Aseguramiento de que el ingreso a la información sea realizado solo por quienes estén acreditados para consultarla.
- ✓ **Control De Acceso:** Implica quienes son los que tienen permisos a los sistemas informáticos de una organización. Son sistemas que restringen o permiten el acceso de usuarios a determinada área, valida los datos por medio de diferentes

[13] BAUTISTA TORRES, Luis. Política de SI, implementado a la empresa XYZ Soluciones [online]. [Consultado 3 diciembre de 2018]. Publicado en Internet: [http://cort.as/-RaXf.]
[14] MARKUS, Erb Amenazas y Vulnerabilidades [online]. Blogs Gestión de Riesgo de SI, [Consultado: 11 de octubre de 2018]. Publicado en Internet: [http://cort.as/-RaXt]

tipos de lectura, ya sea por control de huellas, por tarjetas u otro medio de autenticación.

- ✓ **Declaración De Aplicabilidad:** Documento que describe cuales son los controles pertinentes que se pueden aplicar para el SGSI de una organización.
- ✓ **Disponibilidad:** Permite que la información pueda ser consultada en cualquier momento y pueda ser utilizada por entidades, personas o procesos autorizados.
- ✓ **ISO:** International Standards Organization.- Organización de normalización más importante del mundo.
- ✓ **ISO 27000:** Orienta sobre la implementación de un SGSI a una organización. El SGSI busca reducir los peligros que se encuentra sometida la información.
- ✓ **ISO 27001:** Permite certificar la implementación de un SGSI en una empresa. Describe los pasos y procedimientos que se deben realizar para que las organizaciones tengan una mejora continua en todos los procesos.
- ✓ **ISO 27002:** Procedimiento que da orientación a realizar buenas prácticas de gestión de SI, Cuenta con recomendaciones importantes sobre los controles que se deben tomar para resguardar los sistemas de información.
- ✓ **ISO 27005:** Su propósito fundamental es la de gestionar los riesgos e incidentes que atentan contra la integridad de la información, esta normalización ha sido adoptada para que todas las organizaciones apliquen directrices a la gestión del riesgo.
- ✓ **ITIL:** Norma encaminada a la Gestión e investigación de incidentes de SI.
- ✓ **PCN**: Plan de Continuidad del Negocio
- ✓ **PDCA:** (Planear-Ejecutar-Verificar-Actuar)
- ✓ **PGR:** Plan de Gestión de Riesgos
- ✓ **DRP:** Plan de Recuperación de Desastres
- ✓ **MAGERIT:** Metodología de análisis y gestión del riesgo. Creada con el objetivo de reducir los peligros, y dar el tratamiento adecuado a la gestión de eventos e incidentes.
- ✓ **Normas ISO:** Organismo internacional encargado de regular las reglas de normalización y estandarización de las diferentes políticas relacionadas al

campo de la informática.

- ✓ **Políticas De Seguridad:** Es la base del SGSI, se encarga de velar por que sean establecidos niveles de seguridad, adecuados para cada una de las organizaciones. busca establecer reglas para ser aplicadas internamente y proteger las instalaciones de todo riesgo.
- ✓ **SGSI:** Estándar desarrollado para que las empresas puedan evaluar los peligros, identificarlos y la manera de cómo pueden ser controlados.
- ✓ **Seguridad De La Información (SI):** Establece lineamientos de seguridad para proteger los valores de la organización a través de controles, métodos y procedimientos de seguridad, con el objetivo bloquear el ingreso de intrusos no deseados, el éxito de ataques informáticos y la fuga de información.[15]
- ✓ **Seguridad Informática:** Procedimientos de seguridad que emplean las entidades para proteger los datos que utiliza una infraestructura[16] tecnológica y de telecomunicaciones.
- ✓ **Tratamiento del Riesgo:** Medidas implementadas que sirven darle tratamiento al riesgo, la manera en la que se puede controlar y como reducir las brechas de seguridad de cualquier evento o incidente de SI.

5.3 MARCO LEGAL.

Cantidades múltiples de fuentes del derecho, que existen para tomar como referencias, esta puede ser la ley, decreto, resolución, artículos, normas, la jurisprudencia, los acuerdos internacionales, que rigen la SI.

- Todo negocio debe tener sus propias políticas de seguridad en base a la información interna que maneja, la pérdida de estos genera grandes afectaciones económicas al rendimiento de una organización. El implementar políticas basadas en la estandarización internacional de **ISO 27001**, ayuda que toda empresa mantenga los pilares de SI, en continua operación.

[15] MARKUS, Erb. SI y protección de datos [online]. Blogs Estudio de los peligros en la seguridad informática. [Consultado: 21 de septiembre de 2018]. Publicado en Internet: [http://cort.as/-RaY0/].
[16] MARKUS, Erb. Definición de Seguridad informática [online]. Gestión de riesgo en la SI. [investigado: 21 de septiembre de 2018]. Publicado en Internet: [http://cort.as/-RaY7]

- Se debe evaluar la normativa legal colombiana contra los malos procedimientos, la tipificación de los delitos informáticos, creados como consecuencia del abuso de delincuentes informáticos.

El ICONTEC, establece políticas de gestión de SI, (SGSI), se ha convertido en un estándar que sirve de guía para que toda organización logre documentarse sobre políticas, normas internas, manuales y procedimientos de SI.

Se logra definir algunas normas que están relacionados a la SI, que ayuda proteger los datos y a la reducción de brechas de seguridad, a continuación, se definen:

5.3.1 LEY 1273 DE 2009

Ley que fue ingresada a la legislación colombiana, el cual tiene como nombre "**de la protección de la información y de los datos**". [17] Esta ley busca conservar la integridad de todo sistema de información, cualquier mal procedimiento ejecutado que atente contra cualquier sistema puede llevar a condenas aproximadas a los 10 años de prisión, y multas elevadas a quienes incurran en estos delitos. La ley castiga los atentados que se realicen en contra de los pilares de la SI.

5.3.2 LEY 527 DE 1999

Esta ley fue creada con el objetivo de regular el control del comercio electrónico, las firmas digitales y uso de los mensajes de datos[18].

5.3.3 LEY 962 DE 2005

Ley creada con el objetivo de concientizar a las organizaciones que ejercen funciones estatales hacer uso de las tecnologías de información y las comunicaciones Tics. Respaldado por el ministerio de telecomunicaciones.

[17] Proyecto de ley 1273 de 2009. Legislación colombiana denominada: "protección de la información y de los datos".
[18]Proyecto de ley 527 de 199, creada con el objetivo de regular el control del comercio electrónico, las firmas digitales, y uso de los mensajes de datos. [online] Bogotá DC, 21 de agosto 1999.

5.3.4 LEY 1341 DE 2009

Ley encaminada a la formulación de políticas públicas del sector de las TICS, a la protección de usuario, a la calidad y al desarrollo de las tecnologías[19].

5.3.5 LEY 1581 DE 2012 – LEY DE PROTECCION DE DATOS

Permite proteger los derechos fundamentales, como la defensa de los datos personales, el derecho a la intimidad[20]. Esta legislación se encuentra relacionada a los principios de seguridad y confidencialidad.

5.3.6 ISO/IEC 27001:2005

Es la norma que hace parte de la **ISO27000**, divulgada el 15 de octubre de 2005, contiene todas las guías, procesos y procedimientos básicos para la realización de un **SGSI**. Es la norma que certifica a una organización, y es efectuada por auditores externos.

De acuerdo con los peligros y riesgos existentes, la implementación de esta norma debería ser de carácter obligatorio en toda organización. Para el desarrollo de este se recomienda el ciclo Planificar – Hacer – Verificar – Actuar para un buen diseño del SGSI.

5.3.7 LA NORMA ISO 27001:2000

Con el transcurrir de los años esta norma ha sido actualizada a varias versiones[21], Esta describe las recomendaciones y procesos que se deben realizar para el aseguramiento de la información, no requiere de certificación, pero es necesario que todas las entidades, sin importar la razón social adopten estas medidas para tener sus activos protegidos, y a su vez servirá para que puedan obtener

[19] Ley 1341 (30, julio, 2009). se definen principios y conceptos sobre la SI y la organización de las TICS, Publicado en Internet: [http://cort.as/-J9nn]
[20] Proyecto de ley 1581 de 2012. Relacionada con la protección de datos personales, [online] Bogotá DC, 18 de octubre de 2012.
[21] ISO 27001, [online]. Norma ISO 27001. [Investigado: 15 de marzo de 2019]. Publicado en Internet: [http://cort.as/-RaYw]

certificación de SGSI. La **ISO 27001:2013** Abarca todos los aspectos de seguridad desde el desarrollo de políticas hasta aspectos legales.

La norma busca cumplir con un total de **56 objetivos**, para que se cumplan estos se deben medir **127 controles**, de acuerdo los pasos de la norma. Cada negocio decide si implementar o no los controles, dependiendo del nivel seguridad que desea tener para proteger sus activos de información.

5.3.8 ISO/IEC 27002:2005

En esta norma se identifican **11 dominios**, **39 objetivos de control** y **133 controles**[22]. Los dominios que se identifican son los siguientes:

- ✓ Políticas de Seguridad
- ✓ Organización de la SI.
- ✓ Gestión de activos
- ✓ Seguridad de los recursos humanos
- ✓ Seguridad física y ambiental
- ✓ Gestión de comunicaciones y operaciones
- ✓ Control de accesos.
- ✓ Sistemas de información, adquisición, desarrollo y mantenimiento.
- ✓ Gestión de incidentes de SI.
- ✓ Gestión de continuidad del negocio.

De acuerdo con las descripciones planteadas por **ISO 27001** e **ISO 27002**, se relacionan las diferentes **Políticas de Seguridad** que serán instrumento de uso de control de interno de la organización para el buen manejo de la información y de activos informáticos. Evidencias que serán recolectadas en base al estudio previo realizado, y plasmado dentro cada política de seguridad. Estas serán desarrolladas y aplicadas a la Alcaldía Municipal de Montecristo.

- ✓ Políticas de SI.
- ✓ Organización de SI.

[22] OSTEG, Blog. ISO 27002, Buenas prácticas para Gestión de la SI [online]. Blogs OSTEG [Investigado: 20 de mayo de 2019]. Publicado en Internet: [http://cort.as/-RabN]

- ✓ Políticas de control de acceso.
- ✓ Políticas de intercambio de información.
- ✓ Políticas de escritorio limpio y pantalla despejada.
- ✓ Políticas de respaldo de información.
- ✓ Controles criptográficos.
- ✓ Estudios de activos de información.
- ✓ Estudios de eventos e incidentes.
- ✓ Política de seguridad informática y ciberseguridad.
- ✓ Relaciones con tercero.
- ✓ Inventario y clasificación de activos de información.
- ✓ Análisis y gestión de riesgo.
- ✓ Política de Herdening – Endurecimiento de equipos de infraestructura.
- ✓ Control de cambios.

5.4 MARCO TEORICO.

Desde hace muchos años las empresas hacen un esfuerzo continuo por dotarse de sistemas informáticos que permitan proteger la información con la idea de dar un mejor y mayor servicio a sus clientes y hacer más eficaz la gestión y el trabajo dentro de sus organismos[23].

El uso acelerado del internet ha permitido que las empresas adopten controles que ayuden a proteger sus activos de información, debido a la cantidad de ataques informáticos que existen, es por esta razón que la información debe ser protegida en cualquier estado mientras se almacene, procese o transmita, implementando las medidas, de acuerdo con el impacto que se pueda generar por la divulgación o modificación no autorizada de la misma.

Por lo anterior, se deberá implementar el Gobierno de SI, en la alcaldía municipal de Montecristo, que permita proteger la información propia, ante una serie de riesgos que atenten contra estos principios.

[23] LOPEZ, Agustín. Portal de ISO 27001, SGSI [Consultado: 28 de enero de 2019]. Publicado en Internet: SGSI, [http://cort.as/-Rae7]

5.4.1 ¿Qué es un SGSI?

Concepto del inglés, information Security Management System[24], Sistema de Gestión de SI. Desarrollo de políticas y procedimientos que se realizan al interior de una organización para proteger los pilares de la SI.

> ***5.4.1.1 Información:*** Conjunto de datos propios de una entidad que tienen valor para la misma, es decir, son todos los activos de información que son utilizado a nivel interno de cualquier organización ya sea papel, o almacenada electrónicamente.

Según la ISO 27001, la SI consiste en conservar los pilares fundamentales. Aquí se Se detallan los tres conceptos.

- ✓ **Confidencialidad:** Garantiza el acceso solo para personal autorizado.
- ✓ **Integridad:** Evita modificaciones no autorizadas.
- ✓ **Disponibilidad:** Garantiza que la información esté apta cuando se necesite.

5.4.2 ¿Para qué sirve un SGSI?

La implementación de un SGSI permite mejorar los procedimientos internos de una organización, con el fin de salvaguardar los principios de seguridad, en cualquiera de sus estados, alineado a la misión, visión y objetivos de la entidad.

5.4.3 ¿Qué Incluye un SGSI?

Se ha mostrado mediante una gráfica la documentación del SGSI, mediante pirámide que tiene 4 niveles[25], en el que se puede evidenciar de la siguiente forma de acuerdo la norma ISO 27001.

Figura 1. Pirámide SGSI

[24] http://cort.as/-RaeL
[25] INTECO - CERT. (s.f.). Centro de Respuesta a incidentes de Seguridad TIC. Recuperado el 22 de junio de 2012, de Conceptos básicos de SGSI: [http://cort.as/-Rael].

Fuente: www.iso27000.es

5.4.4 Alcance del SGSI:

El Gobierno de SI, aplica a todo el negocio, incluye a cada una de las dependencias que hacen parte de ella, a todo el funcionario que tiene relación directa o indirecta con la organización. El diseño de políticas debe ser organizado y aplicado a todo sector productivo, (divisiones, áreas, procesos, sistemas, funcionarios), hacerse llegar por intermedio del personal encargado en el área, mediante capacitaciones y otras técnicas utilizadas para que se implemente de forma adecuada este buen gobierno de seguridad.[26]

5.4.5 ¿Cómo Implementar un SGSI?

Para la implantación de cualquier SGSI, en referencia de la ISO 27001[27], debe realizarse mediante el ciclo **PHVA** (Planear, Hacer, Verificar, actuar), sería la forma como se debe realizar cada proceso de acuerdo a los procedimientos que se explica en cada parte del ciclo.

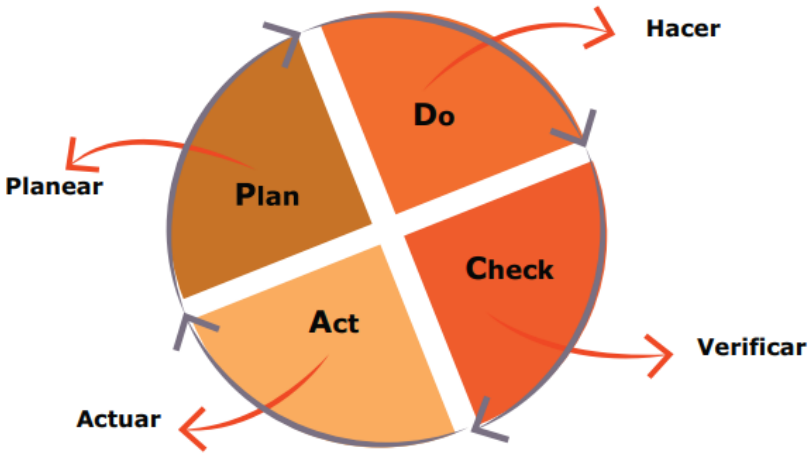
Este ciclo continuo, ayuda a conocer los peligros que está sometida la información, determinar que se debe hacer, y como se debe actuar de una manera correcta para preservar de forma clara la disponibilidad, la confidencialidad e integridad de los

[26] Gestión de Riesgo en SI: El método que se puede aplicar en diferentes contextos, [Consultado 20 de mayo de 2019]. encontrado en Internet: [http://cort.as/-Raf4].
[27] Alberto G. Alexander. (2007). Diseño de SGSI (1ra edición). Bogotá, Colombia: Editorial Alfa omega.

activos de una organización.

Aquí se describen las fases del buen diseño de un SGSI basado en el ciclo antes mencionado.

Figura 2. Fases implementación de un SGSI



Fuente: SGSI-Sena

5.4.5.1 Plan (planificar): establecer el SGSI.

En esta fase se establece la parte inicial del sistema de gestión, aquí se evalúa y se mide el estado en el que se encuentra la información y cada uno de los activos. Realizar una indagación de cuales son los procediemientos que se encuentran en alta criticidad de amenaza, para posteriormente realizar una planificación con todos los procesos para establecer el SGSI.

Algunas de las actividades que se deben realizar en esta etapa son:

- ✓ **Inicio del proyecto:** En este se realiza la respectiva investigación, se extrae la informacion necesaria para realizar un sistema de gestión. se identifican los activos que hacen parte del negocio mediante tecnicas de recolección de datos, y se evalúan los riesgos que en la acrtualidad existen en la organización.
- ✓ **Definición del SGSI:** Se establece el alcance y los procedimientos que se harán para que el Sistema de Gestión de Seguridad quede realizado

totalmente.

- ✓ **Análisis de riesgo:** Se identifica por intermedio de una matriz o cualquier metodología, adoptada para clasificar los riesgos y para realizar inventario de los activos informaticos que deben ser protegidos.
- ✓ **Gestión de riesgo:** Se escogen los controles adecuados y se hace el debido tratamiento de los riesgos, para posteriormente realizar el plan de gestión y el debido tratamiento.

5.4.5.2 Do (hacer): implementar el SGSI.

En esta parte se realiza detalladamente la manera como se va a tratar el riesgo, se ejecutan acciones para implementar los controles de seguridad tanto físicos como lógicos que fueron seleccionados anteriormente.

Las tareas que se realizan en esta etapa son:

- **Formación y sensibilización:** se capacita al personal sobre los controles que serán implantados en la organización.
- **Implantación del SGSI:** Se ejecutan los controles, políticas y los procedimientos que están contemplados en el Sistema de Gestión.

5.4.5.3 Check (verificar): Monitorizar y revisar el SGSI.

Las métricas e indicadores que han sido dispuestos en cada uno de los activos, se mide la eficacia de los controles, con el fin de verificar que el SGSI funcione correctamente.

Las principales tareas que este realiza son:

- ✓ **Monitorización del SGSI:** Se Monitorea las funciones del sistema, para encontrar fallas, errores de procesos y fallos de seguridad para que sean corregidos inmediatamente.
- ✓ **Revisión del SGSI**: Se debe realizar periódicamente la política, en caso de efectuarse modificaciones, registrarlos a través del control de cambios con autorización de la alta dirección.

5.4.5.4 Act (actuar): Mantener y mejorar el SGSI.

Se realizan las acciones de mantenimiento que sean pertinentes para el correcto funcionamiento del SGSI, las cuales se pueden contemplar desde la mejora de un proceso hasta la corrección de algún punto débil detectado en el sistema.

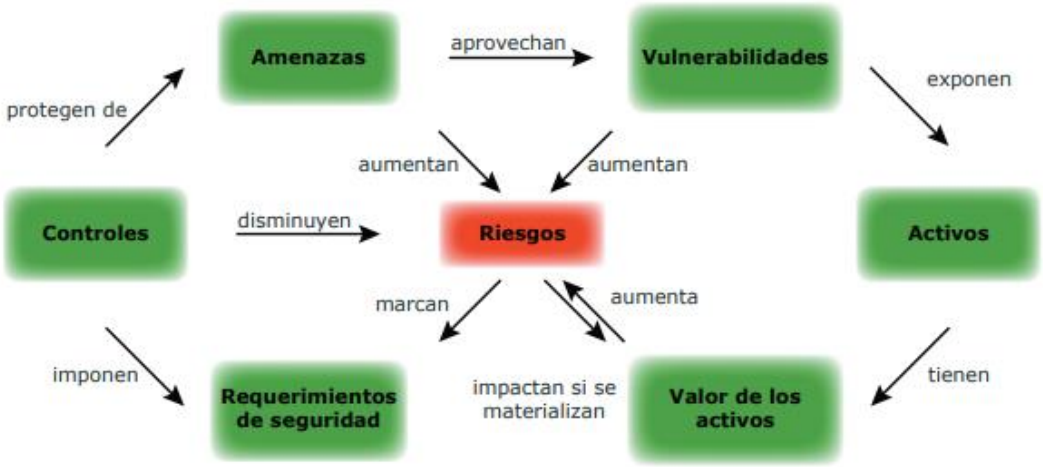
Las principales tareas que aquí se realiza son:

- ✓ **Mantenimiento del SGSI:** Se ajustan las mejoras del Gobierno de seguridad, mediante actualizaciones, agregando otras acciones preventivas y correctivas que puedan agregar al diseño de políticas.
- ✓ **Mejora continua:** Se mantiene el rendimiento del sistema y se continúa con las mejoras identificadas en procesos anteriores del SGSI.

5.4.6 Procedimiento para análisis del riesgo

La siguiente grafica proporciona una visión general de los elementos que deben ser tenidos en cuenta durante el procedimiento de análisis de gestión del riesgo:

Figura 3. Procedimiento análisis de riesgo.



Fuente: SGSI-Sena

5.4.7 ¿Qué tareas tiene la gerencia de un SGSI?

Un componente fundamental en una organización es la implementación exitosa de un SGSI, la no utilización de esta puede afectar la operación de toda empresa. La gerencia tiene la principal responsabilidad de velar que se cumpla todo el sistema de Gestión, desde el diseño de políticas, procedimientos, manuales hasta las buenas prácticas de SI, dentro de la organización. Este activo es el principal responsable de cualquier evento de seguridad o incidente de la compañía, y está en capacidad de gestionar y controlar cualquier tipo de eventos que se presente, requiere tomar de decisiones y acciones sobre la hardenización de la infraestructura tecnológica.

6 MARCO CONTEXTUAL.

La alcaldía Municipal de Montecristo Bolívar cuenta con múltiples dependencias entre las que se encuentran secretarias como la de planeación, tesorería, Comisaria de Familia, Archivos, Control interno, secretaria de gobierno, despacho del alcalde, Unidad de víctimas[28], más familias en acción, y secretaria de salud[29].

Las dependencias precitadas manejan gran cantidad de activos de información a través de equipos interconectados a una misma red, de acuerdo con visita técnica cada una de estas dependencias está en constante peligro al robo de la información, ya que su infraestructura tecnológica no cuenta con los elementos de control para el adecuado amparo de la información. Para el desarrollo de toda esta problemática se tiene estimado realizar el proyecto en un periodo aproximado de seis meses, y se abordará en todas las dependencias que hacen parte de la alcaldía.

[28] UNIDAD PARA LAS VICTIMAS [online]. [Consultado: 20 de mayo de 2019]. encontrado en Internet: [http://cort.as/-RafU]

[29] PROGRAMA MAS FAMILIAS EN ACCION, iniciativa del estado colombiano que brinda ayudas de nutrición a las familias con niños menores de 7 años.

7 DISEÑO METODOLÓGICO.

7.1 LÍNEA Y TIPO DE INVESTIGACIÓN.

La base de esta investigación está relacionada a la infraestructura tecnológica, rama fundamental del campo de la informática, implementando un SGSI, conforme en la norma técnica Colombiana **ISO 27001**, sobre una entidad del sector estatal como es la Alcaldía Municipal de Montecristo, ubicada al sur del departamento de bolívar.
Este proyecto está definido como una investigación descriptiva, debido a que se realizaran procedimientos y actividades de seguridad que vinculan a toda la infraestructura tecnológica de una organización

La investigación representa un gran dominio ajustado a las TI, y se realizará investigación completa sobre otras metodologías existentes que permita evaluar y medir los riesgos, metodología (**MAGERIT)** y sirvan como complemento al completo desarrollo de esta propuesta tecnológica.

Se planea en una primera parte, contactar la ayuda de una empresa especializada, que esté certificada en ISO 27001, que brinde asesoramiento durante todo el proceso. A partir de ahí empezar con la metodología **PHVA** (Planificación, Ejecución, Seguimiento, Mejora)[30], ya que esta es la base para implementar cualquier buen gobierno de SI, y lo que busca es establecer controles necesarios en la seguridad de en las organizaciones, y como la idea es llevarlo a la alcaldía municipal se tratará desarrollar de acuerdo con cada una de sus fases.

Durante la **fase de planificación,** realizar el estudio del estado en que se observan los activos de la alcaldía municipal. Medir las vulnerabilidades y así calcular las medidas que se van a tomar. Con todos estos análisis y datos recolectados se deberán establecer los debidos controles, que permitan minimizar todos esos riesgos.

Para la **fase de Ejecución,** desarrollar los controles necesarios mencionados anteriormente.

[30] INTECO - CERT. (s.f.). Centro de Respuesta a incidentes de Seguridad TIC. investigado el 22 de junio de 2012, de Conceptos básicos de SGSI: [http://cort.as/-Rael]

En la **fase de seguimiento,** medir la eficiencia y éxito de los controles utilizados, que han permitido reducir los riesgos de SI, a nivel interno de la entidad y, por último, **la fase de mejora,** ejecutar las labores que permitan optimizar el **Gobierno de SI**.

Para el desarrollo y diseño del gobierno de SI, hay que seguir todos los pasos adecuados descritos en las guías de desarrollo, con el objetivo de que todos los procesos seguros que se deben realizar estén descritos en todas las **políticas, guías, manuales, procedimientos** y **formatos.** Con esto se permitiría la creación de un sistema de muy buena calidad para la alcaldía municipal.

7.2 METODOLOGÍA DE DESARROLLO.

El Desarrollo de este trabajo se encuentra especificado bajo una serie de etapas que comprenden un conjunto de procesos encaminados al desarrollo de los objetivos.

7.2.1 Etapa 1: Realizar un informe que permita hacer un análisis de los riesgos que están presentes en la infraestructura tecnológica de la alcaldía municipal.

7.2.1.1 Actividades:

- ✓ Verificar los servicios del negocio, con el fin de conocer los activos informáticos que tiene la organización.
- ✓ Solicitar una revisión de las máquinas de cómputo y hojas de vida de estos.
- ✓ Indagar información con funcionarios encargados de cada dependencia para evaluar y medir los activos de información que están a cargo del área.

7.2.2 Etapa 2: Definir los parámetros y políticas que ayuden a reducir los peligros presentes en el departamento de informática de la organización.

7.2.2.1 Actividades:

- ✓ Valorar los activos mediante los principios de SI.
- ✓ Determinar y medir cuales son los peligros y las vulnerabilidades que están expuestos los activos informáticos.

- ✓ Calcular la consecuencia y el riesgo de los activos, si se logra materializar una amenaza. Después de analizados estos aspectos se puede definir los parámetros y políticas, manuales y procedimientos de seguridad.

7.2.3 Etapa 3: Proponer la implementación de procesos de control que pretendan minimizar y mitigar los tipos de ataques que existan en la actualidad.

7.2.3.1 Actividades:

- Verificar cuales son los controles que existen y que están situados a nivel interno de la entidad municipal.
- Inspeccionar la infraestructura tecnológica de la Alcaldía Municipal.
- Implementar técnicas por intermedio de sistemas que permitan controlar ataques realizados a nivel externo.

7.2.4 Etapa 4: Plantear un sistema gestión de información para toda la organización que busque conservar los pilares de SI.

7.2.4.1 Actividades:

- ✓ Realizar entrevistas con el personal de la alcaldía municipal, con el objetivo de establecer controles que no hayan sido relacionados.

7.2.5 Etapa 5: Diseñar el sistema y aplicarlo a toda la infraestructura tecnológica, que ayude a velar la protección y conservación de los activos informáticos más valioso que tiene la entidad.

7.2.5.1 Actividades:

- ✓ Definir el objetivo del diseño de políticas para la gestión de la información de la Alcaldía Municipal de Montecristo.
- ✓ Definir el alcance del Gobierno de SI.
- ✓ Definir las Políticas, Manuales y Procedimientos relacionados al gobierno de SI, de la entidad municipal.

8 ANÁLISIS Y GESTIÓN DE RIESGOS

8.1 INFORME PARA EL LEVANTAMIENTO DE INFORMACIÓN Y ANÁLISIS DE RIESGOS.

A continuación, se presenta un informe detallado de cómo se encuentran los activos informáticos de la alcaldía municipal, el estado en que se encuentran los equipos y su posterior evaluación.

La Alcaldía Municipal por intermedio del área de SI, deberá realizar los análisis de los peligros necesarios en materia de Hardware, Software y Servicios, encaminados a garantizar la SI, basados en estándares internacionales como la metodología (**Magerit**, **ISO 27005**, **NIST 800-30**) orientándolos a un modelo encaminado a mitigar los riesgos con la implementación de los respectivos controles. Por todo lo investigado, se realizará un pequeño informe del estado en que se encuentra la entidad municipal y se hará un levantamiento detallado de la información con que esta cuenta, para más adelante medir y evaluar los riesgos y las medidas de salvaguardas que se puedan implementar para disminuir la probabilidad de las amenazas sean materializadas.

A continuación, se presenta un informe de cómo se encuentra la alcaldía Municipal.

8.1.1 Situación actual de la entidad:

En primera instancia, se realizó una visita a cada una de las oficinas de la alcaldía, e identificándose la infraestructura TI, los servicios, aplicaciones y políticas con las que esta cuenta. Hay que destacar que en la alcaldía no se encontraron procedimientos documentados.

8.1.2 Infraestructura:

La entidad municipal cuenta con infraestructura informática, en esta se encuentra:

> ***8.1.2.1 Data center:*** La alcaldía cuenta con un data center, en el que se encuentra el servidor de la entidad. Estos equipos se encuentran ordenados en un soporte metálico (**RACKS**), que ayuda a protegerlos. Se encuentra ubicado en la segunda planta de la edificación donde se distribuye el cableado que comunica a todas las oficinas. Esta área se encuentra restringida y se encuentra bajo llave, y solo tiene acceso el personal

autorizado. Dentro de esta área se debe implementar y administrar el software y hardware necesario para proteger la seguridad informática del negocio, previniendo ataques de denegación de servicios, inyección de código, interceptación de comunicaciones, intrusiones y cualquier otra modalidad empleada por los hackers.

8.1.2.2 Cableado estructurado: Es la que mantiene interconectada todas las oficinas, esta permite trabajar con aplicaciones que requieran de acceso a bases de datos.

8.1.2.3 Dispositivos de respaldo: Se cuentan con dispositivos de almacenamientos externos (Disco Duros).

8.1.3 Estaciones de trabajo: son los equipos informáticos que se encuentran en las diferentes dependencias de la organización y que son utilizados por los usuarios finales. Estos equipos son entregados a una persona de la cual se hace responsable por el buen uso que se le dé. Las oficinas que cuentan con estaciones de trabajo son:

- ✓ Unidad para la atención y reparación a las Víctimas.
- ✓ Oficina de Mas Familias en Acción.
- ✓ Oficina del Sisben.
- ✓ Secretaria de Salud Municipal.
- ✓ Secretaría de Planeación.
- ✓ Comisaría de Familia.
- ✓ Tesorería Municipal.

8.1.4 Servicios: Se describen los diferentes servicios utilizados por los funcionarios de la entidad, resaltando que el responsable de los servicios mencionados es el departamento de TI.

8.1.4.1 Internet: Permite la navegación de los funcionarios a los portales web. Para el control de acceso a los sitios web se utiliza servicio proxy – firewall donde se Configura para permitir o denegar accesos a sitios.

8.1.4.2 Correo electrónico: permite a los funcionarios de la entidad tener su propio correo corporativo, aquí cada funcionario puede enviar o recibir mensajes que estén acordes a las actividades realizadas en sus funciones.

8.1.4.3 BD: Se cuentan con sistemas de bases de datos (DBMS) de los diferentes programas sociales que ofrece el estado.

8.1.4.4 Aplicaciones: Los programas informáticos diseñados para realizar trabajos específicos dentro de una dependencia. Se brinda soporte cada vez que lo sea necesario.

Seguidamente, se presenta una relación de cómo se clasifican los activos según **MAGERIT**.

8.2 IDENTIFICACIÓN Y CLASIFICACIÓN DE ACTIVOS DE INFORMACIÓN.

La Metodología **MAGERIT**, clasifica los activos de forma jerárquica para una sistematización precisa. A continuación, se define y se clasifican los tipos de activos existentes en una organización y cada descripción al que hace alusión cada activo perteneciente a la Alcaldía Municipal.

Tabla 1. Activos de información según la metodología **MAGERIT.**

IDENTIFICACIÓN	TIPO DE ACTIVO	DESCRIPCION
[D]	**Datos/Información.**	Principal activo de cualquier organización, a través de estos se generan resultados de cualquier consulta de información.
[K]	**Claves Criptográficas.**	Procedimientos realizados para la protección en el envío de datos, el cifrado de información que se envía por los diferentes canales de comunicación.
[S]	**Servicios.**	Actividades que se brindan a los usuarios a nivel de servicios a través de los sistemas.
[**SW**]	**Software.**	Aplicativos ejecutados en los ordenadores para generar información a través de los datos.

[HW]	**Equipamiento.**	Equipos que prestan servicios en la alcaldía municipal.
[COM]	**Redes de Comunicación.**	Medios de comunicación propios destinados a transmitir información.
[Media]	**Soportes de información.**	Medios de almacenamiento que almacenan información de forma permanente o provisional.
[AUX]	**Equipamiento auxiliar.**	Equipamientos informáticos de respaldo.
[L]	**Instalaciones.**	Infraestructura municipal donde se encuentran los activos de la organización.
[P]	**Personal.**	Funcionarios que tienen relación contractual con la alcaldía Municipal de Montecristo.

Fuente: El Autor.

De acuerdo a los resultados de la revisión hecha a la infraestructura tecnológica de la alcaldía y los elementos que la conforman, se identifican los activos de información con los que cuenta la alcaldía Municipal de Montecristo, no obstante que esta infraestructura no cuenta con equipos informáticos robustos pertenecientes al área de infraestructura, carece de instalaciones para resguardar los servidores, esta desprovista de equipos de protección de tráficos de datos, como **WAF**, **NAC**, **Endpoints**, **Active Directory**, **Switches**, y otros elementos que son propios de una infraestructura tecnológica. A continuación, se describen los activos informáticos disponibles en la Alcaldía Municipal de Montecristo.

8.3 IDENTIFICACIÓN DE ACTIVOS INFORMÁTICOS:

Tabla 2. Identificación de activos informáticos.

TIPO DE ACTIVOS	NOMBRE	CARACTERISTICAS
Comunicaciones [COM]	**Enrutador Routerboard Mikrotik.**	10 puertos Gigabit Jaula SFP 1 puerto USB 3.0 Cantidad: **2**
	Routerboard Mikrotik	Puerto USB 2.0 Puerto SFP para agregar conectividad de fibra óptica. Cantidad: 1
	Router Inalámbrico AirRouter.	Funcionamiento de red-Router, y Bridge • Funcionamiento inalámbrico: Estación WDS, Access Point y Access Point WDS. Cantidad: 1
	Rompemuros 3bumen	• El Repetidor de Señal Wifi • Cuenta con 3 antenas de 5dB. • Con sus antenas puede alcanzar velocidades de transmisión de hasta 300Mbps • Permite la ubicación de la estación inalámbrica en lugares estratégicos
Hardware [HW]	**Impresoras/Scanner EPSON**	Se cuentan con 9 impresoras multifuncional EPSON, distribuidos en las diferentes dependencias.
	Equipos de Cómputo.	38 equipos informáticos de escritorio, referencias HP, 1TB de almacenamiento, Procesador i3, Séptima generación, 8 Memoria RAM, Ddr3.
	Equipos De cómputo, Portátiles.	5 portátiles HP, 1TB de almacenamiento, Procesador i3, Séptima Generación, 8 memoria Ram.
	UPS de 3Kva	Funciona como respaldo de energía, para mantener equipos funcionales, en caso de fluctuación eléctrica.
	Sistemas Operativos.	Windows 10. Windows 7.

Software. [SW]	**Paquete de Microsoft Office.**	Herramienta Ofimática, 2010 y 2013.
	Correos Electrónicos	Cuentas de correos electrónicos corporativos. Asociados a Gmail.
	Arsoft.	Software perteneciente a la Secretaría de Salud Municipal.
	SisbenApp.	Software perteneciente a la oficina municipal del Sisben.
	Software Vivanto.	Software Perteneciente a la Oficina de Víctimas.
Información Física. [Media]	**Documentos**	Activo de mayor valor perteneciente a todos los procesos que presta la alcaldía Municipal de Montecristo.
Información Digital [ID]	**Activos de información Digital.**	Respaldo de datos, almacenado en cada disco interno de cada máquina, Se almacenan los documentos, archivos y toda la información propia de cada dependencia de la Alcaldía Municipal.
Personal [P]	**Funcionarios**	La Alcaldía Municipal cuenta con un total de 30 funcionarios nombrados directamente por la alcaldía, y 22 funcionarios contratados por prestación de Servicios.
	Usuarios.	Personal a los que se les brinda atención de los diferentes programas.
	DBA	Administradores que brindan soporte de los diferentes sistemas de información.

Fuente: El Autor.

8.4 VULNERABILIDADES, AMENAZAS Y RIESGOS DE SEGURIDAD DEL ÁREA INFORMÁTICA O DEPARTAMENTO DE SISTEMAS EN CADA UNO DE LOS ACTIVOS INFORMÁTICOS.

8.4.1 Análisis de los riesgos presentes en la infraestructura tecnológica.

Tratando sobre la metodología **MAGERIT**, podemos hacer un estudio **acerca de** los sistemas de información y los activos que posee la alcaldía municipal.

Como procedimiento fundamental al análisis de riesgo, es que se debe organizar la metodología para el estudio los activos expuestos, a través de la identificación de las vulnerabilidades, amenazas y controles que tengan los activos de información pertenecientes a la alcaldía municipal, y puedan priorizar la mitigación de cada uno de estos a través de la gestión de los riesgos residuales y la implementación de nuevos controles.

Para la ejecución del estudio de riesgos sobre un activo y/o grupo de activos determinado debe primero obtenerse una valoración aplicando el Procedimiento de Clasificación de Activos de Información.

La siguiente será una directriz general para el estudio de riesgos, La identificación del riesgo debe realizarse por cada propiedad de seguridad del activo y/o grupo de activos de información en análisis, por lo que siempre se evaluaran los siguientes riesgos:

- ✓ **Perdida de confidencialidad del activo.**
- ✓ **Perdida de integridad del activo.**
- ✓ **Perdida de disponibilidad del activo.**

Para el estudio de riesgo cada negocio dentro de su política de SI, puede establecer su propia metodología de análisis, valoración y evaluación del riesgo tomando como referencia lo establecido en el presente proyecto.

La identificación del riesgo deberá realizarse por cada propiedad de seguridad del activo y/o grupo de activos de información en análisis, por lo que siempre se evaluaran los peligros en base a la perdida de los pilares de seguridad.

Se debe tener en cuenta que muchas son las causas que originan afectaciones a nivel interno. Se pueden especificar esos riesgos como se definen en la siguiente tabla.

***Tabla 3**. Análisis de los riesgos presentes.*

RIESGOS	CAUSAS
Fallos no intencionados	• Errores de los usuarios. • Ataques de DDoS, DOS. • Difusión de malware. • Backdoor (Puertas traseras) • Brechas de Seguridad. • Pérdida de equipos.
Ataques deliberados o intencionados	• Manipulación de los ficheros de configuración. • Spoofing. • Injections SQL. • Denegación de servicio • Robo de equipos • Indisponibilidad del funcionario. • Ataque destructivo.
De origen industrial	• Fuego. • Daños por agua. • Desastres naturales. • Contaminación medio ambiente. • Corte de suministro eléctrico.
Desastres Naturales.	• Terremotos. • Temblores. • Desastres naturales.

Fuente: El Autor.

También se pueden presentar vulnerabilidades existentes que afectan el rendimiento de una empresa, como lo son:

- Existencia de materiales inflamables.
- El cableado estructurado inapropiado
- Poco conocimiento del funcionario en SI.
- Falta de procedimientos de control sobre el manejo de internet
- Falta de Políticas sobre la protección de equipos.

- Carencia de políticas en la instalación de software seguro.

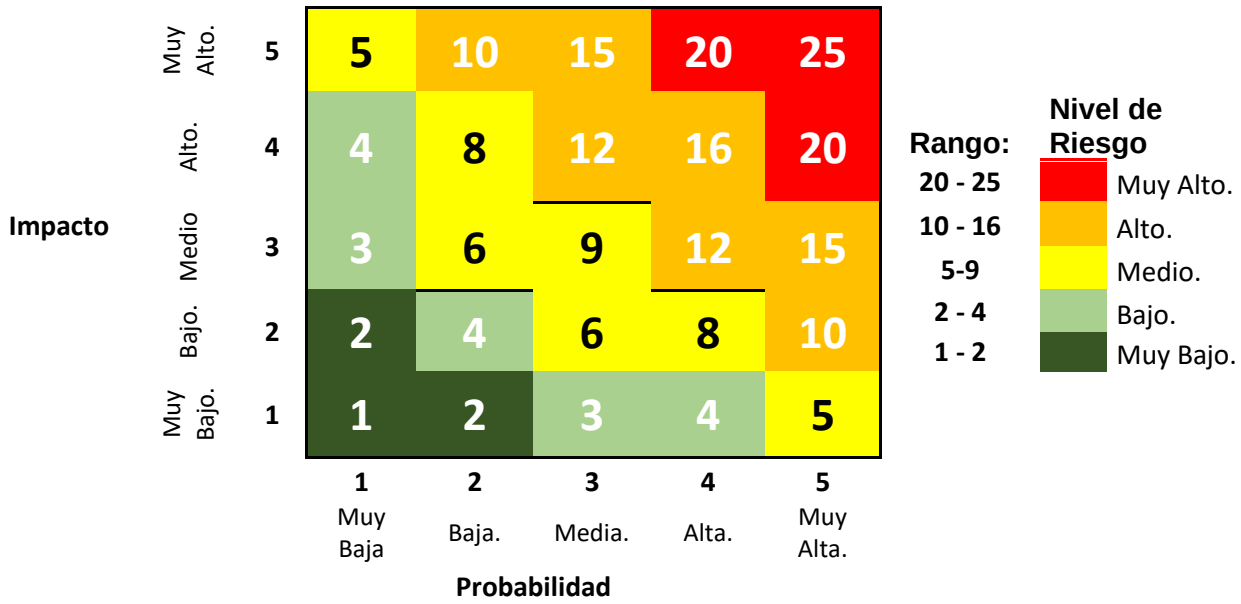
Para poder obtener una valoración adecuada se debe tener en cuenta que:

Riesgo = **Probabilidad** x **Impacto.**

Por lo que se debe contar con la valoración del activo y/o grupo de activos (Muy alto, Alto, Medio, Bajo y Muy Bajo), correspondiente a las características de SI, (Integridad, Confidencialidad y Disponibilidad) y evaluar la probabilidad de materialización de cada riesgo teniendo en cuenta los siguientes parámetros:

- **Muy Alto:** Ocurre en promedio varias veces a la semana.
- **Alto:** Ocurre en Promedio una vez a la semana.
- **Medio:** Ocurre en Promedio una vez al mes.
- **Bajo:** Ocurre en Promedio una vez al año.
- **Muy Bajo:** Ocurre en Promedio una vez cada cinco años.

Finalmente, para obtener el nivel de riesgo se deberá asignar un valor numérico a la probabilidad y al impacto correspondiente a su nivel donde 1 es muy bajo y 5 muy alto. La clasificación del riesgo se dará de acuerdo con la siguiente matriz.



Fuente: el Autor.

8.4.2 Criterios De Valoración.

Tabla 4. Criterios de valoración.

Disponibilidad	Alguna de las informaciones siempre se encuentre disponible 24X7.
Integridad de los Datos.	Solo permite modificar información con la autorización del administrador de la BDA.
Confidencialidad de los Datos.	Permitido solo ingreso a los encargados de la dependencia.
Autenticidad.	Permitido con ingreso al sistema con los usuarios y contraseñas establecidas.

Fuente: El Autor.

8.4.3 Amenazas:

Tabla 5. Criterios de valoración

FUEGO: Equipos informativos	Disponibilidad	Probabilidad que el fuego afecte los recursos del sistema
Soportes de información	Disponibilidad	
Instalaciones	Disponibilidad	
DAÑOS POR AGUA: Equipos informativos	Disponibilidad	Riesgos ocasionados por el agua.
Soportes de información	Disponibilidad	
Instalaciones	Disponibilidad	
DESASTRES NATURALES: Equipos informativos	Disponibilidad	• Rayos. • Tormentas. • Terremotos. • Inundación. • Deslizamiento.
Soportes de información	Disponibilidad	
Instalaciones	Disponibilidad	
MANIPULACION DE LOS EQUIPOS: Equipos informativos	Confidencialidad.	Alteraciones en los programas en busca de beneficios particulares.
Soportes de información	Disponibilidad	
Instalaciones		
INGENIERIA SOCIAL: Personal interno.	Confidencialidad. Disponibilidad Integridad.	Práctica de engaño para que funcionarios cedan información confidencial.

Fuente: El Autor.

8.4.4 Valoración De Salvaguardas

Las salvaguardas se crean como mecanismo o procesos que permiten garantizar la disminución del riesgo.

MAGERIT permite definir las diferentes maneras de salvaguardas los activos de información:

Tabla 6. Libro 1- método Magerit.

ACTIVIDAD	TIPO
Preventivas: Reducen la probabilidad de ocurrencia.	[PR] Preventivas
	[DR] Disuasorias
	[EL] Eliminatorias
Reducen la degradación.	[IM] Minimizadoras
	[CR] Correctivas.
	[RC] Recuperativas.
Consolidan el efecto de las demás.	[MN] Monitorización
	[DC] Detección.

Fuente: El Autor.

Mirando el catálogo de salvaguardas y de acuerdo la metodología, se identifica cuáles son los procesos utilizados en la entidad, para resguardar los activos frente a las diferentes amenazas que existen.

Se relaciona en una tabla, la identificación de salvaguardas y el grado en que estas pueden estar aseguradas.

Tabla 7. Identificación de salvaguardas

SALVAGUARDAS	TIPO	EVALUACIÓN
Protecciones	**Identificación y autenticación**	**70%**
	Controles de acceso	**40%**
	Herramientas de detección/prevención de intrusos	**10%**
	Herramientas monitorización de tráfico	**10%**
Protección de la información.	**Copias de seguridad (backups)**	**80%**
	Cifrado de datos	**20%**

Protección de los servicios.	**Perfiles de seguridad.**	**60%**
	Protección en aplicaciones web.	**30%**
Protecciones de las aplicaciones (software)	**Copias de seguridad.**	**80%**
	Actualizaciones y Mantenimientos.	**60%**
Protección de los equipos. (Hardware)	**Se aplican perfiles de SI.**	**70%**
Protección de las comunicaciones	**Uso de internet.**	60%
	Seguridad Wireless	40%
Seguridad física – Seguridad en las instalaciones.	**Control de los accesos físicos.**	50%

Fuente: El Autor

De acuerdo con la siguiente Tabla también se valoran los activos de la alcaldía municipal teniendo en cuenta los pilares de SI.

Tabla 8. Valoración activos de la alcaldía.

Confidencialidad, Disponibilidad, Integridad.	Clasificación
1	**Bajo.**
2	**Medio.**
3	**Critico.**
4	**Catastrófico.**
5	**Evento.**

Fuente: Tomado del módulo de SGSI.

Tabla 9. Niveles de Criticidad.

Nivel Criticidad	Descripción.
Bajo	Sistemas que afectan a cualquier sistema de información o área de trabajo, ejemplo: ✓ Estaciones de trabajo donde los funcionarios no manejan tareas criticas
Medio	Sistemas que apoyan a una sola dependencia o proceso de la entidad y no afecta los servicios de la compañía:

	✓ Es de carácter informativo al Grupo de Respuesta de Incidentes -GRI. ✓ No se ve afectada la reputación. ✓ Afecta la productividad momentáneamente. ✓ No ocasiona multas ni sanciones
Crítico	Sistemas que apoyan a más de una dependencia o procesos de la Alcaldía, y afectan la operación de los procesos en un 50%, la afectan ocasionando: Baja Productividad. Multas o sanciones Reputación Amenaza a la vida (salud de usuarios o trabajadores)
Catastrófico	Sistemas que apoyan todas las dependencias o procesos de la entidad y afectan la productividad en un 100%. los procesos se ven interrumpidos totalmente, lo que le ocasiona a la alcaldía: ✓ Debe ser informado inmediatamente al encargado de SI. quién tomará decisiones para contener el incidente. ✓ Productividad paralizada. ✓ Multas o sanciones. ✓ Reputación
Evento	Ocurrencia identificada en el estado de un sistema, donde no se ve afectada la operación, no ocasiona multas ni sanciones, no existe perdida de reputación, no se involucra el riesgo a la ✓ Pérdida de vidas humanas. ✓ Un intento fallido de un Usuario para ingresar a una aplicación. ✓ Una notificación de cambio de contraseña de un usuario o un privilegio.

Tabla 9. Valoración confidencialidad.

- **Confidencialidad (C).**

Escala Cuantitativa	Escala Cualitativa	Descripción
1	**Muy Bajo.**	Puede ingresar cualquier Usuario
2	**Bajo.**	Solo ingresan Empleados o contratistas OPS
3	**Medio.**	Pueden acceder Administrativos
4	**Alto.**	Solo debe ingresar personal con credenciales asignadas.
5	**Muy Alto.**	Solo es posible el ingreso a personal operativo.

Fuente: El Autor.

Tabla 10. Valoración integridad.

- **Integridad**

Escala Cuantitativa	Escala Cualitativa	Descripción
1	**Muy Bajo.**	Algunas pueden ser modificadas en cualquier momento
2	**Bajo.**	Es posible modificarlo por cualquier Empleado o contratista OPS
3	**Medio.**	Lo pueden modificar cualquier funcionario
4	**Alto.**	Solo se puede modificar con autorización del alcalde Municipal
5	**Muy Alto.**	Solo es posible modificar con la autorización del administrador.

Fuente: El Autor.

Tabla 11. Valoración disponibilidad.

- **Disponibilidad (D)**

Escala cuantitativa	Escala Cualitativa	Descripción
1	**Muy Bajo.**	Los recursos están aptos por una semana y no perturba a la entidad.
2	**Bajo.**	Los recursos no están aptos hasta por 3 días y no perturba a la entidad.

3	Medio.	Los recursos no están aptos hasta por 1 día y no perturba a la entidad.
4	Alto.	Los recursos no están aptos hasta por 4 Horas.
5	Muy Alto.	Los recursos siempre deben estar disponibles.

Fuente: El Autor.

Cada activo de la información debe ser valorado de acuerdo con la Integridad, Confidencialidad y Disponibilidad.

Fórmula 1. Valor de los activos.

Se tiene que el: **Valor Activo = Confidencialidad + Integridad + Disponibilidad**

En base a esto se tiene una valoración acumulada de acuerdo con la siguiente Tabla:

Tabla 12. Valoración acumulada.

Clasificación Valor del Activo.	Rango Según Valor del Activo.
Muy Alto.	20 – 25
Alto.	10 – 16
Medio.	5 – 9
Bajo.	2 – 4
Muy Bajo.	1 – 2

Fuente: El Autor.

9 PROCEDIMIENTO ANÁLISIS Y GESTIÓN DE RIESGO:

9.1 IDENTIFICAR LOS ACTIVOS Y SU VALORACIÓN: Se debe tener en cuenta cuales son los activos de información involucrados en el análisis, con el fin de usar la valoración para identificar el impacto de que un riesgo logre ser materializado. En caso de que el activo no se encuentre valorado, realizar el procedimiento de clasificación de activos de información.

9.2 IDENTIFICAR EL CONTEXTO DE RIESGO: Es necesario tener identificada claramente las amenazas y vulnerabilidades que tiene cada activo, para luego realizar por cada activo, o grupo de activo el análisis de vulnerabilidades.

9.3 IDENTIFICAR CONTROLES EXISTENTES: Además de la identificación de vulnerabilidades y amenazas para cada activo de información, es necesario encontrar los controles de seguridad existentes que sean aplicables, con el objeto de obtener un panorama completo de los riesgos.

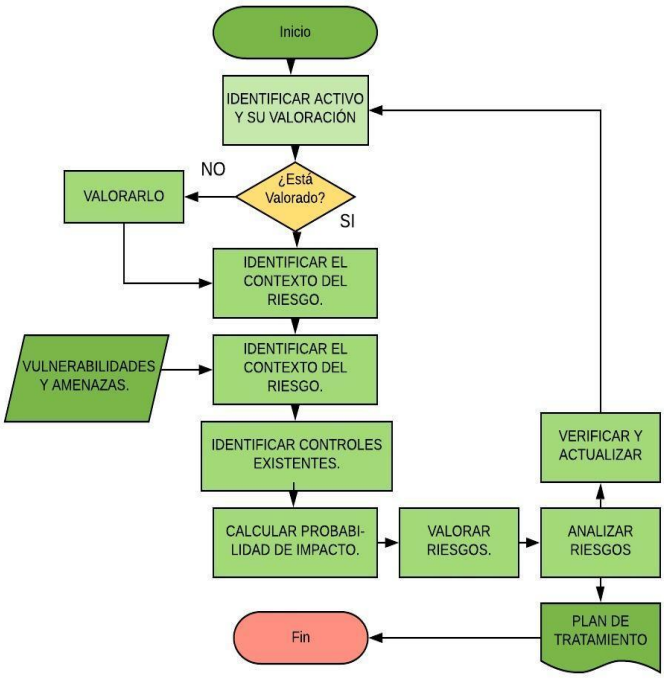
9.5 CALCULAR PROBABILIDAD E IMPACTO: Es necesario obtener el nivel de probabilidad u ocurrencia que causaría la materialización de un riesgo de seguridad (Confidencialidad, Integridad y Disponibilidad). Este valor puede ser obtenido de acuerdo con la valoración del activo por cada una de sus propiedades.

9.6 VALORACIÓN DE RIESGOS: Obtenida las probabilidades y el impacto por cada riesgo, se procede a calcular el riesgo puro (Riesgo sin control), como el riesgo residual (Riesgo con controles) de cada uno de los riesgos y por cada uno de los activos o grupo de activos. Al final se podrá obtener la calificación del riesgo entre **Muy alto** o **Muy Bajo.**

9.7 ANÁLISIS DE RIESGOS: Se estudian los riesgos residuales resultantes y se define el tratamiento que se les va a dar, es decir, mitigarlos, transferirlos, eliminarlos o aceptarlos.

9.8 VERIFICACIÓN Y ACTUALIZAR: Finalmente, una vez realizado el gobierno de SI, a la alcaldía Municipal de Montecristo, este debe actualizarse por lo menos una vez al año, o cuando las condiciones o el contexto de riesgo sean modificados significativamente.

Flujograma:



Fuente: El Autor.

10 PARÁMETROS Y POLÍTICAS DE SEGURIDAD PARA MINIMIZAR LOS RIESGOS.

10.1 SISTEMA DE CONTROL INTERNO INFORMÁTICO, DE ACUERDO CON LA NORMA ISO/IEC 27001:2013

Los componentes informáticos objeto de este estudio deben cumplir con las buenas prácticas establecidas y los estándares de seguridad informática, relacionada a la norma técnica colombiana NTC-ISO-IEC 27001, sobre los controles internos que se realizarán en la Alcaldía Municipal de Montecristo, se debe efectuar el buen gobierno de SI, de acuerdo a la ISO en mención, teniendo en cuenta que esta norma busca crear una estrategia sobre cómo tratar los aspectos de seguridad y la implementación de controles.

A partir de todo el análisis realizado, siempre se debe:

- Determinar lo que se quiere proteger.
- Identificar de que es necesario protegerse.

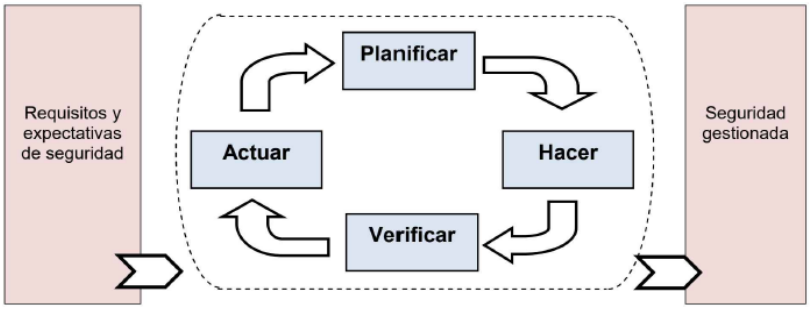
El modelo a implementar en el proceso de gestión de SI, desarrollado a la Alcaldía Municipal de Montecristo, sería el ciclo (Planificar, Hacer, Verificar, Actuar). A continuación, se describe las fases y conceptos del Modelo de sistema de control interno, definiendo cada proceso que se establece en la realización del Gobierno de Seguridad.

Figura 4. Sistema de control interno

Planificar (Establecer el SGSI)	Establecer las políticas, los objetivos, procesos y procedimientos de seguridad necesarios para gestionar el riesgo y mejorar la seguridad informática, con el fin de entregar resultados acordes con las políticas y objetivos globales de la organización.
Hacer (Implementar y operar el SGSI)	Tiene como objetivo fundamental garantizar una adecuada implementación de los controles seleccionados y la correcta aplicación de los mismos.
Verificar (Revisar y dar seguimiento al SGSI)	Evaluar y, en donde sea aplicable, verificar el desempeño de los procesos contra la política y los objetivos de seguridad y la experiencia práctica, y reportar los resultados a la dirección, para su revisión.
Actuar (Mantener y mejorar el SGSI)	Emprender acciones correctivas y preventivas basadas en los resultados de la verificación y la revisión por la dirección, para lograr la mejora continua del SGSI.

Fuente: www.iso27000.es

Figura 5. Requisitos y expectativas de seguridad



Fuente: www.iso27000.es

Aunque se ha analizado la situación actual en la que se encuentra la alcaldía Municipal de Montecristo en aspectos de seguridad, se ha desarrollado internamente investigación detallada de todos los activos de información, con la idea de estimar las medidas y controles que se van a implementar mediante la realización del Análisis de riesgo. Análisis que se encuentra detallado anteriormente en este apartado.

No hay que dejar excluido el plan de control interno informático, aunque no se dejado plasmado, es de suma importancia incluirlo. A continuación, se relaciona el plan de acuerdo con los tipos de activos existentes: **Información, software, Hardware, Servicios, Intangibles, Componentes de Red, Personas, Instalaciones.**

Tabla 13. Plan de control interno informático.

PLAN DE CONTROL INTERNO INFORMÁTICO		
RECURSOS	**ACTIVO A PROTEGER**	**PLAN DE CONTROL O MEDIDA DE SEGURIDAD.**
Información:	• **Documentos:**	• Existirán acuerdos de confidencialidad y tiempos de respuestas en los diferentes contratos que sostiene la entidad. • Debe existir un control periódico del grado de deterioro de la documentación existente.
Software:	• **Sistemas Operativos.** • **Microsoft office.** • **Bases de datos.** • **Vivanto – Victimas.** • **Arsoft – Salud.** • **SisbenApp – Sisben.**	• Se debe implementar manual de políticas de seguridad del contenido SMTP. • Se debe contar con actualizaciones periódicas sobre los diferentes tipos de software instalados en los equipos. • Crear estándares sobre mejores prácticas de seguridad sobre las distintas BD.
Hardware:	• **Servidores.** • **Computadores.** • **Portátiles.** • **Impresoras.** • **Escáneres.**	• Deberá existir controles de acceso a la información existente en los equipos corporativos. • Se deben realizar controles rigurosos sobre los equipos para que no se presenten fugas de información. • Se debe controlar y monitorear cada uno de los programas y sistemas instalados en los equipos.
	• **Switches.** • **Routers.**	• Debe haber políticas de seguridad manejo de equipos de red.

Componentes de Red:	• **Puntos de Acceso.**	• Estándares de mejores políticas de SI, para servidores. • Debe existir delimitación de responsabilidades referente a la SI, en contratos con proveedores, es decir que se limite a ciertos tipos de accesos. • Que existan mejores prácticas de seguridad para configuración de firewall.
Personas:	• **Funcionarios.** • **Usuarios.** • **Concejo Municipal.**	• Se debe contar con inventario de los accesos de los funcionarios a los diferentes portales existentes de la administración municipal. • Se debe revisar periódicamente los perfiles y accesos de usuarios por parte del coordinador de sistemas de la entidad pública. • Llevar a cabo capacitaciones a funcionarios sobre los riesgos existentes en la seguridad informática.
Instalaciones.:	• **Centro de Datos y Cableados.**	• Con el objetivo de reducir los peligros, la alcaldía municipal deberá buscar certificar sus centros de datos, el cual debe ser emitido por una empresa con las competencias para ello.

Fuente: El Autor.

Una vez realizadas todas las acciones de implantación del Gobierno de SI, en la alcaldía Municipal, se buscará que esta cuente con todos los Manuales, Procedimientos, Políticas, Instructivos que se piden en la ISO en referencia, para que se evidencie que la administración municipal cuenta con todos los procedimientos de seguridad estandarizados y que pueda a largo plazo certificarse en **ISO 27001**.

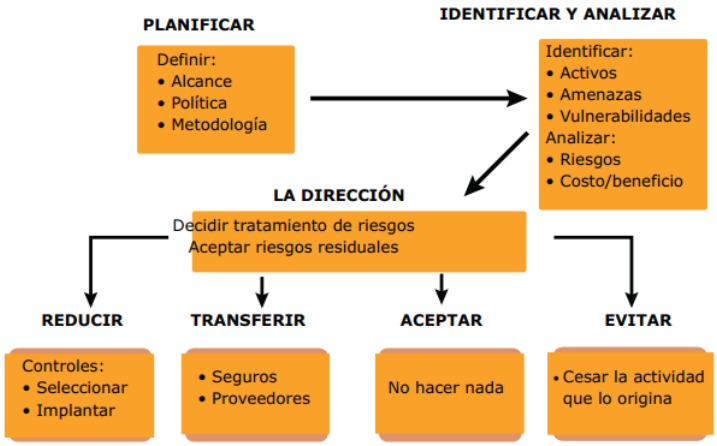
10.2 TRATAMIENTO DE LOS RIESGOS.

Antes de considerar el tratamiento de los riesgos, se debe hacer saber este procedimiento a la autoridad municipal, para que este determine si los riesgos pueden ser aceptados o no por la entidad.

Estos riesgos pueden ser aprobados por la organización si se logra determinar, que el impacto ocasionado no causa ninguna consecuencia negativa en la productividad de la organización.

El siguiente grafico muestra los diferentes enfoques que existen para abordar el tratamiento de los riesgos.

Figura 6. Enfoque tratamiento de los riesgos.



Fuente: SGSI- Sena.

Para cada uno de los peligros identificados, se debe realizar investigación de forma inmediata, a fin determinar las causas y buscarle una solución. Hay que tener en cuenta que existen procedimientos seguros para el tratamiento de los riesgos. Mediante esto se puede como mecanismo:

- ✓ Establecer controles para mitigar los riesgos **(Reducir).**
- ✓ Transferir el riesgo a un tercero **(Transferir).**
- ✓ Aceptar el riesgo y establecer porque es imposible de eliminar **(Aceptar).**
- ✓ Quitar los procesos del negocio que generan el riesgo **(Evitar).**

Para garantizar estos riesgos se puede **Transferir el riesgo,** lo cual a la entidad municipal se le debe proponer subcontratar un servicio externo, especialmente con organizaciones encargadas de respaldar la información, a fin de que se logren reducir las brechas de seguridad y escape de información.

Figura 7. Transferir el riesgo.

Fuente: www.iso27000.es

Para la transferencia de los riesgos a nivel de software, la información se encuentra almacenadas en servidores que almacenan información, algunas se pueden transferir para evitar posibles pérdidas de los datos.

Aceptar el riesgo en cuestión, sería la otra determinación para la cual la alcaldía Municipal, debería tomar debido a que cuando ese riesgo es grande no se tome medidas de protección, es decir cuando el costo de eliminar el peligro es mayor que el daño que causará.

Figura 8. Aceptar el riesgo.

Fuente: www.iso27000.es

Y por último mitigar el riesgo que ayuda a minimizarlos, esto se puede hacer paralizando las actividades de la empresa que supone demasiado nivel de riesgo, adicionalmente estableciendo procesos que brinden seguridad y den medidas de control para que la infraestructura no genere perdidas en ninguna de las dependencias tanto físicas como tecnológicas, implantando medidas en la que se permita salvaguardar los activos de la Alcaldía en mención.

Figura 9. Mitigar el riesgo.

Fuente: www.iso27000.es

10.3 POLITICAS DE SI.

10.3.1 Políticas de la organización de la SI.

La Alcaldía Municipal debe fundamentar un manual que ayuda a describir cuales son los roles y responsabilidades de cada funcionario frente al manejo de la información.

10.3.1.1 Responsabilidades como:

- ✓ Definir claramente las responsabilidades que se refieren a la administración de la SI.
- ✓ Establecer contacto con las diferentes autoridades cuando se requiera, y establecer los responsables de dicho proceso.
- ✓ Fortalecer la cultura a nivel interno de la SI.
- ✓ Que se brinden los recursos necesarios para garantizar el adecuado funcionamiento del Gobierno de SI.

10.3.1.2 Responsabilidades del área de tecnología.

- ✓ Asignar a cada uno de los funcionarios las responsabilidades que tienen frente a la infraestructura tecnológica. todo este proceso debe estar documentado y firmado por los responsables. Así mismo a cada uno de los funcionarios que tengan a su cargo activos informáticos de la organización.
- ✓ Solicitar al Alcalde Municipal que autorice la disponibilidad de los recursos, con el fin de tener una correcta operación del buen gobierno de Seguridad.

10.3.2 Políticas para el tratamiento de Datos Personales.

Aplica a todo sistema de información o archivos que conserven datos de todo el personal vinculado a la administración municipal. De esta manera se permite fortalecer el grado de confianza entre la alcaldía y los empleados en el tratamiento de los datos. Cualquier envío de datos personales será notificado al titular para su debido conocimiento.

Las finalidades para que los datos personales puedan ser transmitidos por una organización son:

- ✓ Dar cumplimiento a las obligaciones emanadas por las leyes laborales colombianas, u órdenes que impartan las autoridades con la solicitud de información.
- ✓ Consultar llamados de atención o memorandos.
- ✓ Aplicar procesos disciplinarios.
- ✓ Contactar a familiares en casos de emergencias.

10.3.2.1 Responsabilidades de la dirección.

- ✓ Se deberá contar con acuerdos de confidencialidad para los empleados.
- ✓ Garantizar la seguridad de los ambientes.
- ✓ Permitir ambientes de trabajo adecuados.

10.3.2.2 Responsabilidades del área de Tecnología.

- ✓ Encargados de darle buen trato al manejo de los datos, manejar la confidencialidad de la información.

10.3.2.3 Responsabilidades de los usuarios.

- ✓ Todo funcionario que utilice los datos de la Alcaldía Municipal, debe darle cumplimiento al gobierno de SI, y a todos los procedimientos establecidos por la organización.

10.3.3 Políticas sobre la gestión de los activos de información.

Esta política garantizará que los datos y activos propios de la alcaldía, que son entregados a los empleados para realizar actividades, se utilicen de manera eficiente y que se garantice la protección ante cualquier amenaza presentada.

10.3.3.1 Responsabilidades del área de tecnología.

- ✓ Velar por el correcto funcionamiento de los activos de información.
- ✓ Manipular el equipo con el mayor cuidado, evitando golpes, rayones, presiones o temperaturas excesivas y ambientes muy contaminados. Mantener líquidos y otras sustancias nocivas alejadas de el/los equipos.
- ✓ Verificar que todo activo de información cuente con hoja de vida, para identificar cada una de sus características, así mismo el empleado que ha sido asignado.
- ✓ Desarrollar los mantenimientos preventivos/correctivos según cronogramas establecidos.

10.3.3.2 Responsabilidades de los usuarios.

- ✓ Darle correcto uso a los activos que se le asignaron.
- ✓ No instalar o almacenar software, salvo aquellos programas utilitarios libres de licencia o en evaluación, de uso corporativo que requiera para su trabajo. En todo caso, deberán respetarse los acuerdos de licencia del software y el usuario será el único responsable por todo aquél que no le haya sido instalado por personal de tecnología de la Alcaldía de Montecristo.
- ✓ Informar sobre cualquier incidente o evento que se presente sobre cualquier activo de información.

10.3.4 Políticas de gestión de acceso de usuarios.

El equipo de tecnología debe administrar los usuarios aptos para los diferentes servicios, en el que se garantice la creación, o eliminación de cuentas.

10.3.4.1 Responsabilidades del área de gestión de tecnología.

- ✓ Las cuentas de usuarios deben ser administrada para los diferentes servicios.
- ✓ Establecer perfiles y privilegios a los usuarios que brinden servicios.
- ✓ Definir y orientar sobre contraseñas seguras y robustas, de igual forma orientar sobre el cambio de forma periódica.

10.3.4.2 Responsabilidades de los usuarios.

- ✓ El funcionario es responsable de cualquier acción realizada sobre los servicios, así mismo sobre las credenciales de autenticación suministrada.
- ✓ No almacenar contraseñas en medios que puedan ser accedidos por terceras personas, ya sean en medio físico o digital.
- ✓ Las contraseñas son de uso personal e intransferible.

10.3.5 Políticas de áreas seguras

La alcaldía municipal contará con procedimientos de seguridad física y de control de acceso en el que se permita proteger las instalaciones y las áreas de trabajo, para que las amenazas internas y externas no logren materializarse.

10.3.5.1 Responsabilidades del área de tecnología.

- ✓ Cualquier actividad realizada en el centro de cómputo, debe estar supervisado por personal del área de tecnología.
- ✓ Controlar el ingreso de personal a la infraestructura tecnológica y verificar las actividades a desarrollar.
- ✓ Proteger las estaciones de trabajos y servidores a través de control ambiental, extintores, sistema de alarmas y video vigilancia. Debe documentarse cualquier evento para tener registro de antecedentes.

10.3.6 Políticas de protección sobre software malicioso.

La Alcaldía municipal de Montecristo debe disponer de controles que permitan proteger la información mediante malware instalado.

Responsabilidades del área de tecnología.

- ✓ Tener herramientas sofisticadas que ayuden reducir el riesgo ante instalación de software malicioso.
- ✓ Garantizar que las herramientas instaladas contra software malicioso se actualicen de forma periódica.
- ✓ Mantener actualizado el sistema operativo y el software de productividad, especialmente en lo relativo a corrección de fallas (agujeros) de seguridad.
- ✓ Restringir operaciones ante instalaciones de software de dudosa procedencia.

10.3.6.1 Responsabilidades de los usuarios.

- ✓ No eliminar herramientas o programas instalados para proteger los recursos tecnológicos de software malicioso.
- ✓ No instalar o almacenar software, salvo aquellos programas utilitarios libres de licencia o en evaluación, de uso corporativo que requiera para su trabajo.
- ✓ No descargar, ni distribuir pornografía, contenidos ofensivos o violatorios de las leyes vigentes.

10.3.7 Políticas de uso del correo electrónico.

El correo es un instrumento de comunicación importante que ayuda a la transferencia de información. El uso adecuado de esta debe estar fundamentado en los principios de SI.

10.3.7.1 Responsabilidades del área de tecnología.

- ✓ Procedimientos para creación y asignación de correos corporativos.
- ✓ Capacitar a los funcionarios sobre el uso adecuado del correo electrónico para prevenir ataques e intrusiones por intermedio del phishing o instalación de malware.
- ✓ Establecer controles que permitan proteger el servidor de correo electrónico.

10.3.7.2 Responsabilidades de los usuarios.

- ✓ El correo institucional es personal e intransferible.

- ✓ La información que se encuentre en los correos debe estar estrictamente relacionada con actividades laborales.
- ✓ Los mensajes enviados deben estar registrado bajo la firma e imagen corporativa de la alcaldía, y no debe estar modificada en ninguna circunstancia.

10.3.8 Políticas del uso de internet.

La Alcaldía municipal debe comprender la importancia del internet en los procesos, se deben proporcionar lineamientos que garanticen una navegación segura.

10.3.8.1 Responsabilidades del área de tecnología.

- ✓ Realizar procesos y procedimientos que permitan garantizar una prestación eficiente y segura al momento de navegar en internet.
- ✓ Limitar la descarga de programas o software malicioso. Así mismo reportar visitas a sitios categorizados como no relevantes y que no son para uso laboral.
- ✓ Bloquear acceso a redes sociales y a sitios que afecten el desempeño y productividad de la entidad.
- ✓ Generar informe sobre consumo y ancho de banda generado por las aplicaciones y usuarios.

10.3.8.2 Responsabilidades de los usuarios.

- ✓ El uso de internet deberá ser de utilidad solo para las actividades de la alcaldía.
- ✓ Evitar descargar e instalar software en los equipos asignados.
- ✓ No permitir el ingreso a redes sociales.
- ✓ No se permite el ingreso a sitios que atenten contra la ética y moral la organización.

10.3.9 Políticas de cumplimiento.

La alcaldía municipal de Montecristo debe velar por que se cumpla la legislación referente a la SI, teniendo en cuenta principalmente la ley 1273 de 2009.

10.3.9.1 Responsabilidades de la dirección:

- ✓ Garantizar que en la administración le dé cumplimento a la legislación vigente.

- ✓ Brindar los recursos necesarios para que se ejecute de forma correcta la normatividad y legislación colombiana de SI.

10.3.9.2 Responsabilidades del área de tecnología.

- ✓ Todo programa instalado en los equipos de la administración municipal debe contar con el debido licenciamiento y descargados desde los portales oficiales.
- ✓ Ejecutar procesos de control que permita proteger los datos personales.

11 PROCESOS DE CONTROL QUE PRETENDAN MINIMIZAR Y MITIGAR LOS TIPOS DE ATAQUES QUE EXISTEN EN LA ACTUALIDAD.

11.1 ANÁLISIS GAP CON BASE EN LAS BUENAS PRACTICAS EMITIDAS POR EL SGSI.

En esta parte se pretende describir el análisis **GAP**[31] **(Análisis de Brecha)** del estándar **ISO27001:2013**, permite determinar el nivel de cumplimiento que tiene la alcaldía municipal de Montecristo, respecto a los lineamientos especificados por la norma técnica, la cual contempla diversos aspectos que deben tenerse en cuenta como buenas prácticas para asegurar la SI de la organización.

Los niveles de madurez del sistema se miden en 5 estados. Aquí se describen:

Tabla 14. Niveles de madurez.

Nivel de implementación	% de Cumplimiento	Descripción.
GESTIONADO	**100**	Se deben gestionar profundamente el análisis de los riesgos y peligros encontrado con los sistemas de información.
		Realizar seguimiento y dar cumplimiento a los procedimientos, tomar las acciones correctivas o preventivas cuando se encuentren fallas.
MEDIBLE	**80**	Medir el cumplimiento de los procesos, aunque no es constante que se tomen las

[31] GAP ANALISIS PARA IMPLEMENTACION DE ISO 9001:2005 [online]. [Consultado: 20 de febrero de 2019]. Encontrado en Internet: [http://cort.as/-ReEb]

		acciones correctivas o preventivas.
DEFINIDO	**60**	Los procesos están documentados pero la responsabilidad del cumplimiento recae en cada individuo y es poco.
REPETIBLE	**40**	Los procesos se desarrollan hasta un punto en el que los procedimientos son utilizados por personas diferentes.
INICIAL	**20**	Se identifica una situación que debe ser tratada, y se deben implementar acciones cuando no hay directivas o documentos relacionados al incidente.
INEXISTENTE	**0**	Carencia de los procesos de SGSI. La entidad no ha encontrado la situación que deba ser tratada.

Fuente: El Autor.

La alcaldía de Montecristo en este momento está en un nivel de madurez del **20%,** de acuerdo a la descripción de la tabla y a la identificación de las situaciones que deben ser tratadas, se necesita implementar como primera medida este proyecto relacionado a la gestión de SI, para salvaguardar los activos de la organización, respecto a la disponibilidad, confidencialidad e integridad.

La calificación que se observa de acuerdo con cada dominio se ilustra en la tabla siguiente.

Tabla 15. Niveles de Cumplimiento.

Ítem.	Dominio	Cumplimiento.
5	Políticas de seguridad	0%
8	Gestión de activos.	45%
9	Control de acceso.	30%
10	Criptografía.	0%
11	Seguridad física y del entorno.	45%
12	Seguridad de las comunicaciones	60%
15	Cumplimiento.	40%
TOTAL		31.4%

Fuente: El Autor.

Tabla 16. Análisis GAP.

11.2 ANÁLISIS GAP.

ISO 27001:2013 controles de seguridad.		CONTROLES
Políticas de Seguridad.	**Políticas de SI.**	Realizar documento en el que se especifiquen los estándares de seguridad. Se debe autorizar por el alcalde municipal y posteriormente explicado a los funcionarios de la administración municipal.
	Revisión de las políticas de Seguridad.	Periódicamente se debe realizar las políticas y realizar las modificaciones al diseño de políticas con el fin de mantenerlo actualizado.
Organización de la SI.	**Roles y Responsabilidades.**	El administrador municipal dispondrá y decidirá quienes son los responsables, con la intención de que permanezca la SI dentro de la alcaldía.
	Contacto con Autoridades.	Se determinarán los procedimientos ante situaciones que se presenten, con las autoridades competentes, con el objetivo de dar respuesta oportuna a un evento o incidente presentado.
Seguridad en los recursos Humanos.	**Verificación de antecedentes previo ingreso al empleo**.	Esta verificación debe hacerse a cada funcionario nuevo a ingresar a laborar a la alcaldía municipal. Debe hacerse en base a la normatividad actual. Adicional se debe verificar las referencias laborales y la validación de títulos profesionales.

	Términos y condiciones del empleo.	Se deben fijar las condiciones contractuales a los nuevos funcionarios, se deben firmar los acuerdos de confidencialidad, en el que se explica las políticas sobre el uso de la información confidencial de la alcaldía, y cuáles son los serios problemas que se pueden presentar ante la divulgación de la misma.
Gestión de Activos.	**Inventario de activos.**	Debe realizarse periódicamente inventario de los equipos, para determinar el estado en el que se encuentran.
	Propiedad de los activos.	Realizar mediante la entrega de acta a cada funcionario activo, con su debida firma para que este administre de forma correcta los equipos a su cargo, durante ciclo de vida.
	Devolución de Activos.	Realizar procedimiento para que cada funcionario una vez deje de laborar, haga entrega de los activos en las condiciones óptimas del cual se les hizo entrega.
	Clasificación de la información	De la importancia del activo, se debe clasificar la información, para realizar la correcta gestión y administración.
	Manejo de activos	Se debe revisar el correcto funcionamiento frente al manejo de activos, Estableciendo políticas manejo seguro, Aquí deben estar plasmado las restricciones, la protección y almacenamiento.
Controles de acceso.	**Políticas de control de acceso**	La administración municipal debe contar con políticas de control, en el que se determinen las reglas correctas de acceso físico y lógico.

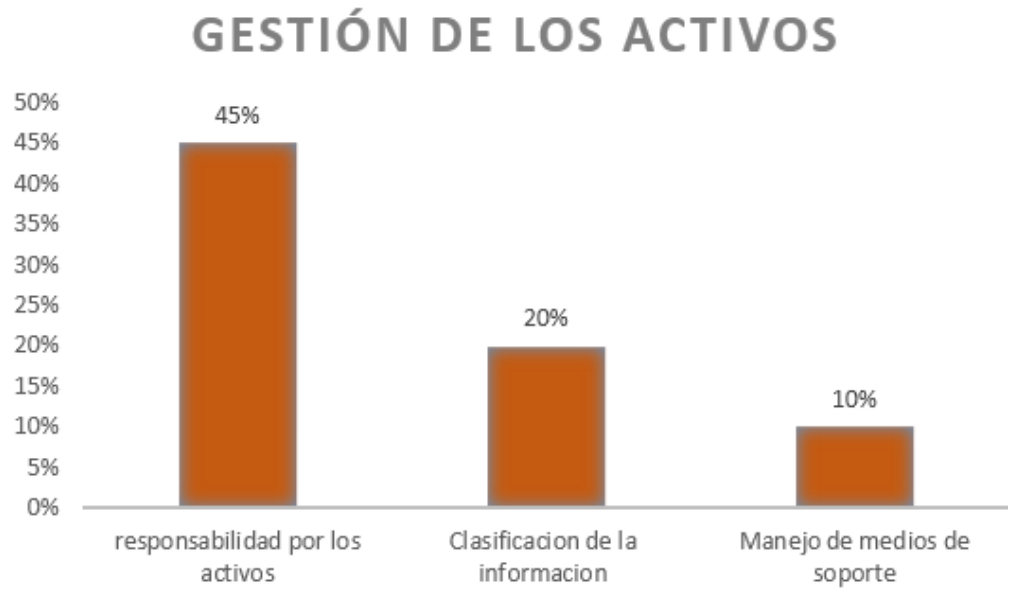
	Acceso a redes y Servicios de red.	Se debe estipular una política de acceso de red para que cada funcionario de la alcaldía haga uso exclusivo de los servicios a los cuales le pertenezca.
Criptografía	**Políticas del uso de controles criptográficos.**	Montar una infraestructura de clave PKI pública.
		Gestionar llaves tales como Smart Card y Smart Token.
Seguridad física y del Entorno.	**Perímetro de Seguridad Físico.**	En el centro de datos se debe disponer un espacio seguro, con el fin de que el procesamiento de información se maneje de forma segura.
	Protección contra amenazas externas.	En la ubicación del DataCenter se debe contar con equipos para el manejo gradual de la temperatura, aires acondicionados y la detección de incendios, tales como extintores.
	Trabajo en áreas seguras.	Inspeccionar las áreas para mirar las condiciones en las que se encuentran, antes de realizar actividades.
	Servicios de soporte	Disponer de servicios de respaldos que se adapten a las necesidades de la alcaldía, a nivel eléctrico y de telecomunicaciones.
	Seguridad en el cableado	Que estas cuenten con las debidas certificaciones ya sea certificación RETIE, para el cableado estructurado y las instalaciones eléctricas.
	Mantenimiento de los equipos.	Disponer de un cronograma de mantenimientos para los equipos informáticos existentes en la organización. Y evidenciar último mantenimiento realizado.
	Eliminación segura de equipos	Dejar evidenciado mediante actas la eliminación de activos informáticos en mal estado. Extraer la información de los equipos para proceder con la eliminación.

	Instalación y protección de los equipos.	Realizar manual de procesos para la instalación y protección de equipos de cómputo, se debe tener priorizado la prevención de amenazas ambientales.
Seguridad en las comunicaciones.	**Controles de red.**	Definir las reglas y políticas para el uso de sistemas de detección de intrusos. **IDS, firewall, etc.**
	Seguridad en los servicios en red.	Establecer reglas de servicio relacionados a la SI.
	Políticas y procedimientos para la transferencia de información.	Para la transferencia de información por intermedio de canales se deben implementar políticas de transferencia de datos unidos a los controles criptográficos, garantizar que el envío de la información sea cifrado.
Seguridad en las operaciones	**Documentación de procedimientos operacionales.**	Procedimientos operacionales y responsabilidades cuyo objetivo es que todos los procesos y operaciones y procesamiento de datos sean realizados de forma correcta.
	Protección de Software Malicioso.	Se fundamenta en que todos los sistemas de información estén protegidos contra códigos maliciosos.
	Respaldo de información.	Los procedimientos de copias de respaldo deberán realizarse periódicamente, se hace con el de Proteger la información contra la perdida de los datos.
	Bitácoras.	La persona encargada debe realizar seguimientos a través de Bitácoras de para los diferentes servicios que se realicen.
Adquisición Desarrollo y	**Especificaciones de requerimientos de seguridad.**	La Alcaldía desarrolla actividades en los que utiliza herramientas ofimáticas y tecnológicas, de lo que es necesario contar con licenciamientos y a su vez proteger los documentos internos antes de realizar cambios en la tecnología de la entidad.
	Control de Cambios en paquetes de Software.	Restringir las modificaciones en los equipos a través de configuraciones.

Mantenimiento de Sistemas.	**Principios de seguridad en la ingeniería de sistemas**	Documentar los principios para la construcción de sistemas seguros que se realicen en cualquier organización.
Gestión de incidentes de SI.	**Responsabilidades y Procedimientos.**	Se debe establecer cuáles son las responsabilidades, roles y procedimientos que debe haber sobre la gestión de SI, a nivel interno de la organización.
	Reporte de eventos.	Establecer los medios de comunicación para la buena gestión de TI.
Cumplimiento.	**Identificación de legislación**	Para el estudio de la información se deberá hacer revisiones periódicamente de acuerdo con la legislación, para garantizar el cumplimiento ante cualquier requerimiento.
	Propiedad intelectual.	Dar cumplimiento a los requisitos legales acorde a la propiedad intelectual y al software patentado.
	Privacidad y protección de la información.	Procedimientos para proteger la información personal.

Fuente: **El Autor.**

Figura 10. Gestión de activos.



Fuente: El Autor.

Según lo evidenciado en las entrevistas realizadas a la alcaldía municipal de Montecristo, en la actualidad esta no cuenta con una definición clara de los activos, ni una clasificación de la información. En el transcurso de las actividades realizadas, se logró organizar de forma mínima la gestión de los activos de TI, de las cuales se realizaron actas, formatos y documentos que fueron entregados a cada funcionario que hace parte de la planta de personal de la administración, con el fin de hacerse responsable de los activos a su cargo.

El proceso de definición de los activos y la clasificación de la información depende del estudio de riesgo, que se haya realizado en la organización, por ello es que se debe realizar un concepto de los activos, de la información y de las políticas de transferencia de activos.

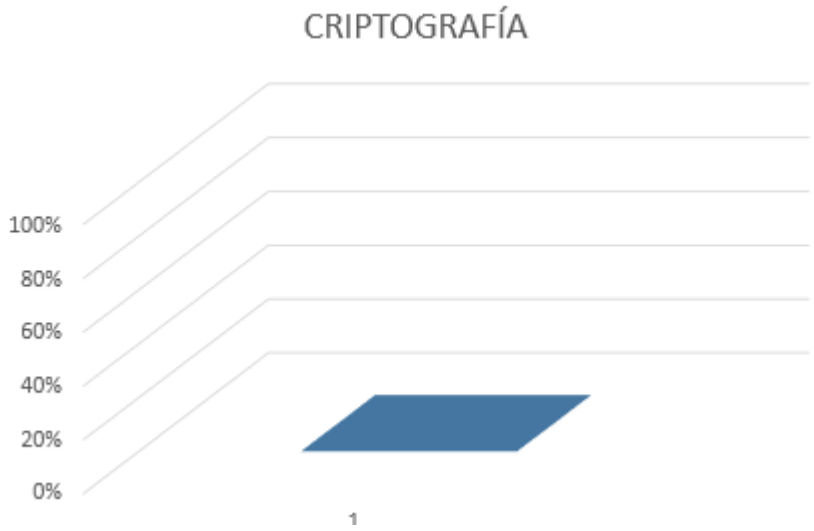
Figura 11. Control de acceso.

Fuente: El Autor.

Con la idea de salvaguardar activos críticos de la Alcaldía Municipal, todos estos procesos deben ser documentados en su totalidad, adicional se debe definir un formato único que sea administrado por la persona encargada de tecnología para que se les enuncien a los funcionarios cuales son las responsabilidades que conlleva la asignación de un usuario.

Es importante que la alcaldía municipal implemente un sistema centralizado de usuarios, en el que se incluyan todas las aplicaciones, con la idea de minimizar los riesgos, y así mejorar las novedades y procesos realizados en cada una de las BD internas.

Figura 12. Criptografía.



Fuente: El Autor.

En la actualidad la Alcaldía Municipal no cuenta con tecnología que le permita manejar este dominio, es importante que en el análisis de riesgo se mida que información se necesita de la aplicación de este control y de esta forma aplicarlo, definir los formatos y las responsabilidades.

Figura 13. Seguridad física y del entorno

Fuente: El Autor.

Es importante que se instalen controles contra riesgos ambientales como incendios, inundaciones, explosiones y otros riesgos, ya que no se cuentan con estos. El centro de cómputo debe ser un área restringida el cual se encuentra ubicado en un lugar de fácil acceso a los y funcionarios y personas.

Importante mirar que en procesos anteriores se han realizado borrado seguro de equipos, en los que se dan de baja. Esto se ha hecho con el objetivo de que la información no quede flotante o que pueda recuperarse con herramientas que realicen dicha función.

Los procedimientos de mantenimientos preventivos y correctivos deben mantenerse, con el fin de minimizar incidentes de SI, a fin de mantener la disponibilidad de los activos.

Figura 14. Seguridad de las comunicaciones.

Fuente: El Autor.

El dominio de seguridad de las comunicaciones pide que las redes se encuentren segregadas por funcionalidad. La alcaldía municipal cuenta con la definición de áreas seguras, las conexiones de red no están aptas a la vista, y están aseguradas al acceso físico.

Figura 15. Cumplimiento.

Fuente: El Autor.

La organización como entidad estatal debe dar cumplimiento a la ley 1582 de 2012, protección de datos personales en primera medida. También se debe verificar toda

la normatividad vigente y darle cumplimiento. La alcaldía debe garantizar que tanto los archivos físicos como digitales estén protegidos ante modificaciones, destrucciones y fugas que puedan presentarse.

11.3 PLAN DE ACCIÓN Y RECOMENDACIONES.

- ✓ Garantizar la aprobación del buen gobierno de SI, por la máxima autoridad Municipal.
- ✓ Crear un cargo laboral de analista de SI, en la alcaldía Municipal.
- ✓ Realizar un estudio de riesgo en la infraestructura municipal relacionado con la ISO 27001.
- ✓ Clasificar la información en base a los activos y a los procesos que se realizan.
- ✓ Adquirir herramientas que sirvan para salvaguardar la información.
- ✓ Asegurar el centro de datos, partiendo desde el aseguramiento físico (Puertas de seguridad), hasta los temas de controles contra amenazas ambientales, (incendios, inundaciones, terremotos, entre otros.)
- ✓ Concienciar a cada uno de los empleados, sobre la importancia del gobierno de la información, a través de campañas, sensibilizaciones, entre otros.
- ✓ Definir una guía para la atención de eventos e incidentes informáticos donde se estipulen los procesos de seguridad, las fallas y los costos que se pueda generar en el manejo de los SI, esto debe estar apto en un servidor local por intermedio de una Intranet institucional.

11.4 DECLARACIÓN DE APLICABILIDAD.

Este proyecto contiene los numerales de la norma NTC-ISO/IEC 27001:2013 que aplican a la (**Alcaldía Municipal De Montecristo**) y las exclusiones de la misma, para efectos de implementar el buen gobierno de SI.

De acuerdo a los resultados reflejados anteriores de la valoración de riesgo se puede evidenciar la siguiente tabla.

Tabla 17. Declaración de aplicabilidad.

DECLARACIÓN DE APLICABILIDAD		
A.5 POLÍTICA DE SEGURIDAD.		
A.5.1.1	Documento de la política de SI.	**Control:** Documento que debe ser aprobado por el Alcalde Municipal y ser puesto en conocimiento a todos los funcionarios de la de la alcaldía municipal.
A.5.1.2	Revisión de la política de SI.	**Control:** Revisar periódicamente la política de SI, y anexar actualizaciones si se requiere.
A.6 ORGANIZACIÓN DE LA SI.		
A.6.1.1	Compromiso de la dirección con la SI.	**Control:** La autoridad municipal deberá brindar apoyo al Gobierno de SI, demostrar que hay interés en proteger los activos de información pertenecientes a la alcaldía municipal.
A.6.1.2	Coordinación de la SI.	**Control:** Toda actividad en relación con la SI, debe estar coordinada por el analista de seguridad y todo el funcionario que hace parte de la alcaldía Municipal.
A.6.1.3	Asignación de responsabilidades para la SI.	**Control:** El analista de SI, definirá responsabilidades de los funcionarios, con el manejo de los datos.
A.6.1.4	Proceso de autorización para los servicios de procesamiento de información.	**Control:** Para el procesamiento de información, cualquier modificación o ajuste debe ser autorizado por el analista de seguridad.
A.6.1.5	Acuerdos sobre confidencialidad.	**Control:** Existirá política de confidencialidad para la no divulgación de información propia de la entidad y el correcto funcionamiento del tratamiento de los datos.
A.6.1.6	Contacto con las autoridades.	**Control:** Deberá existir contacto directo con las autoridades encargadas de regular el control sobre los procedimientos SI, sobre fraude o daño a cualquier organización.
A.6.1.7	Contacto con grupos de interés especiales.	**Control:** No se debe perder contacto con grupos de SI, para estar informado sobre intereses y temas relacionados de seguridad.
A.6.1.8	Revisión independiente la SI.	**Control:** Realizar por lo menos una vez al año, auditorías externas, que ayude hacer más efectivo el control del diseño de políticas para el manejo de la información.
A.7 GESTIÓN DE ACTIVOS.		
A.7.1.1	Inventario de activos.	**Control:** Se necesita tener un control de los activos, para tener un completo inventario.

A.7.1.2	Propiedad de los activos	**Control: C**ontextualizar la metodología para el estudio de activos, que busque establecer el nivel de importancia y los controles necesarios para la protección.
A.7.1.3	Uso aceptable de los activos.	**Control:** Se encuentra documentado y firmado por cada funcionario las reglas de uso de cada activo de información.
A.7.2 Clasificación De La Información		
A.7.2.1	Directrices de clasificación.	**Control:** La información se encuentra clasificada, y se encuentra protegida.
A.7.2.2	Etiquetado y manejo de información.	**Control:** La información se encuentra clasificada, y se encuentra protegida.
A8 SEGURIDAD FÍSICA Y DEL ENTORNO		
A.8.1 Áreas Seguras.		
A.8.1.1	Perímetro de seguridad física.	**Control:** las áreas deben estar señalizadas y protegidas, así mismo existir ruta de evacuación para la protección de cada funcionario en caso de presentarse algún evento.
A.8.1.2	Controles de acceso físico	**Control:** Las estaciones de trabajo, los recursos y los funcionarios están protegidos contra amenazas físicas y ambientales.
A.8.1.3	Seguridad de oficinas, recintos e instalaciones.	**Control:** Los equipos, los recursos y los funcionarios están protegidos contra amenazas físicas y ambientales. cada oficina cuenta con su seguridad
A.8.1.4	Protección contra amenazas externas y ambientales	**Control:** La alcaldía municipal cuenta con una infraestructura propia para protegerse de amenazas externas. A nivel interno cada equipo y activo informático cuenta con sus medidas de protección para contener las amenazas ambientales.
A.8.1.5	Trabajo en áreas seguras.	**Control:** Se realizan trabajos en áreas seguras.
A.8.1.6	Áreas de carga, despacho y acceso público.	**Control:** Se cuenta con lo relacionado.
A.8.2 Seguridad de los equipos		
A.8.2.1	Ubicación y protección de los equipos	**Control:** Los equipos se encuentran bien ubicados y protegidos ante eventualidades que se puedan presentar.
A.8.2.2	Servicios de suministro	**Control:** Debe la administración contar con planta eléctrica para toda la infraestructura, asi mismo contar con respaldo de energía para los equipos, (UPS) en cada ordenador.
A.8.2.3	Seguridad del cableado	**Control:** Deben estar protegidos por canaletas.

A.8.2.4	Mantenimiento de los equipos.	**Control:** Registrar por medio de formatos control de cada mantenimiento realizado a cada equipo de cómputo, para tener secuencia del ultimo mantenimiento.
A.8.2.5	Seguridad de los equipos fuera de las instalaciones.	**Control:** Los equipos deben estar exclusivamente al interior de la alcaldía municipal, cualquier equipo que sea llevado afuera deberá estar autorizado, documentado y firmado por el responsable de la salida del equipo.
A.8.2.6	Seguridad en la reutilización o eliminación de los equipos,	**Control:** Documento que evidencia la eliminación de activos, y los que están en proceso de eliminarse.
A.8.2.7	Retiro de activos.	**Control:** Se debe mirar que ningún activo se debe retirar sin autorización previa.
A.9 Control de acceso		
A.9.1 Requisito del negocio para el control de acceso		
A.9.1.1	Política de control de acceso	**Control:** Definir los lineamientos que limiten el acceso, sólo al personal autorizado, a la información propiedad o bajo custodia de la alcaldía municipal de Montecristo.
A.9.1.2	Registro de usuarios.	**Control:** Cada funcionario debe identificarse, autenticarse, acorde a los accesos permitidos.
A.9.1.3	Gestión de privilegios.	**Control:** El uso de privilegios se encuentra restringido.
A.9.1.4	Gestión de contraseñas para usuarios.	**Control:** Establecer los lineamientos que se deben cumplir para la generación de contraseñas de las cuentas de usuario.
A.9.2 Responsabilidades de los usuarios		
A.9.2.1	Uso de contraseñas.	**Control:** Las contraseñas debe tener por los menos 6 caracteres y debe contener letras mayúsculas, símbolos especiales, @#&/% (),
A.9.2.2	Equipo de usuario desatendido.	**Control:** Se capacita a usuarios para darle protección adecuada a los equipos.
A.9.2.3	Política de escritorio despejado y de pantalla despejada	**Control:** Documentar políticas que permita tener el escritorio limpio y la pantalla despejada.
A.9.3 Control de acceso a las redes.		
A.9.3.1	Política de uso de los servicios de red.	**Control:** El acceso a los servicios, será al personal autorizado.
A.9.3.2	Autenticación de usuarios para conexiones externas	**Control:** Se autoriza a los usuarios realizar conexiones externas siempre y cuando sea para realizar actividades propias de la entidad.
A.9.3.3	Identificación de los equipos en las redes.	**Control:** Los funcionarios deben identificarse y autenticarse de acuerdo los privilegios establecidos.

A.9.3.4	Protección de los puertos de configuración y diagnóstico remoto.	**Control:** Como políticas se bloquean puertos de configuración para evitar la instalación de malware.
A.9.3.5	Separación en las redes	**Control:** Establecer una directiva que defina los controles de acceso a las redes de la alcaldía.
A.9.3.6	Control de conexión a las redes	**Control:** Definir la forma como debe llevarse a cabo la conexión a redes internas de la entidad.
A.9.3.7	Control de enrutamiento en la red.	**Control:** Se debe controlar de manera adecuada el tráfico de datos en la red.
A.9.4 Control de acceso al sistema operativo.		
A.9.4.1	Procedimientos de ingreso seguros	**Control:** Desarrollar política para el control de acceso a servicios, que los ingresos sea totalmente seguros.
A.9.4.2	Identificación y autenticación de usuarios	**Control:** Todo funcionario cuenta con Identificador único (ID del usuario).
A.9.4.3	Gobierno de Seguridad de contraseñas.	**Control:** Se debe asegurar que la gestión de contraseñas esté establecida de acuerdo al manual de políticas.
A.9.4.4	Uso de las utilidades del sistema	**Control:** Restringir uso de programas, que pueden generar riesgos a los equipos.
A.9.4.5	Tiempo de inactividad de la sesión	**Control:** Ante la inactividad por determinado tiempo de un aplicativo se cerrar sesión automáticamente.
A.9.4.6	Limitación del tiempo de conexión.	**Control:** cada aplicativo después de determinado tiempo de inactividad deberá suspender el acceso (Bases de datos de programas sociales del estado)
A.9.5 Control de acceso a las aplicaciones y la información.		
A.9.5.1	Restricción de acceso a la información	**Control:** Definir los procesos de gestión de los usuarios a los SI.
A.9.5.2	Aislamiento de sistemas sensibles.	**Control:** los sistemas sensibles se encuentran aislados.
A.10 GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO		
A.10.1 Aspectos de SI, de la gestión de la continuidad del negocio.		
A.10.1.1	Inclusión de la SI, en el proceso de gestión de la continuidad del negocio.	**Control:** Realizar el plan de contingencia, describiendo como debe reaccionar ante un impacto.
A.10.1.2	continuidad del negocio y evaluación de riesgos	**Control:** Estos eventos pueden ocasionar interrupciones en los procesos de negocio. Los deslizamientos, vendavales, crecientes, lluvias. Implementar el **BCP** y el **DRP.**
A.10.1.3	Desarrollo e implementación de planes de continuidad que incluyen la SI.	**Control:** Evidenciar los planes de continuidad ante desastres y planes de contingencia (Plan

		de continuidad del Negocio, Plan de Recuperación ante desastres.)
A.10.1.4	Estructura para la planificación del BCP.	**Control:** Los planes son consistentes con una sola estructura y cuenta con los requisitos de la SI.
A.10.1.5	Pruebas, mantenimiento y reevaluación de los planes de continuidad del negocio	**Control:** Falta someterlos a pruebas y revisiones periódicas para asegurar la eficacia del plan de continuidad.
A.11 CUMPLIMIENTO		
A.11.1 Cumplimiento de los requisitos legales.		
A.11.1.1	Identificación de la legislación aplicable	**Control:** Es necesario conocer las reglamentaciones que están actualmente vigentes en Colombia que aplican a la seguridad informática.
A.11.1.2	Derechos de propiedad intelectual (DPI)	**Control:** Debe estar documentada sobre todos los Software, Sistemas e información propiedad de la alcaldía Municipal.
A.11.1.3	Protección de los registros de la organización.	**Control:** La información de alta importancia para la organización que se encuentre soportada físicamente debe estar protegida contra perdida, destrucción y falsificación.
A.11.1.4	Protección de los datos y privacidad de la información personal	**Control:** Se garantiza la protección de los datos en base a los acuerdos de confidencialidad anteriormente estipulados.
A.11.1.5	Prevención del uso inadecuado de los servicios de procesamiento de información	**Control:** Se deben realizar controles del uso adecuado de los sistemas y plataformas.
A.11.1.6	Reglamentación de los controles criptográficos.	**Control:** Establecer controles criptográficos, La información enviada por diferentes sistemas esté codificada por algoritmos matemáticos. (SHA-1,SHA-256,SHA-384, DES, MD5,). Entre otros.
A.11.2 Cumplimiento de las políticas y las normas de seguridad y cumplimiento técnico		
A.11.2.1	Cumplimiento con las políticas y normas de seguridad.	**Control:** Será fundamental tener un plan de auditoría, que permita verificar que se está cumpliendo con el diseño de políticas.
A.11.2.2	Verificación del cumplimiento técnico.	**Control:** Por parte del analista de seguridad debe revisarse periódicamente todas las dependencias, a fin de determinar que se esté dando cumplimiento a las normas de seguridad.
A.11.3 Consideraciones de la auditoría de los sistemas de información		
A.11.3.1	Controles de auditoría de los sistemas de información.	**Control:** Se planifica y se efectúa las actividades en la que se requiere verificación de los sistemas operativos a fin de reducir el peligro.

A.11.3.2	Protección de las herramientas de auditoría de los sistemas de información.	**Control:** Las contraseñas de las herramientas encargadas de realizar monitoreo, pruebas y análisis de vulnerabilidades, deben estar administradas por la mano de obra encargada.

Fuente: El Autor

12 DESARROLLO DE POLÍTICAS DE SI, PARA LA ALCALDÍA MUNICIPAL DE MONTECRISTO.

ANUNCIO DE CONFIDENCIALIDAD

Por clara razón de índole estratégica, puede resultar en perjuicio de los intereses de quien presenta estas Políticas, las ideas, estrategias, conceptos, planes de acción y en general todo el material contenido en este documento, sea conocido por personas, entidades u organizaciones diferentes. Teniendo en cuenta que estas políticas serán de uso interno de la **Alcaldía Municipal De Montecristo,** Su contenido no debe ser divulgado, publicado total o parcialmente, sin la autorización consentimiento escrito de la **Entidad Municipal**.

Por lo anterior el diseño de estas Políticas y Procedimientos, son **CONFIDENCIAL** de la organización y por ende no deber ser compartida y estará prohibida su copia o divulgación a terceros.

12.1 DISEÑO DE POLÍTICAS DE SI.

12.1.1 INTRODUCCIÓN

El gobierno de SI, contribuye a gestionar el correcto funcionamiento de la información de la alcaldía municipal de Montecristo, quien es consciente del valor importante que tienen los activos, y en cumplimiento a la misión, visión y valores, se tratará preservar la información propia de la entidad, en el que se garantice en nivel adecuado de:

- ✓ **Confidencialidad:** Garantizar el acceso solo para los usuarios autorizados.
- ✓ **Integridad:** Garantizar que la información no sea modificada sin autorización.
- ✓ **Disponibilidad:** Garantizar que la información esté apta, cuando se necesite.

Razón por la cual la información debe ser protegida en cualquier estado mientras se encuentre almacenada, implementando los controles de acuerdo con el impacto

que se pueda generar por la divulgación o modificación no autorizada de la misma. Por todo lo anterior es que se debe ejecutar y mantener el gobierno de SI, en la alcaldía Municipal de Montecristo.

12.1.2 ALCANCE DEL SGSI.

Política que aplica a todos los funcionarios, SI, procesos o terceros de la alcaldía municipal, que tengan o puedan tener contacto con los diferentes estados de la información propia o bajo su custodia.

12.1.3 OBJETIVOS DEL SGSI.

Implementar, mantener en la Alcaldía Municipal de Montecristo un SGSI, con el fin de salvaguardar los pilares de SI, en cualquiera de sus estados, que estén alineados con la misión, visión, objetivos estratégicos, normativas vigentes, y relacionadas con la SI.

12.1.3.1 Objetivos específicos:

Disminuir los peligros que se encuentran dentro de la organización, para que se logre mantener correctamente los pilares de SI.

- ✓ Gestionar los peligros de SI, sobre los procesos que se encuentren dentro del SGSI, alineados al proceso de riesgo de la entidad.
- ✓ Estandarizar el proceso de SI, que debe cumplir la alcaldía, mediante la elaboración de políticas y documentos relacionados.
- ✓ Gestionar los incidentes de SI.
- ✓ Fomentar en los funcionarios y terceros de la alcaldía municipal un nivel apropiado de concienciación, competencia y cultura de SI.
- ✓ Velar que todos los procesos y SI, cumplan con las procedimientos y documentos relacionados con la SI.

12.1.4 NIVEL DE CUMPLIMIENTO.

Cualquier funcionario o tercero, que incumpla esta política o las que se requieran para desarrollar el Gobierno de SI, deberá asumir las responsabilidades y sanciones que haya lugar, definidas al interior de la Alcaldía Municipal.

12.1.4.1 Principios:

- ✓ Se debe implementar y mejorar diariamente el Gobierno de Seguridad que siempre se encuentre alineado a la misión y visión de la Alcaldía Municipal.
- ✓ Se deberá establecer y aplicar el sistema documentado para el estudio de los riesgos de SI, de acuerdo con los requisitos definidos en la política. Los criterios para la evaluación y aceptación de los peligros deben ser establecido, formalizado y aprobado por el alcalde Municipal.
- ✓ El Área de SI, de la Alcaldía Municipal debe definir un plan de capacitación periódico en "SI".
- ✓ Todo tercero debe firmar un anexo de SI, el cual debe ser parte integral del contrato.
- ✓ La autoridad municipal reconocerá que el gobierno de SI, forma parte de la cultura organizacional de la alcaldía, por lo cual se compromete con el cumplimiento de los objetivos y alcance del diseño de políticas.

12.1.5 SANCIONES POR INCUMPLIMIENTO.

El incumplimiento del buen gobierno de SI, planteadas en el proyecto tendrá como resultado las respectivas sanciones a acuerdo a la magnitud y característica del daño.

12.2 POLÍTICA DE INTERCAMBIO DE INFORMACIÓN.

12.2.1 ALCANCE.

Política aplicada todos los funcionarios, sistemas de información, procesos o terceros de la Alcaldía Municipal de Montecristo, que tengan o puedan tener contacto con los diferentes estados de la información propia o bajo su custodia.

12.2.2 OBJETIVO.

Proteger la información de propiedad o bajo custodia de la Alcaldía Municipal en tránsito frente a interceptaciones, copia, modificación o destrucción no autorizada, que puedan afectar los principios de la SI.

12.2.3 GENERALIDADES

Se debe asegurar la conservación de los principios de SI, de acuerdo con las directrices estipuladas por la Alcaldía Municipal para el intercambio de información, y las definidas por el área de SI.

Se debe clasificar la información, cual es confidencial y cual no. Debe ser definida por el área SI de la organización.

12.2.4 INTERCAMBIO DE INFORMACIÓN CON TERCEROS

Cualquier intercambio de información con terceros, debe quedar formalizado por medio de los procesos de control dispuestos por la entidad, deben quedar descritos en el anexo de SI, que se haya establecido.

En caso de que alguna autoridad de carácter administrativo, ente regulador o judicial requiera la presentación de información propiedad o bajo custodia de la alcaldía se debe solicitar autorización al Mandatario Local, Representante legal, o Secretaría General. Sólo con la autorización de éstos se podrá proceder a divulgar dicha información.

12.2.4 INTERCAMBIO DE INFORMACIÓN INTERNA

Cualquier intercambio de información confidencial debe realizarse de manera segura, por procedimientos que se acuerden entre las partes.

Para los controles que no queden descritos en la política, se debe tener como referencia la legislación vigente o los acuerdos contractuales suscritos.

12.3 POLÍTICA DE ALISTAMIENTO DE SERVIDORES.

El área de Infraestructura Tecnológica de la Alcaldía será responsable de realizar el alistamiento de los servidores de la Alcaldía Municipal.

El alistamiento de los servidores se realiza en dos fases, la primera es la preparación operativa que consiste en el mantenimiento preventivo y correctivo del DataCenter, la segunda fase es el alistamiento lógico que consiste en la instalación de sistemas operativos y configuración de servidores.

12.3.1 Seguridad de los servidores

- ✓ Habilitar y tener configurado todos los servidores en la prestación de los servicios y planes de contingencias.
- ✓ Todo servidor debe ser formateado mediante buenas prácticas de SI, preservando los principios de SI.
- ✓ En el aseguramiento de los servidores se debe realizar las siguientes actividades: actualización de sistemas operativos, creación de usuarios con sus perfiles y grupos, definición de permisos y configuración de las reglas de firewall.

Para el alistamiento de los servidores, se requieren el uso de buenas prácticas de continuidad de negocio y SI, acorde con los recursos y requerimientos que sean aprobados por la alcaldía.

12.4 POLÍTICA PROCEDIMIENTO DE HARDENING – ENDURECIMIENTO.

12.4.1 OBJETIVO

Establecer la línea base del proceso de Hardening (endurecimiento) para los elementos de infraestructura (servidores, bases de datos, Routers, Switches, firewalls, IDS/IPS WAF, entre otros), basados en estándares y/o recomendaciones de cada fabricante, a fin de minimizar los puntos vulnerables de la infraestructura tecnológica de la alcaldía Municipal de Montecristo.

12.4.2 ALCANCE

Las configuraciones deben ser aplicadas por el área de Infraestructura sobre todos aquellos elementos de misión crítica que se encuentran detallados en el Inventario de Servidores.

12.4.3 CONDICIONES GENERALES

Los elementos de infraestructura estarán ubicados físicamente en un Centro de Datos, cuya gestión es responsabilidad de la Dirección de Infraestructura. El ingreso físico, se realiza conforme con el procedimiento de solicitud y asignación de

permisos de ingreso de personal y equipos al DataCenter y, conforme con las políticas de seguridad del proveedor del servicio.

12.4.4 RECURSOS

En el proceso de endurecimiento de los elementos de infraestructura, debe implementarse el uso de plantillas de aseguramiento que permitan realizar pruebas de funcionalidad de los elementos de infraestructura.

Es necesario implementar una gestión de vulnerabilidades con una periodicidad no superior a 3 meses, definir indicador de mitigación y una bitácora de seguimiento de incidentes de seguridad.

12.4.5 PROCEDIMIENTO DE ASEGURAMIENTO.

MEJORES PRÁCTICAS DE CONFIGURACIÓN DE CUENTAS		
Parámetros de contraseñas	**Valor**	**Excepciones**
Histórico de contraseñas	10 contraseñas	N/A
Máxima antigüedad de la contraseña	30 días	N/A
Mínima longitud de la contraseña	8 caracteres	N/A
Mínima antigüedad de la contraseña	1 día	N/A
Número mínimo de dígitos	1	N/A
Intentos fallidos de conexión	5 intentos	N/A
Duración de Bloqueo Cuenta	0	N/A
Tiempo antes de reiniciar el contador	1440	N/A
Cantidad de intentos fallidos para Bloquear	5 intentos	N/A
Número mínimo de letras en la contraseña	1	N/A
Número mínimo de símbolos especiales	1	N/A
Número mínimo de mayúsculas	1	N/A
Número mínimo de minúsculas	1	N/A
Número de segundos antes de desconectar automáticamente a usuarios inactivos del sistema	600 segundos	
Registro de cambios en las tablas	ON/ALL N/A	N/A

12.5 POLÍTICA DE SEGURIDAD INFORMÁTICA Y CIBERSEGURIDAD.

12.5.1 ALCANCE: El desarrollo de esta Política está dirigida a todos los funcionarios, sistemas de información, procesos o terceros de la alcaldía Municipal de Montecristo.

12.5.2 OBJETIVO: Definir los aspectos de seguridad informática y Ciberseguridad a tener en cuenta para sostener los principios de SI, de la alcaldía Municipal.

12.5.3 GENERALIDADES: Para velar por la SI en la alcaldía municipal, se debe cumplir con las siguientes directrices, que buscan generar conciencia en los funcionarios sobre la importancia de los procesos y recursos críticos que ayudan a la administración mantener su competitividad frente a otras organizaciones. Para ello se debe garantizar la seguridad informática teniendo en cuenta lo siguiente:

12.5.4 SEGURIDAD EN EQUIPOS DE CÓMPUTO:

- ✓ Habilitar y tener configurado en todos los equipos de cómputo un software de firewall personal, cuyas reglas no puedan ser modificadas por los funcionarios, ni detener el servicio.
- ✓ Tener configurado en todos los equipos de la alcaldía, software de protección contra programa maligno, ajustado para actualizarse de forma automática y realizar evaluaciones periódicas de los sistemas, cuyas reglas no puedan ser modificadas por los usuarios, ni detener el servicio, a su vez este software debe generar alertas sobre la detección de un malware en un equipo o la red, y ser informadas al área de Tecnología, para su remediación.
- ✓ Todo ordenador debe contar con una línea base de configuración, que debe tener el área de tecnología para definir con que herramientas se debe entregar un equipo de cómputo.
- ✓ Todo funcionario debe entregar todos los activos de su dependencia una vez finalice su relación contractual con la alcaldía Municipal de Montecristo.

12.5.5 SEGURIDAD DE LA RED:

- Mantener un diagrama actualizado de red de la alcaldía Municipal**.**

- Disponer de sistemas que permita limitar el tráfico por intermedio de un esquema de zona segura (DMZ, Zona Desmilitarizada).
- Ubicar los sistemas de bases de datos en una red interna segregada de la zona segura.
- Mantener un documento actualizado de los servicios, protocolos y puertos abiertos en firewalls, en el mismo se debe incluir la justificación pertinente en los casos que se estén utilizando protocolos no seguros (HTTP, FTP, Telnet, IMAP, POP3, SNMP, entre otros).
- Realizar una inspección semestral de la configuración de los Firewall y Routers por parte del proceso de sistemas (seguridad informática donde aplique) y el proceso de SI.

12.5.6 RESPONSABLES:

La responsabilidad de SI, está a cargo del alcalde municipal, por el responsable de seguridad y por todo el equipo de trabajo, es decir es responsabilidad de todos los funcionarios de la entidad.

El servicio de red debe prestarse a los servidores, equipos de trabajo y dispositivos que sean propiedad de la alcaldía municipal. Todo acceso realizado por parte de un tercero a la red interna debe estar debidamente documentado y aprobado por el área de sistemas.

12. 6 POLÍTICAS DE RESPALDO DE INFORMACIÓN.

12.6.1 GENERALIDADES: Como se ha mencionado anteriormente, la información es el valor más significativo de toda organización. La alcaldía de Montecristo debe velar por la conservación de la información, realizando procedimientos de respaldo, sea de la misma alcaldía o de los habitantes. Para tal fin, el área de tecnología es responsable de aplicar el proceso definido para ello, teniendo en cuenta que:

- ✓ El área de tecnología debe mantener y actualizar un inventario específico de la información que se debe respaldar. El tipo, sitio de almacenamiento y el tiempo de custodia de la información. Debe ser definido de acuerdo con la clasificación de la información.

12.6.2 ALCANCE: Esta política está encaminada a todos los procesos de respaldo de información, propiedad o bajo custodia de la alcaldía Municipal de Montecristo.

12.6.3 OBJETIVOS:

- ✓ Proteger los datos críticos de la Alcaldía Municipal de Montecristo.
- ✓ Velar por el cumplimiento de la confidencialidad, integridad y disponibilidad de la información.

12.7 POLÍTICAS DE CLASIFICACIÓN DE ACTIVOS DE INFORMACIÓN.

12.7.1 OBJETIVO: Identificar los activos de información de la entidad, para posteriormente realizar los respectivos controles sobre los mismos.

12.7.2 ALCANCE: Aplica a todos los activos de la alcaldía municipal, que están definidos dentro del alcance del gobierno de SI.

12.7.3 LÍDERES DE PROCESOS: Este documento se refiere así a los cargos de secretarios, alcalde, coordinador de sistemas, analistas de SI y demás recursos asociados.

12.7.4 VALORACIÓN DE ACTIVOS DE INFORMACIÓN: De acuerdo con la política, dentro de la valoración e inventario de activos, se diligenciará un formato de inventario y clasificación de activos de información que se encuentra desarrollado a nivel interno.

12.7.5 IDENTIFICACIÓN DE LOS ACTIVOS DE INFORMACIÓN DEL PROCESO:
Los líderes de los procesos deberán realizar el inventario de los activos de información existentes en la alcaldía municipal.

Para conocer los activos de información del proceso, se recomienda enfocarse en:

- ✓ Entrada y salida de los procesos.
- ✓ Sistemas de información utilizados.
- ✓ Documentos e información creados en el desarrollo del proceso.
- ✓ Servicios utilizados en el proceso, tales como internet, correo electrónico.
- ✓ Información de respaldo.

12.7.6 APROBACIÓN DE LOS ACTIVOS DE INFORMACIÓN: Una vez registrados los activos se debe remitir el formato al analista de SI, el cual deberá verificar que todos los activos de información estén registrados y valorados.

Una vez valorado se debe validar con el analista del proceso, para que este sea aprobado en definitiva y quede estipulado a la organización.

12.8 POLÍTICA DE GESTIÓN DE EVENTOS DE INCIDENTES DE SI.

12.8.1 ALCANCE: Esta política aplica a todos Todo el personal que se encuentre vinculado laboralmente con la ALCALDÍA MUNICIPAL DE MONTECRISTO.

12.8.2 OBJETIVO:

- ✓ Describir el procedimiento para el registro de eventos e incidentes de SI.
- ✓ Asegurar que los eventos e incidentes de SI, sean reportados oportunamente para las acciones correctivas pertinentes.
- ✓ Dejar evidenciado mediante la matriz de riesgos, los eventos e incidentes de SI, una vez estos sean reportados.
- ✓ Garantizar el reporte y oportuna gestión frente a los distintos eventos e incidentes de SI.

12.8.3 DEFINICIONES:

- ✓ **Evento de SI:** Acciones ejecutadas en una organización que implica una posible violación de las políticas de SI. Este puede presentar falla en los controles o situación previamente desconocida que no ha sido identificada.
- ✓ **Incidente de SI:** Acciones ejecutadas en una organización que busca comprometer la operación de una empresa, y amenaza con los principios de seguridad.

12.8.4 GENERALIDADES: Todos los funcionarios de la alcaldía municipal serán responsables de reportar los eventos e incidentes de SI, de los cuales tengan conocimiento. Es responsabilidad del analista de seguridad gestionar el reporte e investigación de estos de acuerdo los lineamientos definidos por la alcaldía.

Los funcionarios o terceros cuyo resultado de las investigaciones de los incidentes, se encuentren responsables de la generación de estos, deberán asumir las acciones disciplinarias, legales y reglamentarias.

12.8.5 IDENTIFICACIÓN DE EVENTO O INCIDENTE:

Todo funcionario de la Alcaldía Municipal está en la capacidad y obligación de reportar cualquier evento que ponga en riesgo el gobierno de SI. A continuación, se relacionan algunos ejemplos:

- ✓ Ingreso de dispositivos no autorizados
- ✓ Filtración de información confidencial
- ✓ Un funcionario que se conecta a un sistema no autorizado
- ✓ Un intento fallido de un usuario para ingresar a una aplicación.
- ✓ Un firewall que permite o bloquea un acceso.
- ✓ Una notificación de cambio de contraseña de un usuario privilegiado, etc.
- ✓ Ingreso de personal no autorizado a las instalaciones.

12.8.6 CONTACTO CON AUTORIDADES.

Contacto	Email/URL	Teléfono
Equipo de SI de la alcaldía.	segurinfo@motecristo-bolivar.gov.co	
Policía Nacional de Colombia	http://www.policia.gov.co/portal/page/portal/Noticias_y_Documentacion/Medios_Comunicacion_Institucionales/Contactos_CE	Se encuentra en la URL especificada
Centro Cibernético – Policía Nacional.	http://cort.as/-SC6x	+57 (1) 4266302
Grupo de respuesta de Emergencias Cibernéticas.	http://cort.as/-SC71 http://cort.as/-SC78	+57 (1) 2959897

12.8.7 DOCUMENTAR EL INCIDENTE:

El equipo de SI, debe documentar los incidentes presentados en el formato corporativo.

12.9 POLÍTICAS DE SEGURIDAD PARA EL USO DE SOFTWARE

12.9.1 GENERALIDADES: La entidad debe contar con procedimientos y procesos que permita proteger los pilares de seguridad de todos los sistemas de información pertenecientes a la alcaldía municipal de Montecristo.

12.9.2 OBJETIVO: Proveer herramientas y controles que permitan disminuir el peligro frente los diferentes tipos de software malicioso que puedan existir, que puedan instalarse equivocadamente por los mismos funcionarios.

12.9.3 ALCANCE: Debe ser puesto en práctica hacia todos los funcionarios, mediante charlas y capacitaciones en temas relacionados, que permita concientizarlo sobre el uso y manejo adecuado del software.

12.9.4 RESPONSABLE: Es responsabilidad del personal encargado del área de tecnología y de todos los funcionarios que tengan relación directa con el manejo de software.

12.9.5 POLÍTICAS:

- ✓ **Cierre de sesión:** Los equipos que se utilizan en la alcaldía municipal deben tener la opción de cerrar sesión de cualquier aplicativo que se esté utilizando después de un lapso de inactividad. De esta manera se evita el acceso de usuarios no permitidos.
- ✓ **Prueba de software:** Todo software nuevo que se instale debe ser probado y evaluado correctamente, para evitar la instalación de software incorrecto que pueda poner en riesgo la integridad de la información.
- ✓ **Instalación de actualizaciones:** Se debe realizar periódicamente revisiones al software, e instalar nuevas actualizaciones que estén aptas para que se pueda aprovechar al máximo el rendimiento de este.
- ✓ **Propiedad intelectual:** Únicamente se debe permitir la instalación de software totalmente licenciado y acorde a la propiedad intelectual. Con esto se evita el uso de software pirata que induzca al mal uso de los recursos y que genere grandes pérdidas en la productividad de la organización.

12.10 POLÍTICAS DE CONTROL DE ACCESO:

12.10.1 OBJETIVO: Definir los lineamientos que limiten el acceso, solo al personal autorizado, a la información propiedad o bajo custodia de la alcaldía Municipal de Montecristo.

12.10.2 ALCANCE: Aplica a todos los funcionarios, sistemas de información, procesos o terceros de la alcaldía Municipal de Montecristo, que tengan relación con la organización.

12.10.3 RESPONSABLE: Es responsabilidad del encargado del área informática y del buen manejo que les den los funcionarios a los SI y bases de datos.

12.10.4 GENERALIDADES: cada funcionario es responsable del control de acceso de los diferentes aplicativos a su cargo, de acuerdo con las políticas a desarrollar.

12.10.5 POLÍTICAS DE USOS DE CONTRASEÑAS:

Como buena práctica para el aseguramiento de la información propia de la alcaldía y de los usuarios, que hacen uso de la IT. Se debe tener en cuenta que las contraseñas:

- ✓ Deben ser únicas y personalizadas.
- ✓ Se deben cambiar regularmente.
- ✓ No se deben utilizar nombres ni fechas personales.
- ✓ El usuario y contraseña no se debe anotar en ninguna parte, debe ser memorizada.
- ✓ No se debe registrar físicamente las contraseñas.
- ✓ No compartir la contraseña de usuarios asignadas.
- ✓ Las contraseñas almacenadas deben estar cifradas.

- **Métodos de autenticación:** Implementar controles de acceso y métodos de autenticación.
- **Segmento de red:** Segmentar la red (adquirir Enrutadores y Gateways).
- **Definir perfiles:** Definir los perfiles de acceso a los sistemas, asignar los roles dentro del sistema de información con funciones específicas a cada funcionario.
- **Registro de usuarios:** Administración de usuarios y contraseñas, para dar o eliminar accesos.
- **Control de acceso a la red:** El Coordinador de sistemas estará en capacidad brindar los accesos a la red y todos los recursos. Se debe controlar los servicios como el correo electrónico, transferencia de archivos, entre otros.

12.11 POLÍTICAS DE RESPALDO DE INFORMACIÓN

12.11.1 ALCANCE

Aplica a todos los procesos de respaldo de información, que se encuentren en propiedad o bajo custodia de La Alcaldía Municipal de Montecristo.

12.11.2 OBJETIVO

- ✓ Proteger la información crítica del negocio y la de todos los usuarios pertenecientes a los distintos programas sociales del estado.
- ✓ Velar por el cumplimiento de los principios de SI respaldada.

12.11.3 GENERALIDADES

La Alcaldía Municipal de Montecristo, debe velar por la conservación de la información, realizando copia de los datos, sea propia o de los usuarios. Para tal fin, el área de Tecnología es responsables de aplicar el proceso definido para ello, teniendo en cuenta:

- ✓ El área de Tecnología debe mantener y actualizar un inventario específico de la información que se debe respaldar. El tipo, la frecuencia, sitio de almacenamiento y el tiempo de retención de los respaldos de la información, deben ser definidos teniendo en cuenta la clasificación de la información.
- ✓ Registrar los pasos de restauración de copias de seguridad (backup) para cada tipo de información a respaldar.

12.11.4 DEFINICIONES

- ✓ **Información Sensible:** información con un alto grado de confidencialidad en el que depende el éxito de una organización (como: secretos comerciales, transacciones financieras, información confidencial de terceros confiada a la organización, etc.).
- ✓ **Información Crítica:** información que debe permanecer apta para cumplir los objetivos misionales de la organización.

12.11.5 DESCRIPCIÓN DEL ESTÁNDAR

- ✓ **Programa de Respaldo de Información:**

Las Áreas de Tecnología deben mantener y actualizar un inventario específico de la información que se debe respaldar en la organización, teniendo en cuenta las directrices de la **Política De Respaldo De Información.**

- ✓ **Pruebas de restauración de copias de seguridad**

Los procesos de Tecnología deben documentar los procesos de ejecución de restauraciones de copias de seguridad para cada tipo de información a respaldar. El área de Tecnología debe generar un plan de restauración de la información que respalda, definiendo tipo de restauración, frecuencia y condiciones que apliquen, que cubra como mínimo los siguientes criterios:

INFORMACIÓN RESPALDADA	RESTAURACIONES MÍNIMAS A EJECUTAR
Los Archivos de Gestión de los Usuarios.	Muestra aleatoria para el Alcalde, Secretarios de Despacho, y aquellos funcionarios que dentro de su labor conservan información soporte de los usuarios.
Correos Electrónicos corporativos	Muestra aleatoria para el Alcalde, Secretarios de Despachos, y aquellos usuarios que dentro de su labor tienen contacto directo y permanente con los usuarios.
Bases de Datos de los Servidores	Todas las bases de datos existentes.
Repositorios de imágenes o archivos críticos.	Muestra aleatoria de los archivos de imágenes de la alcaldía Municipal.
Códigos Fuentes de aplicativos propios de las compañías	El Área de Tecnología es responsable del Backup del servidor de versionamiento de software. Será responsable de retener la información de los códigos fuentes de sus aplicaciones actualizadas en los servidores. Por lo anterior Tecnología responde por la restauración de los códigos fuentes que se encuentren dentro del servidor de versionamiento. y debe garantizar las pruebas de restauración de los demás códigos existentes de sus aplicaciones que no se encuentren en dicho servidor.
Árbol de Backups	Mensualmente.

Toda prueba de restauración se realizará a partir del medio de almacenamiento que contiene la copia de respaldo. Los datos restaurados deben ser destruidos de forma segura según el Estándar Para La Eliminación O Destrucción De Información.

Es necesario que área de Tecnología disponga de ambientes adecuados para ejecutar las pruebas de restauración y el diligenciamiento del correspondiente soporte de realización de estas en la herramienta Service Desk definida por la Alcaldía Municipal de Montecristo.

12.11.6 ALMACENAMIENTO

Las instalaciones donde se almacenen los medios de respaldo de información deben cumplir con las siguientes características:

- ✓ Procedimiento de seguridad física y de acceso que garanticen su integridad y confidencialidad.
- ✓ Condiciones ambientales adecuadas (como temperatura y humedad) que garanticen su preservación.

Las copias de respaldo deben ser custodiadas en una instalación diferente al sitio de procesamiento de la información, con el objetivo de preservar la operación del negocio.

Tecnología deberá definir la estrategia de custodia que asegure la conservación del backup de la información.

Es necesario que los medios magnéticos y ópticos sean correctamente etiquetados y organizados para facilitar su identificación y ubicación en el momento en que se requiera recuperar información. Asimismo, deben almacenar los datos confidenciales y que contractualmente se establezcan, utilizando procesos de cifrado.

12.11.7 TIEMPO DE RETENCIÓN DE LOS BACKUP.

Según lo indicado en la Política de respaldo, el área de Tecnología debe definir los programas de respaldo de información con tiempos de retención. Retenciones adicionales a las definidas, por necesidad de la alcaldía.

12.11.8 ROLES Y RESPONSABILIDADES

- ✓ El propietario de la información debe informar a Tecnología sobre la necesidad de respaldo y retención de su información.
- ✓ El proceso de Tecnología es responsable del respaldo de la información inventariada en el Programa de Respaldo de Información definido.
- ✓ El proceso de Tecnología será responsable de la ejecución del Plan de Restauración definido.
- ✓ Los Líderes de Procesos dentro de Alcaldía Municipal, son responsables de informar a Tecnología la necesidad o cambios en los programas de respaldo y restauración.

12.12 POLÍTICAS DE ESCRITORIO LIMPIO Y PANTALLA DESPEJADA

12.12.1 ALCANCE

Aplica a todos los funcionarios, sistemas de información, procesos o terceros de la Alcaldía Municipal de Montecristo, que tengan o puedan tener contacto con los diferentes estados de la información propia o bajo su custodia.

12.12.2 OBJETIVO

Establecer los principios de protección de la información que reside en los puestos y estaciones de trabajo, así como salvaguardar los principios de SI, de la alcaldía Municipal.

12.12.3 GENERALIDADES

Todos los funcionarios de la Alcaldía, que hagan uso de la infraestructura, para el desarrollo de sus labores deben:

- ✓ La información en todo momento debe estar custodiada, salvaguardada de personas no autorizadas.
- ✓ Se debe clasificar la información confidencial, Mantener los puestos de trabajo organizados, y la información física almacenarse bajo llave o en lugares seguros.

En cuanto a la información que se maneja en los ordenadores de la alcaldía municipal, los funcionarios deben:

- ✓ Conservar la pantalla libre de accesos directos a información clasificada como Confidencial.
- ✓ Verificar que en los equipos asignados o bajo su responsabilidad se bloquee la sesión de trabajo, cuando se ausenten.
- ✓ Evitar que los documentos que contengan información clasificada como Confidencial, se expongan en las impresoras, fax, fotocopiadoras y escáneres.
- ✓ Evitar la pérdida o deterioro de la información que reposa en los puestos de trabajo por acciones que atenten contra las normas corporativas.
- ✓ La información que esté guardada en medios de almacenamientos debe cumplir con lo estipulado en la política.

12.13 POLÍTICAS DE USO DE CONTROLES CRIPTOGRÁFICOS:

12.13.1 ALCANCE

Política aplicada a todos los funcionarios, sistemas de información, procesos o terceros de la alcaldía Municipal de Montecristo, que tengan contacto con los diferentes estados de la información propia o bajo su custodia.

12.13.2 OBJETIVO

Proteger la información propiedad o bajo custodia de Alcaldía Municipal, Utilizando procedimientos de encriptación para garantizar la confidencialidad e integridad, en su transmisión y almacenamiento.

12.13.3 GENERALIDADES

Teniendo en cuenta la clasificación de la información, de acuerdo con su criticidad, se debe proteger con procesos de cifrado apropiados, cuando se procese, almacene o transmita en:

- ✓ Información contenida en medios de almacenamiento (USB, Discos, CDs, DVD´s, Cintas, entre otros).

- ✓ Copias de respaldo.
- ✓ Información propia o bajo custodia de la alcaldía transmitida de manera interna o externa, a través de cualquier medio de comunicación o aplicación.

Las páginas web institucionales publicadas en Internet deben contar con certificado digital emitido por una entidad certificadora externa avalada.

12.14 POLÍTICAS DE ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE LOS SISTEMAS DE INFORMACIÓN:

12.14.1 GENERALIDADES:

La Alcaldía municipal de Montecristo debe tener en cuenta que cualquier sistema de información obtenido o desarrollado por cualquier empresa, este deba cumplir con los requisitos de calidad, siendo este parte integra del producto.

12.14.2 OBJETIVO:

Suministrar los recursos necesarios para que se cumpla con todas las políticas de mantenimiento y desarrollo de los SI.

12.14.3 ALCANCE:

Esta política debe ser aplicada a todos los SI, con los que cuente la alcaldía municipal.

12.14.4 RESPONSABLE:

Es responsabilidad del área informática, ya que este se encarga de asignar las claves, de que se cumpla con los estándares de seguridad de software.

12.14.5 POLÍTICAS:

- ✓ Asegurar que los sistemas de información cuenten con sus respectivos controles, y relacionados a las políticas de SI de la organización.
- ✓ De realizarse el procedimiento dentro de la entidad, estos deben quedar debidamente registrados y documentados. Se debe relacionar el versionamiento del software.
- ✓ Hacer registro ante la dirección general de derechos de autor.

12.15 POLÍTICAS DE SEGURIDAD DEL SISTEMA ELÉCTRICO.

12.15.1 GENERALIDADES: Implementar generador de corriente eléctrica para que no se suspendan las actividades diarias en caso que se pierda el fluido eléctrico.

12.15.2 OBJETIVO: implementar medidas y políticas de seguridad para el buen manejo y uso del sistema eléctrico.

12.15.3 ALCANCE: Dirigido a todos los funcionarios en especial al encargado de la manipulación de dicho equipo.

12.15.4 RESPONSABLE: Será responsabilidad del área de seguridad de SI, y personal de control interno, transmitir el reglamento sobre el uso y funcionamiento de los aparatos eléctricos.

12.15.5 POLÍTICAS:

- ✓ **Generador de corriente:** La fuente eléctrica debe ser controlada y restringida. Solo sea manipulada por el personal autorizado y capacitada en el manejo de electricidad, de este se garantiza que no sea averiada por terceras personas y garantice durabilidad de la fuente.
- ✓ Norma RETIE: Todos los equipos eléctricos deberán cumplir con las normas de reglamento de electricidad (RETIE), así se evita que se generen daños a personas y a equipos asociados a la unidad eléctrica.

13 PROCEDIMIENTOS DE APOYO EN EL DISEÑO DEL GOBIERNO DE SI, DE LA ALCALDÍA MUNICIPAL DE MONTECRISTO.

13.1 ACCIONES DE MEJORA.

13.1.1 Objetivo:

Implementar las acciones preventivas y correctivas necesarias, con el fin de identificar, analizar y eliminar las amenazas que puedan presentarse y así garantizar la total disponibilidad de los recursos tecnológicos de la Alcaldía Municipal de Montecristo.

13.1.2 Alcance:

Aplica a todos los funcionarios, sistemas de información, Procesos o terceros de la Alcaldía Municipal de Montecristo que tengan o puedan tener contacto con los diferentes estados de la información propia o bajo su custodia.

13.1.3 Documentos de referencia:

- ✓ NTC ISO 27001.
- ✓ NTC ISO 27002
- ✓ NTC 1486.
- ✓ Registros de auditorías internas.

13.1.4 Responsabilidad:

13.1.4.1 Autoridad municipal:

- ✓ Suministrar los recursos necesarios para que se dé cumplimiento a todo el procedimiento.
- ✓ Mantenerse informado de las acciones correctivas, preventivas y de los resultados, para medir sin son adecuadas y eficaces.

13.1.4.2 Coordinador de área de tecnología:

- ✓ Identificar la raíz del problema.
- ✓ Identificar cuáles son las causas que se presentan ante amenazas externas y utilizar las herramientas necesarias y apropiadas para dar solución.

- ✓ Contar con los recursos necesarios para ejecutar las acciones.
- ✓ Hacer seguimiento a los informes que se realicen.
- ✓ Analizar si las acciones planeadas son adecuadas y le convienen a la entidad.
- ✓ Cerrar las incidencias, cuando se dé solución a las actividades planteadas.

13.1.5 Aspectos críticos:

- ✓ Evaluar las causas de los posibles problemas.
- ✓ Reportar situaciones de no conformidad.
- ✓ Realizar seguimiento a todas las acciones.
- ✓ Medir la eficacia y eficiencia de la solución tomada.

13.1.6 Registros:

- ✓ Creación de informe de las acciones de mejora.
- ✓ Seguimiento.

13.1.7 Definiciones:

- ✓ No conformidad: Cuando se incumple a un requerimiento.
- ✓ Corrección: Acción que se toma ante una no conformidad encontrada.
- ✓ Acción correctiva: Correctivo tomado para sustraer una conformidad y evitar que vuelva a suceder.
- ✓ Acción preventiva: Acción que se toma para mitigar riesgos.

14. RESULTADOS A ENTREGAR.

Al finalizar el proyecto aplicado, la Alcaldía Municipal de Montecristo, logrará tener una guía conceptual importante que se puede aplicar a la gestión de la SI, de la misma entidad.

Esta guía está conformada por:

- Un diseño de políticas de gestión de SI, guiado por la Norma **ISO 27001** para la Alcaldía Municipal de Montecristo.

- Desarrollo de una matriz donde se identifican, se clasifican y se valoran los activos de información de la Alcaldía Municipal.

- Una matriz de las amenazas y los riesgos que se encuentran en la entidad municipal.

15 RECURSOS NECESARIOS PARA SU REALIZACIÓN.

15.1 Recurso humano:

- Se necesita presupuesto económico y disponibilidad por parte de la autoridad municipal para el desarrollo del proyecto.

- Se necesita un asesor o una empresa especialista en SI, con experiencia en la implementación de un SGSI.

- Analista de SI, responsable de velar por el cumplimiento al buen gobierno de SI.

- Funcionario de la Alcaldía Municipal implicado en los procesos para su desarrollo.

15.2 Recursos tecnológicos:

- Ordenadores y herramientas ofimáticas.

15.3 Normas, estándares y documentación:

- ISO 27001.
- ISO 27002
- Metodología Magerit.

16. CONCLUSIONES.

Mediante el levantamiento de la información que se ha llevado a cabo, se evidencia que la Alcaldía municipal de Montecristo presenta un alto riesgo, debido a que no tiene los pasos necesarios para la protección de la información. Actualmente se puede observar que esta alcaldía es muy vulnerable a ataques informáticos, desde hace muchos años no se ha contado con la implementación de un gobierno de SI, que permita mitigar estas amenazas.

Con la implementación de diferentes metodologías entre ellas **MAGERIT**, se permite reducir los riesgos que tiene la entidad, ya que a través de esta se puede eliminar los peligros que se encuentran los activos, y así mismo indica cuales se van a proteger.

Es de suma importancia realizar capacitación a todo el funcionario que hace parte la alcaldía Municipal de Montecristo, en temas relacionados de seguridad, se debe dejar claro que esta es de gran importancia a nivel organizacional, ya que su implementación ayuda a la productividad de la empresa.

Con la implementación de estas metodologías es importante la creación todos los manuales, políticas y procedimientos tendientes a la SI. A través de estas se puede dar operación eficiente del gobierno de SI, y mantener la productividad del cualquier negocio.

17. RECOMENDACIONES.

Implementar el Gobierno de SI, para toda la infraestructura de la Alcaldía Municipal de Montecristo.

Tener un plan estratégico que sirva para controlar y proteger la SI de la alcaldía municipal cuando se presenten amenazas ya sea internas o externas.

La Alcaldía Municipal debe iniciar un proceso de sensibilización al funcionario en base a los aspectos más importantes de la SI.

Es de gran importancia que la entidad realice auditorias mínimo una vez al año en la gestión de SI.

Que se establezcan los perfiles y roles de acuerdo con la estructura organizacional. Recalcarles la importancia de este proyecto en la organización.

La alcaldía municipal debe establecer procedimientos y políticas de acuerdo con la ley 1581 de 2012, tratamiento de los datos personales, respecto a la información que está bajo la responsabilidad de la entidad.

18. BIBLIOGRAFIA.

ALBERTO G. ALEXANDER. (2007). Diseño SGSI (1ra edición). Bogotá, Colombia: Editorial Alfaomega. **CICLO PDCA.** Obtenido de http://cort.as/-RsNi.

ALEXANDRA PARCO, Paola Alexandra. SGSI en el comando provincial. Ecuador: Universidad del Norte. Ingeniería, 2013. 399.

AMUTIO, MIGUEL Y CANDAU, JAVIER. MAGERIT. Versión 3.0 Metodología de Magerit Libro I. Método.

CARRILLO ARIAS, GONZALO. Implementación de firewall controlar los accesos no autorizado a la red inalámbrica del hospital de Santander. – Trabajo de grado seguridad informática. – UNAD.

CORLETTI Alejandro, Controles de SI. 2006. Obtenido de [http://cort.as/-RsO-]

DE FRAITAS. Vidalina. 2009. Análisis y evaluación del riesgo de SI: Proyecto presentado a la Universidad simón Bolívar.

DE LA CRUZ GUERRERO, César Wenceslao y VÁSQUEZ MONTENEGRO, Juan Carlos. Desarrollo de SGSI para la USAT. Trabajo de grado Ingeniería de Sistemas.

DIRECCIÓN GENERAL DE MODERNIZACIÓN ADMINISTRATIVA ESPAÑOLA, "MAGERIT v.3".

ERIK IVAN CRUZ Y DIANA VANESSA RODRÍGUEZ Propuesta de grado presentada en noviembre de 2010, Tesis de grado - ciudad de México.

FORMACIÓN, Líderes Nacionales de Cadena La Investigación en la Escuela de Ciencias Básicas, Bogotá D.C.: UNAD, 2011.

GOMEZ GALLO (2005), Luis Humberto Presidente del senado. Diario oficial 45.963. [http://cort.as/-RsOC]

GONZALEZ HERNANDEZ, LUIS FELIPE. Implementación de Cloud Computing – título de especialista en Seguridad Informática. CUCUTA 2016,

GONZALEZ RETAMOZO, JOSE EDWIN. Auditoría de Seguridad informática Para la Institución Educativa Luis Carlos Galán- MUNICIPIO DE YACOPÍ CUNDINAMARCA. Proyecto de Seguridad Informática. UNAD.

ISO / IEC 27002 (2013). Tecnología de la información - Técnicas de SI MINVIVIENDA (2010). Decreto 1469, Obtenido: http://cort.as/-RsNo

PATIÑO ALPALA, LUIS O. Políticas de seguridad informática a empresa corporativa, PROPOLSINECOR- Trabajo de grado de Seguridad informática

PRESSMAN, ROGER S. (2002). Ingeniería del software: Editorial McGraw Hill, Capítulo 6: “Análisis y Gestión del Riesgo”.

REYES PLATA, ALEJANDRO. (2011). Ethical Hacking. UNAM-CERT. Recuperado de [http://cort.as/-RsO7]

ROBAYO LOPEZ, JAVIER HUMBERTO, RODRIGUEZ, RICHAR MAURICIO, Seguridad de los sistemas de la empresa sitiosdima.net, Monografía De SI.

SERRANO LATORRE, JAIRO D HEYMANN PIGNOLO, ELISA, CÉSAR GALO BARDES, EDUARDO, Universidad Autónoma De Barcelona. Dpto. de Arq. de Computadores. Aparece en Internet: http://cort.as/-RsNe

SOMMERVILLE, IAN. (2005). Ingeniería del software. Editorial Pearson, Sección 5.4 “Gestión de riesgos”.

TORI, CARLOS. (2008). HACKING ÉTICO. Rosario Argentina. Recuperado de [http://cort.as/-RsO9]

UNIVERSIDAD DISTRITAL. SI: Política de SI de la Universidad José de Caldas, obtenido en: http://cort.as/-RsNt

UNIVERSIDAD JAVERIANA. Manual del SGSI, Obtenido: http://cort.as/-RsNw

19. ANEXOS.

Anexo 1. LISTA DE VERFICACIÓN CUMPLIMIENTO EN NORMA ISO 27001:2013

PROCESO	FECHA	HORA	LUGAR
AUDITADOS	**NOMBRE**	**CARGO**	**FIRMA**
Responsable del proceso			
Acompañante(s)			
GRUPO AUDITOR	**NOMBRE**	**CARGO**	**FIRMA**
Auditor Líder.			
Auditor(res) Acompañante(s)			
DOCUMENTO DE REFERENCIA			

Anexo 2. INFORME ACCIÓN DE MEJORA

CODIGO HALLAZGO:

TIPO ACCIÓN		NO CONFORMIDAD		ORIGEN		INFORMACION AUDITORIA	
CORRECTIVA		CRITICA		REPORTE INTERNO		AUDITOR	
PREVENTIVA		MAYOR		AUDITORIA		FECHA	
		MENOR		REVISION POR LA DIRECCION		PROCESO	
		OBSERVACION		REPORTE EXTERNO		AUDITADO	

HALLAZGO – NO CONFORMIDAD
_____ RESPONSABLE DEL PROCESO

ANALISIS DE CAUSAS
Describa la conclusión del análisis.

PLAN DE ACCION PROPUESTO			
N°	**Actividades propuestas**	**Responsable**	**Fecha máxima Implementación.**

SEGUIMIENTO A LA EJECUCIÓN DE ACTIVIDADES					
N° de Actividad	**¿Se implementó?**		**Fecha**	**Auditor**	**Observaciones**
	SI	NO			
	SI	NO			
	SI	NO			
	SI	NO			

EFICACIA DE LAS ACTIVIDADES					
N° de Acción	**¿Fue eficaz?**		**Fecha**	**Auditor**	**Observaciones**
	SI	NO			
	SI	NO			
	SI	NO			
	SI	NO			

EFICACIA DEL PLAN DE ACCIÓN					
¿Fue eficaz el plan d acción para el cierre del hallazgo?	Si No	**Firma auditor**		**Fecha cierre acción**	

Anexo 3. FORMATO PLAN DE AUDITORIA

OBJETIVO	ALCANCE

CRITERIOS Y DOCUMENTOS DE	EQUIPO AUDITOR		INICIALES
	Auditor Líder		
	Auditor (as) Acompañantes(s)		

PROCESO A AUDITAR	RESPONSABLE EQUIPO AUDITOR	RECIBE AUDITORIA	FECHA	LUGAR	HORA

FECHA APERTURA	LUGAR APERTURA	HORA APERTURA
FECHA CIERRE	LUGAR CIERRE	HORA CIERRE

LISTA DE ASISTENTES

NOMBRE	CARGO	FIRMA APERTURA	FIRMA CIERRE

Anexo 4. FORMATO DE INFORME DE AUDITORIA

OBJETIVO	ALCANCE

PROCESO AUDITADO	RECIBE AUDITORIA	FECHA	LUGAR	NO CONFORMIDADES	
				Tipo	Cantidades
				Critica	
				Mayores	
				Menores	
				Observaciones	

CRITERIOS Y DOCUMENTOS DE REFERENCIA	EQUIPO AUDITOR	
	Auditor líder	
	Auditores Acompañantes	

Anexo 5. INFORME DE INCIDENCIAS DE SEGURIDAD.

CODIGO DE INCIDENCIA:

FORMATO REGISTRO DE EVENTOS O INCIDENTES DE SI.			
FORMATO REPORTE DE EVENTO O INCIDENTE DE SI		**Versión:**	
		Fecha:	
		Proceso a cargo:	
INFORMACION GENERAL DEL REPORTE			
Incidente:		**Evento:**	
Categoría:		**Estado:**	
Subcategoría:		**Valoración/Prioridad:**	**ALTO**
Reporta:			
Cargo:		**Dependencia:**	
Sede:		**Email:**	
INFORMACIÓN GENERAL DEL EVENTO O INCIDENTE DE SI			
Fecha y hora de ocurrencia:			
Fecha y hora de identificación:			
Fecha y hora de reporte:			
Fecha y hora de contención:			
Sistema de información afectado:			
Quien reporta:			
DESCRIPCIÓN DEL EVENTO O INCIDENTE DE SI			
RECURSO INFORMATICO AFECTADO			
Nombre del recurso:			

Ubicación física	
Información que contiene	
CONCLUSIONES	
LECCIONES APRENDIDAS	

FIRMAS			
Elaborado por: (Nombres y Apellidos):		**Revisado por: (Nombres y apellidos)**	
Firma digital:		**Firma Digital:**	
Cargo:		**Cargo:**	
Fecha:		**Fecha:**	
Revisado por: (Nombres y Apellidos)		**Revisado por: (Nombres y Apellidos)**	
Firma digital:		**Firma digital:**	
Cargo:		**Cargo:**	
Fecha:		**Fecha:**	

FORMATO DE RESULTADO DE GESTIÓN DEL EVENTO O INCIDENTE DE SI.

FORMATO DE RESULTADO DE GESTIÓN DEL EVENTO O INCIDENTE DE SI		
REPORTE DEL RESULTADO DE LA INVESTIGACIÓN DE INCIDENTES	Versión:	
	Fecha:	
	Responsable:	
Objetivo:		
Alcance:		
INFORMACIÓN GENERAL DEL EVENTO E INCIDENTE		
Fecha y hora del reporte:		
Número de Caso:		
RECOLECCIÓN DE FORMACIÓN		
INFORMACION DE VALORACIÓN DE INCIDENTE O EVENTO		
Fecha y hora de Valoración:		
Nombre de quien valora:		
Valoración prioridad:	ALTO	
INFORMACIÓN EQUIPO INVESTIGADOR		
NOMBRE	CARGO	CORREO
CAUSAS		
PASOS EJECUTASDSOS EN LA INVESTIGACIÓN		
BITÁCORA DEL EVENTO O INCIDENTE DE SI.		

Fecha y hora de la acción	Descripción de la acción	Responsable	cargo

FORMATO DE VALORACIÓN DE INCIDENTES O EVENTOS

FORMATO DE VALORACIÓN DE INCIDENTES O EVENTOS		
FORMATO VALORACIÓN DE INCIDENTES DE SI.	Versión:	
	Fecha:	
	Responsable:	
INFORMACIÓN GENERAL DEL INCIDENTE O EVENTO		
Fecha y Hora del Reporte:		
No. De Caso:		
Descripción del incidente o Evento.		
INFORMACIÓN DE VALORACIÓN DE INCIDENTE O EVENTO		
Fecha y hora de Valoración		
Nombre de quien valora:		

Valoración del Incidente o Evento	ALTO
Observaciones de la valoración	
ANEXOS	

ESTADO DEL EVENTO E INCIDENTE DE SI

ESTADO DEL EVENTO E INCIDENTE DE SI			
FECHA DE REPORTE	**DESCRIPCION DEL INCIDENTE O EVENTO**	**RESPONSABLE**	**ESTADO**

Anexo 6. RESUMEN ANALITICO RAE

TITULO	Diseño de Políticas para la Gestión de la información de la alcaldía de Montecristo Bolívar
AUTOR	Jesús David Díaz.
DIRECTOR/ASESOR	Christian Reynaldo Angulo.
AÑO ELABORACIÓN	2018
DESCRIPCIÓN	El trabajo de investigación presentado es un proyecto aplicado, realizado a una entidad estatal, este pretende apoyar los procesos de seguridad informática dentro de la organización, diseñando un sistema de políticas que permita reducir los riesgos y peligros a los que está expuesto la alcaldía Municipal de Montecristo Bolívar, respecto al manejo de la información.
CONTENIDO.	
La Alcaldía municipal de Montecristo desde sus inicios siempre ha manejado grandes cantidades de información confidencial relacionadas con los principales proyectos que de alguna forma benefician a la comunidad, en la reciente construcción de la edificación del palacio municipal se ha creado la infraestructura tecnológica del cual no se ha contado con los procesos de control para el manejo de la información. El problema radica que dentro de la organización se ha presentado desde meses anteriores fuga de información de manera inexplicable, el tráfico de información que se maneja en una de las dependencias de la misma ha generado pérdidas que han ocasionado grandes atrasos en los procedimientos internos de la alcaldía, del mismo modo muchos de los equipos que se encuentran conectados a la red interna han perdido información de la cual no se ha tenido certeza del porque no aparecen, equipos que de alguna forma se han ejecutado programas internos y han hecho que toda la información sea pérdida. El departamento administrativo de informática presenta una infraestructura de red del cual esta propenso a secuestro de información, ya que no posee las medidas	

de seguridad adaptadas para prevenir ataques externos que pretenden entrar y robar la información en los sistemas.

El Avance acelerado de la internet ha hecho que muchos delincuentes informáticos vulneren la SI de las empresas y en este caso se ha llegado a pensar si, **¿Se estarán recibiendo ataques externos a la infraestructura tecnológica de la alcaldía municipal?,** de cierta forma en cualquier momento se ha recibido cualquier indicio de esto, en las entidades públicas existe un alto grado de probabilidad de estar propenso a cualquier ataque que pueda generar daño a la organización.

Es por eso que viendo la necesidad que se viene presentando en la Alcaldía Municipal de Montecristo, la creación de un SGSI, que ayude a tener el control y el tráfico de datos que circulan en la red interna del departamento de informática de la organización evitando así la cibercriminalidad, Así mismo se plantea como propósito fundamental fortalecer la infraestructura tecnológica con los procesos de control necesarios para la protección tanto de la seguridad informática, como de la SI, adaptando medidas como la implantación de UTM, o una DZM de tal forma que se constituya en una alternativa para ayudar a superar todas estas deficiencias las cuales posee la alcaldía en estos momentos.

Se pretende y se proyecta la elaboración del sistema de gestión de SI, que brinde soluciones optimas y eficaces, con el fin de proteger la información interna de la alcaldía municipal, alcanzando a dar la certeza que la información y demás que se manejen a nivel interno en ellas sea totalmente confiable y estén totalmente protegidas.

METODOLOGIA DE INVESTIGACION.

La metodología del proyecto aplicado está enmarcada sobre las siguientes fases que contemplan una serie de procesos que van relacionados a la ejecución de cada una de las fases del proyecto:

ETAPA 1: Realizar informe para el levantamiento de información que permita hacer análisis de los riesgos que están presentes en la infraestructura tecnológica de la alcaldía municipal.

Actividades:

- ✓ Verificar la infraestructura tecnológica de la alcaldía municipal, con el fin de identificar los activos informáticos con las que esta cuenta.
- ✓ Realizar revisión de equipos y hojas de vidas de estos.
- ✓ Indagar información con funcionarios del área tecnológica, con la intención de conocer el estado de las máquinas que hacen parte de la entidad.

ETAPA 2: Definir los parámetros y políticas de seguridad que ayuden a disminuir los riesgos presentes en la alcaldía Municipal.

.

Actividades:

- ✓ Valorar los activos mediante la integridad, disponibilidad y confidencialidad de la información.
- ✓ Determinar y medir cuales son los peligros y vulnerabilidades a los que están expuestas los activos informáticos.
- ✓ Calcular el impacto y el riesgo de los activos en caso de que se materialice una amenaza, para que después analizados estos aspectos se puedan definir los parámetros y procesos de seguridad.

ETAPA 3: Proponer la implementación de procesos de control que pretendan minimizar y reducir los tipos de ataques que existen en la actualidad.

Actividades:

- Verificar cuales son los controles que existen para medir el nivel de amenazas, riesgos y vulnerabilidades.
- Inspeccionar la infraestructura tecnológica de la Alcaldía Municipal.
- Implementar técnicas por intermedio de sistemas que permitan controlar ataques realizados a nivel externo.

ETAPA 4: Plantear un gobierno de gestión de SI, para toda la organización que permita conservar la integridad, disponibilidad y confidencialidad de todos los activos de información.

Actividades:

- ✓ Realizar entrevistas con el personal de la alcaldía municipal, con el fin establecer las normas y procedimientos que no se encuentren documentados.

ETAPA 5: Diseñar e implementar el gobierno de SI, a toda la infraestructura municipal, que garantice la protección y conservación de los activos de información más valiosos que tiene la entidad.

Actividades:

- ✓ Definir el objetivo del diseño de políticas para la gestión de la información de la alcaldía de Montecristo.
- ✓ Determinar el alcance del SGSI.
- ✓ Determinar las Normas, Politicas y Procedimientos.

El desarrollo de este proyecto es realizado mediante la investigación de campo. Esta metodología se aplica sustrayendo datos e información de acuerdo con la realidad de la empresa. La extracción de esta información se ha hecho a través de la técnica de recolección de datos (Como entrevistas, encuestas, etc.).

CONCLUSIONES.

Gracias al levantamiento de la información que se llevó a cabo, se evidencia que la Alcaldía municipal de Montecristo presenta un nivel de riesgo alto, ya que no se cuentan con los procedimientos necesarios para la SI.

Actualmente se puede observar que esta alcaldía es muy vulnerable a ataques informáticos, desde hace muchos años no se ha contado con la implementación de normas de seguridad que permitan mitigar estas amenazas.

Con la implementación de diferentes metodologías entre ellas **MAGERIT**, se permite reducir los riesgos que tiene la entidad, ya que a través de esta se puede identificar los activos que están en riesgo, los cuales se van a preservar y que son fundamentales productividades de la organización.

Es de suma importancia realizar capacitación a todo el funcionario que hace parte de la planta de personal de la alcaldía en temas relacionados a la SI, se debe dejar claro que esta es de gran importancia a nivel organizacional, ya que su implementación ayuda a la productividad de la empresa.

Con la implementación de estas metodologías es importante la creación del manual de políticas de seguridad, a través de esta se puede dar la operación eficiente del diseño de políticas para la gestión de la información **DGPI.**

RECOMENDACIONES.

Implementar el Gobierno de SI, en los procesos que hacen parte de la alcaldía municipal.

Contra con un plan que sirva para controlar y proteger la SI, de la alcaldía municipal cuando se presenten amenazas ya sea internas o externas.

La Alcaldía Municipal debe iniciar un proceso de sensibilización al funcionario en base a los aspectos más relevantes de la SI.

Es importante que la entidad realice auditorias mínimo una vez al año en la gestión de SI.

Que se establezcan los perfiles y roles de acuerdo con la estructura organizacional de la alcaldía Municipal de Montecristo.

Recalcarles la importancia de este proyecto en la organización.

La alcaldía municipal debe establecer procedimientos y políticas de acuerdo a la ley 1581 de 2012, tratamiento de datos personales, de toda la información que está bajo la responsabilidad de la entidad.

Anexo 7. MATRIZ DE TRATAMIENTO DE LOS RIESGOS.

MATRIZ DE ANALISIS Y TRATAMIENTO DE RIESGOS

IDENTIFICACIÓN DE AMENAZAS, VULNERABILIDADES, ANALISIS DE RIESGOS, ESTRATEGIA DE CONTROLES Y PLAN DE TRATAMIENTO A APLICAR

INFORMACIÓN DE LOS ACTIVOS DE INFORMACION

GESTION DE RIESGOS: ANALISIS DE RIESGOS Y TRATAMIENTO DE LOS RIESGOS

Activos de Informacion	No. De Amenazas y Vulnerabilidades	Nombre del activo de información	VALORACIÓN DEL RIESGO DE LOS ACTIVOS	Amenazas Metodologia Magerit	Vulnerabilidades	Probabilidad de vulneración(1 Muy raro, 2 poco probable, 3 posible, 4 probable, 5 practicamente seguro)	Calculo del riesgo neto(Valoracion del riesgo * probabilidad de vulneración)	Criticidad neta (1 a 4 despreciable (d), 5 a 9 baja (B), 10 a 15 apreciable (a), 16 a 20 importante (i), 21 a 25 critico(C))	Calificación de Gestión(1 control no existe, 2 existe pero no efectivo, 3 efectivo pero no documentado, 4 efectivo y documentado)	Si la opción es 2 - 3 o 4 Indique el Control aplicado actual	Riesgo residual (riesgo neto dividido entre la calificación de gestión)	Criticidad residual (1 a 4 despreciable (d), 5 a 9 baja (B), 10 a 15 apreciable (a), 16 a 20 importante (i), 21 a 25 critico(C))	Niveles de aceptación del riesgo(1 a 5 aceptable (A), 6 a 15 moderado (M), 16 a 26 inaceptable(I))
[SW] SOFTWARE	3	[SW] SISTEMAS OPERATIVOS	11	[A] Ataques intencionados	Instalación de software no licenciado	1	11	A	1		11	A	M
[SW] SOFTWARE	4	[SW] OFFICE	8	[E2] Errores del administrador	Instalación de software no licenciado	2	16	I	1		16	I	I
[SW] SOFTWARE	5	[SW] BASES DE DATOS	20	[E2] Errores del administrador	Posible perdida de informacion	2	40	C	1		40	C	I
[SW] SOFTWARE	6	[SW] VIVANTO - VICTIMAS	20	[E2] Errores del administrador	Posible perdida de informacion	2	40	C	1		40	C	I
[SW] SOFTWARE	7	[SW] SOFTWARE ARSOFT-SALUD	20	[E2] Errores del administrador	Posible perdida de informacion	2	40	C	1		40	C	I
[SW] SOFTWARE	8	[SW] SISBENAPP-SISBEN	20	[E2] Errores del administrador	Posible perdida de informacion	2	40	C	1		40	C	I
[HW] EQUIPAMENTO INFORMÁTICO	9	[HW] SERVIDORES	16	[A] Ataques intencionados	Errores actualización hardware y software	4	64	C			0	D	A
[HW] EQUIPAMENTO INFORMÁTICO	10	[HW] COMPUTADORES	11	[E] Errores y fallos no intencionados	Errores actualización hardware y software	4	44	C	1		44	C	I
[HW] EQUIPAMENTO INFORMÁTICO	11	[HW] PORTATILES	11	[E] Errores y fallos no intencionados	Falla de suministro eléctrico	4	44	C	1		44	C	I
[HW] EQUIPAMENTO INFORMÁTICO	12	[HW] IMPRESORAS epson L375	11	[E] Errores y fallos no intencionados	Errores actualización hardware y software	2	22	C			0	D	A
[HW] EQUIPAMENTO INFORMÁTICO	13	[HW] ESCANERES	11	[E] Errores y fallos no intencionados	Errores actualización hardware y software	2	22	C	1		22	C	I
[COM] REDES DE COMUNICACIONES	14	[COM] SWITCHES	8	[E] Errores y fallos no intencionados	Errores de configuración	1	8	B	1		8	B	M
[COM] REDES DE COMUNICACIONES	15	[COM] ROUTERS	8	[E] Errores y fallos no intencionados	Errores de configuración	4	32	C	1		32	C	I
[COM] REDES DE COMUNICACIONES	16	[COM]PUNTOS DE ACCESO A LA RED	19	[E] Errores y fallos no intencionados	Errores de configuración	4	76	C	1		76	C	I
[D] DATOS	17	[D] DOCUMENTOS	16	[E] Errores y fallos no	Denegacion de Servicio	4	64	C	1		64	C	I
[Media] SOPORTE DE INFORMACIÓN	18	[MEDIA] INFORMACION DIGITAL	20	[E] Errores y fallos no intencionados	Modificación o destrucción de la información	4	80	C	1		80	C	I
[Media] SOPORTE DE INFORMACIÓN	19	[MEDIA] ADMINISTRADOR DBA	20	[E] Errores y fallos no intencionados	Modificación o destrucción de la información	3	60	C	1		60	C	I
[Media] SOPORTE DE INFORMACIÓN	20	[MEDIA]CORREOS ELECTRONICOS	12	[A] Ataques intencionados	Posible perdida de informacion	4	48	C	1		48	C	I
[L] INSTALACIONES	21	[L] CENTRO DE DATOS Y CABLEADO	17	[A] Ataques intencionados	Incendio	4	68	C	1		68	C	I
[P] PERSONAL	22	[P] EMPLEADOS	12	[E] Errores y fallos no	Indisponibilidad del personal	4	48	C	1		48	C	I

Anexo 8. DECLARACION DE APLICABILIDAD.

LOGO ALCALDÍA MONTECRISTO	DECLARACIÓN DE APLICABILIDAD ALCALDIA MUNICIPAL DE MONTECRISTO		Versión Formato
	VERSIÓN 2	ESTADO ORIGINAL	PÁG 1 DE 3

SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN BASADO EN LA NORMA ISO/IEC 27001:2013

Este documento contiene los numerales de la norma NTC-ISO/IEC 27001:2013 que aplican a (nombre compañía del grupo Thomas Greg & Sons) y las exclusiones de la misma, para efectos de implementar el Sistema de Gestión de Seguridad de la Información.

Numeral Norma	Objetivo	Control	Aplica Requisit	Justificación	Documento Referencia
A.5	POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN				
A.5.1	Orientación de la dirección para la gestión de seguridad de la información	A.5.1.1 Políticas para la seguridad de la información			
		A.5.1.2 Revisión de las políticas para seguridad de la información			
A.6	ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN				
A.6.1	Organización interna	A.6.1.1 Roles y responsabilidades de Seguridad de la información			
		A.6.1.2 Segregación de funciones			
		A.6.1.3 Contacto con las autoridades			
		A.6.1.4 Contacto con grupos de interés especial			
		A.6.1.5 Seguridad de la información en gestión de proyectos			
A.6.2	Dispositivos móviles y teletrabajo	A.6.2.1 Política para dispositivos móviles			
		A.6.2.2 Teletrabajo			
A.7	SEGURIDAD DE LOS RECURSOS HUMANOS				
A.7.1	Antes de asumir el empleo	A.7.1.1 Selección			
		A.7.1.2 Términos y condiciones del empleo			
A.7.2	Durante la ejecución del empleo	A.7.2.1 Responsabilidades de la Dirección			
		A.7.2.2 Toma de conciencia, educación y formación en la seguridad de la información			
		A.7.2.3 Proceso disciplinario			
A.7.3	Terminación y cambio de empleo	A.7.3.1 Terminación o cambio de responsabilidades de empleo			
A.8	GESTIÓN DE ACTIVOS				
A.8.1	Responsabilidad por los activos	A.8.1.1 Inventario de activos			
		A.8.1.2 Propiedad de activos			
		A.8.1.3 Uso aceptable de activos de información			
		A.8.1.4 Devolución de activos			
A.8.2	Clasificación de la información	A.8.2.1 Clasificación de la información			
		A.8.2.2 Etiquetado de la información			
		A.8.2.3 Manejo de activos			
Numeral Norma	**Objetivo**	**Control**	**Aplica Requisit**	**Justificación**	**Documento Referencia**
A.8.3	Manejo de los medios	A.8.3.1 Gestión de medios removibles			
		A.8.3.2 Disposición de los medios			
		A.8.3.3 Transferencia de medios físicos			
A.9	CONTROL DE ACCESO				
A.9.1	Requisitos del negocio para control de acceso	A.9.1.1 Política de control de acceso			
		A.9.1.2 Acceso a redes y a servicios en red			
A.9.2	Gestión de acceso de usuarios	A.9.2.1 Registro y eliminación de usuarios			
		[illegible]			
		A.9.2.3 Gestión de derechos de acceso privilegiado			
		A.9.2.4 Gestión de información de autenticación secreta de usuarios			
		A.9.2.5 Revisión de los derechos de acceso de usuarios			
		A.9.2.6 Retiro o ajuste de los derechos de acceso			
A.9.3	Responsabilidades de los usuarios	A.9.3.1 Uso de información de autenticación secreta			
A.9.4	Control de acceso a sistemas y aplicaciones	A.9.4.1 Restricción de acceso a información			
		A.9.4.2 Procedimiento de ingreso seguro			
		A.9.4.3 Sistema de gestión de contraseñas			
		A.9.4.4 Uso de programas utilitarios privilegiados			
		A.9.4.5 Control de acceso a códigos fuente de programas			
A.10	CRIPTOGRAFÍA				
A.10.1	Controles criptográficos	A.10.1.1 Política sobre el uso de controles criptográficos			
		A.10.1.2 Gestión de claves			
A.11	SEGURIDAD FÍSICA Y AMBIENTAL				
A.11.1	Áreas seguras	A.11.1.1 Perímetro de seguridad física			
		A.11.1.2 Controles de ingreso físicos			
		A.11.1.3 Seguridad de oficinas, recintos e instalaciones			
		A.11.1.4 Protección contra amenazas externas y ambientales			
		A.11.1.5 Trabajo en áreas seguras			

		A.11.1.6 Áreas de despacho y carga			
Numeral Norma	**Objetivo**	**Control**	**Aplica Requisit**	**Justificación**	**Documento Referencia**
A.11.2	Equipos	A.11.2.1 Ubicación y protección de los equipos			
		A.11.2.2 Servicios de suministro			
		A.11.2.3 Seguridad del cableado			
		A.11.2.4 Mantenimiento de equipos			
		A.11.2.5 Retiro de activos			
		A.11.2.6 Seguridad de equipos y activos fuera de las instalaciones			
		A.11.2.7 Disposición segura o reutilización de equipos			
		A.11.2.8 Equipos de usuario desatendido			
		A.11.2.9 Política de escritorio limpio y pantalla limpia			
A.12	**SEGURIDAD DE LAS OPERACIONES**				
A.12.1	Procedimientos operacionales y responsabilidades	A.12.1.1 Procedimientos de operación documentados			
		A.12.1.2 Gestión de cambios			
		A.12.1.3 Gestión de capacidad			
		A.12.1.4 Separación de los ambientes de desarrollo, pruebas, y operación			
A.12.2	Protección contra códigos maliciosos	A.12.2.1 Controles contra códigos maliciosos			
A.12.3	Copias de respaldo	A.12.3.1 Respaldo de la información			
A.12.4	Registro y seguimiento	A.12.4.1 Registro de eventos			
		A.12.4.2 Protección de la información de registro			
		A.12.4.3 Registros del administrador y del operador			
		A.12.4.4 Sincronización de relojes			
A.12.5	Control de software operacional	A.12.5.1 Instalación de software en sistemas operativos			
A.12.6	Gestión de la vulnerabilidad técnica	A.12.6.1 Gestión de las vulnerabilidades técnicas			
		A.12.6.2 Restricciones sobre la instalación de software			
A.12.7	Consideraciones de auditoría de sistemas de información	A.12.7.1 Controles de auditoría de sistemas de información			
Numeral Norma	**Objetivo**	**Control**	**Aplica Requisit**	**Justificación**	**Documento Referencia**
A.13	**SEGURIDAD DE LAS COMUNICACIONES**				
A.13.1	Gestión de seguridad de redes	A.13.1.1 Controles de redes			
		A.13.1.2 Seguridad de los servicios de red			
		A.13.1.3 Separación en las redes			
A.13.2	Transferencia de información	A.13.2.1 Políticas y procedimientos de transferencia de información			
		A.13.2.2 Acuerdos sobre transferencia de información			
		A.13.2.3 Mensajería electrónica			
		A.13.2.4 Acuerdos de confidencialidad o de no divulgación			
A.14	**ADQUISICIÓN, DESARROLLO Y MANTENIEMIENTO DE SISTEMAS**				
A.14.1	Requisitos de seguridad de los sistemas de información	A.14.1.1 Análisis y especificación de los requisitos de seguridad de la información			
		A.14.1.2 Seguridad de los servicios de las aplicaciones en redes públicas			
		A.14.1.3 Protección de transacciones de servicios de aplicaciones			
A.14.2	Seguridad en los procesos de desarrollo y de soporte	A.14.2.1 Política de desarrollo seguro			
		A.14.2.2 Procedimientos de control de cambios en sistemas			
		A.14.2.3 Revisión técnica de aplicaciones después de cambios en la plataforma de operación			
		A.14.2.4 Restricciones en los cambios a los paquetes de software			
		A.14.2.5 Principios de construcción de sistemas seguros			
		A.14.2.6 Ambiente de desarrollo seguro			
		A.14.2.7 Desarrollo contratado externamente			
		A.14.2.8 Pruebas de seguridad de sistemas			
		A.14.2.9 Prueba de aceptación de sistemas			
A.14.3	Datos de prueba	A.14.3.1 Protección de los datos de prueba			
A.15	**RELACIONES CON LOS PROVEEDORES**				
A.15.1	Seguridad de la información en las relaciones con los proveedores	A.15.1.1 Política de seguridad de la información para las relaciones con proveedores			
		A.15.1.2 Tratamiento de la seguridad dentro de los acuerdos con proveedores			
		A.15.1.3 Cadena de suministro de tecnología de información y comunicación			
Numeral Norma	**Objetivo**	**Control**	**Aplica Requisit**	**Justificación**	**Documento Referencia**

Numeral Norma	Objetivo	Control	Aplica Requisito	Justificación	Documento Referencia
A.15.2	Gestión de la prestación de servicios de proveedores	A.15.2.1 Seguimiento y revisión de los servicios de los proveedores			
		A.15.2.2 Gestión de cambios a los servicios de los proveedores			
A.16	GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN				
A.16.1	Gestión de incidentes y mejoras en la seguridad de la información	A.16.1.1 Responsabilidades y procedimientos			
		A.16.1.2 Reporte de eventos de seguridad de la información			
		A.16.1.3 Reporte de debilidades de seguridad de la información			
		A.16.1.4 Evaluación de eventos de seguridad de la información y decisiones sobre ellos.			
		A.16.1.5 Respuesta a incidentes de seguridad de la información			
		A.16.1.6 Aprendizaje obtenido de los incidentes de seguridad de la información			
		A.16.1.7 Recolección de evidencia			
A.17	ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN DE LA GESTIÓN DE CONTINUIDAD DE NEGOCIO				
A.17.1	Continuidad de seguridad de la información	A.17.1.1 Planificación de la continuidad de la seguridad de la información			
		A.17.1.2 Implementación de la continuidad de la seguridad de la información			
		A.17.1.3 Verificación, revisión y evaluación de la continuidad de la seguridad de la información			
A.17.2	Redundancias	A.17.2.1 Disponibilidad de instalaciones de procesamiento de información.			
A.17.1	Continuidad de seguridad de la información	A.17.1.1 Planificación de la continuidad de la seguridad de la información			
		A.17.1.2 Implementación de la continuidad de la seguridad de la información			
		A.17.1.3 Verificación, revisión y evaluación de la continuidad de la seguridad de la información			
A.17.2	Redundancias	A.17.2.1 Disponibilidad de instalaciones de procesamiento de información.			
A.18	CUMPLIMIENTO				
A.18.1	Cumplimiento de requisitos legales y contractuales	A.18.1.1 Identificación de la legislación aplicable y los requisitos contractuales			
		A.18.1.2 Derechos de propiedad intelectual			
		A.18.1.3 Protección de registros			
		A.18.1.4 Privacidad y protección de información de datos personales			
		A.18.1.5 Reglamentación de controles criptográficos			
A.18.2	Revisiones de seguridad de la información	A.18.2.1 Revisión independiente de la seguridad de la información			
		A.18.2.2 Cumplimiento con las políticas y normas de seguridad			
		A.18.2.3 Revisión del cumplimiento técnico			

Versión Declaración de Aplicabilidad:

Elaborado por: **Fecha de elaboración:**

Revisado por: **Fecha de revisión:**

Aprobado por: **Fecha de aprobación:**

Cargo:

SI-FOR-001 | Instructivo | Historial Cambios