MODELO PARA LA IMPLEMENTACIÓN DEL SISTEMA GENERAL DE SEGURIDAD INFORMATICA Y PROTOCOLOS DE SEGURIDAD INFORMÁTICA EN LA OFICINA TIC DE LA ALCALDÍA MUNICIPAL DE FUSAGASUGÁ, BASADOS EN LA GESTIÓN DEL RIESGO INFORMÁTICO

ANA MILENA PULIDO BARRETO
JENITH MARSELLA MANTILLA RODRIGUEZ

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA
ESCUELA DE CIENCIAS BÁSICAS TECNOLOGÍA E INGENIERÍA
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
FUSAGASUGA
2016

MODELO PARA LA IMPLEMENTACIÓN DEL SISTEMA GENERAL DE SEGURIDAD INFORMATICA Y PROTOCOLOS DE SEGURIDAD INFORMÁTICA EN LA OFICINA TIC DE LA ALCALDÍA MUNICIPAL DE FUSAGASUGÁ, BASADOS EN LA GESTIÓN DEL RIESGO INFORMÁTICO

ANA MILENA PULIDO BARRETO
JENITH MARSELLA MANTILLA RODRIGUEZ

Asesora:
YINA ALEXANDRA GONZÁLEZ SANABRIA

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA
ESCUELA DE CIENCIAS BÁSICAS TECNOLOGÍA E INGENIERÍA
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
FUSAGASUGA
2016

Nota de Aceptación

_____

_____

_____

_____

_____

_____

Firma del Presidente del Jurado

_____

Firma del Jurado

_____

Fusagasugá, Abril de 2016

DEDICATORIA

En primer lugar queremos dedicar nuestro trabajo a Dios, el creador de todas las cosas, quien nos bendice y nos ha dado sabiduría, fortaleza, paciencia, perseverancia y constancia en cada una de las metas que nos hemos propuesto.

De igual forma, a nuestros padres, a quienes les debemos todo lo que somos como seres humanos, por su amor, comprensión, guía y acompañamiento en cada etapa de nuestras vidas; a nuestras hijas, hermanos y esposos por su paciencia y amor incondicional para dedicar con disciplina este proyecto.

AGRADECIMIENTOS

Damos gracias primordialmente a Dios por bendecirnos cada día y desde el momento en que iniciamos la Especialización de Seguridad en Informática en la UNAD, porque nos ha dado inteligencia, sabiduría, paciencia, entendimiento, dedicación y la capacidad para ejercer este proyecto de grado de la mejor manera.

A nuestros Padres, hermanos, hijas y esposos por todo su apoyo, comprensión, confianza y por creer siempre en nuestras capacidades y motivarnos una vez más a conseguir un logro importante en la vida.

A la Alcaldía Municipal de Fusagasugá, a sus funcionarios y en especial a todo el equipo de trabajo de la Oficina de Tecnologías de la Información y las Comunicaciones, por su disposición, apoyo y compromiso para brindarnos la información necesaria para desarrollar este proyecto de grado.

Al ingeniero Julián Bernardo Salinas Díaz, Jefe de la Oficina de Tecnologías de la Información y las Comunicaciones, por autorizar y permitir aportar desde la Seguridad informática en un modelo de seguridad y privacidad de la información acompañado de protocolos y políticas de seguridad en beneficio y cumplimiento de la normatividad vigente para la Alcaldía Municipal de Fusagasugá, así como por brindar y disponer de su equipo de trabajo para desarrollar el proyecto cuando fue necesario.

A la Ingeniera Yina Alexandra González Sanabria, Asesora del proyecto de grado por parte de la UNAD, por indicar y aportar de manera significativa con su experiencia el desarrollo del proyecto, por disponer de espacios propicios para entender y apoyar con el conocimiento la aplicación de la metodología y actividades correctas para obtener los resultados de los objetivos propuestos.

TABLA DE CONTENIDO

Pág.

INDICE DE TABLAS

Pág.

INDICE DE FIGURAS

Pág.

GLOSARIO

Activo: En relación con la seguridad de la información, se refiere a cualquier información o elemento relacionado con el tratamiento de la misma (sistemas, soportes, edificios, personas…) que tenga valor para la organización. (ISO/IEC 27000).[1]

Amenazas: Causa potencial de un incidente no deseado, que puede provocar daños a un sistema o a la organización. (ISO/IEC 27000).

Análisis de Riesgo: Proceso para comprender la naturaleza del riesgo y determinar el nivel de riesgo. (ISO/IEC 27000).

Auditoría: Proceso sistemático, independiente y documentado para obtener evidencias de auditoria y obviamente para determinar el grado en el que se cumplen los criterios de auditoria. (ISO/IEC 27000).

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

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

Compromiso de la Dirección: Alineamiento firme de la Dirección de la organización con el establecimiento, implementación, operación, monitorización, revisión, mantenimiento y mejora del SGSI.

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

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

---

[1] MinTIC. Modelo de Sistema de Seguridad y Privacidad de la Información, Marzo de 2015, Glosario, Pág. 10.

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

Control: Las políticas, los procedimientos, las prácticas y las estructuras organizativas concebidas para mantener los riesgos de seguridad de la información por debajo del nivel de riesgo asumido. Control es también utilizado como sinónimo de salvaguarda o contramedida. En una definición más simple, es una medida que modifica el riesgo.

Declaración de aplicabilidad: Documento que enumera los controles aplicados por el Sistema de Gestión de Seguridad de la Información – SGSI, de la organización tras el resultado de los procesos de evaluación y tratamiento de riesgos y su justificación, así como la justificación de las exclusiones de controles del anexo A de ISO 27001. (ISO/IEC 27000)

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

Disponibilidad: Según [ISO/lEC 13335-1: 2004): característica o propiedad de permanecer accesible y disponible para su uso cuando lo requiera una entidad autorizada.[3]

Evaluación de riesgos: Según [ISO/lEC Guía 73:2002]: proceso de comparar el riesgo estimado contra un criterio de riesgo dado con el objeto de determinar la importancia del riesgo.

Evento: Según [ISO/lEC TR 18044:2004]: Suceso identificado en un sistema, servicio o estado de la red que indica una posible brecha en la política de seguridad de la información o fallo de las salvaguardas, o una situación anterior desconocida que podría ser relevante para la seguridad.

Evidencia: Información, registro o declaración de hechos, cualitativa o cuantitativa, verificable y basada en observación, medida o test, sobre aspectos relacionados con la confidencialidad, integridad o disponibilidad de un proceso o servicio o con la existencia e implementación de un elemento del sistema de seguridad de la información.

[3] Presidencia de la Republica. Manual de la política de seguridad para las Tecnologías de la Información y las Comunicaciones – TICS. Versión 5. Términos y definiciones. Pág. 4.

Gestión de incidentes de seguridad de la información: Procesos para detectar, reportar, evaluar, responder, tratar y aprender de los incidentes de seguridad de la información. (ISO/IEC 27000).

Gestión de riesgos: Proceso de identificación, control y minimización o eliminación, a un coste aceptable, de los riesgos que afecten a la información de la organización. Incluye la valoración de riesgos y el tratamiento de riesgos. Según [ISO/IEC Guía 73:2002]: actividades coordinadas para dirigir y controlar una organización con respecto al riesgo.

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

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

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

Ingeniería Social: En el campo de la seguridad informática, es la práctica de obtener información confidencial a través de la manipulación de usuarios legítimos ganando su confianza muchas veces. Es una técnica que pueden utilizar investigadores privados, criminales, delincuentes computacionales (conocidos como cracker) para obtener información, acceso o privilegios en sistemas de información que les permiten realizar algún acto que perjudique o exponga a la persona o entidad a riesgos o abusos.

Integridad: Mantenimiento de la exactitud y completitud de la información y sus métodos de proceso. Según [ISOIIEC 13335-1: 2004]: propiedad/característica de salvaguardar la exactitud y completitud de los activos.

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

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

ISO 17799: Código de buenas prácticas en gestión de la seguridad de la información adoptado por ISO transcribiendo la primera parte de BS7799. A su vez, da lugar a ISO 27002 por cambio de nomenclatura el 1 de Julio de 2007. No es certificable.

ISO 19011: "Guidelines for quality and/or environmental management systems auditing". Guía de utilidad para el desarrollo de las funciones de auditor interno para un SGSI.

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

ISO 27002: Código de buenas prácticas en gestión de la seguridad de la información (transcripción de ISO 17799). No es certificable. Cambio oficial de nomenclatura de ISO 17799:2005 a ISO 27002:2005 el 1 de Julio de 2007.

ISO 9000: Normas de gestión y garantía de calidad definidas por la ISO.

ISO/IEC TR 13335-3: "Information technology. Guidelines for the management of IT Security .Techniques for the management of IT Security." Guía de utilidad en la aplicación de metodologías de evaluación del riesgo.

ISO/IEC TR 18044: "Information technology. Security techniques. Information security incident management". Guía de utilidad para la gestión de incidentes de seguridad de la información.

ITIL IT: Infrastructure Library, es un marco de gestión de los servicios de tecnologías de la información.

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

Modelo Estándar de Control Interno MECI: Es una herramienta gerencial que tiene como fin servir de control de controles para que las entidades del Estado logren cumplir con sus objetivos institucionales y con el marco legal aplicable a ellas. Su última versión MECI 1000:2014.

No conformidad: Situación aislada que, basada en evidencias objetivas, demuestra el incumplimiento de algún aspecto de un requerimiento de control que

permita dudar de la adecuación de las medidas para preservar la confidencialidad, integridad o disponibilidad de información sensible, o representa un riesgo menor.

No repudio: Los activos de información deben tener la capacidad para probar que una acción o un evento han tenido lugar, de modo que tal evento o acción no pueda ser negado posteriormente.

Oficina TIC: Oficina de Tecnologías de la Información y las Comunicaciones de la Alcaldía de Fusagasugá, creada mediante el Decreto 273 de 2013.

PHVA Planear-Hacer-Verificar-Actuar: Por sus siglas en ingles PDCA Plan-Do-Check-Act, es Modelo de proceso basado en un ciclo continuo de las actividades de planificar (establecer el SGSI), realizar (implementar y operar el SGSI), verificar (monitorizar y revisar el SGSI) y actuar (mantener y mejorar el SGSI).

Plan de continuidad del negocio: Plan orientado a permitir la continuación de las principales funciones misionales o del negocio en el caso de un evento imprevisto que las ponga en peligro. (ISO/IEC 27000).

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

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

Plan de tratamiento de riesgos: Documento que define las acciones para gestionar los riesgos de seguridad de la información inaceptables e implantar los controles necesarios para proteger la misma. (ISO/IEC 27000).

Riesgo: Posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información. Suele considerarse como una combinación de la probabilidad de un evento y sus consecuencias. (ISO/IEC 27000).

Seguridad de la información: Preservación de la confidencialidad, integridad, y disponibilidad de la información. (ISO/IEC 27000). Según [ISO/IEC 27002:20005]: Preservación de la confidencialidad, integridad y disponibilidad de la información; además, otras propiedades como autenticidad, responsabilidad, no repudio, trazabilidad y fiabilidad pueden ser también consideradas.

Selección de controles: Proceso de elección de los controles que aseguren la reducción de los riesgos a un nivel aceptable.

Sistema de Gestión de Calidad: Un sistema de gestión de la calidad es una serie de actividades coordinadas que se llevan a cabo sobre un conjunto de elementos (recursos, procedimientos, documentos, estructura organizacional y estrategias) para lograr la calidad de los productos o servicios que se ofrecen al cliente, es decir, planear, controlar y mejorar aquellos elementos de una organización que influyen en satisfacción del cliente y en el logro de los resultados deseados por la organización. Para las entidades públicas como la Alcaldía de Fusagasugá lo rigen las normas NTC ISO 9001:2008 Norma Técnica Colombiana y NTC GP 1000:2009 Norma Técnica De Calidad en la Gestión Pública.

Sistema de Gestión de Seguridad de la Información SGSI: Conjunto de elementos interrelacionados o interactuantes (estructura organizativa, políticas, planificación de actividades, responsabilidades, procesos, procedimientos y recursos) que utiliza una organización para establecer una política y unos objetivos de seguridad de la información y alcanzar dichos objetivos, basándose en un enfoque de gestión y de mejora continua. (ISO/IEC 27000). Según [ISO/IEC 27001: 20005]: la parle de un sistema global de gestión que, basado en el análisis de riesgos, establece, implementa, opera, monitoriza, revisa, mantiene y mejora la seguridad de la información. (Nota: el sistema de gestión incluye una estructura de Organización, políticas, planificación de actividades, responsabilidades, procedimientos, procesos y recursos.)

Sistema Integrado MECI-Calidad del Alcaldía de Fusagasugá SIMCAF: Es el sistema de gestión que interrelaciona el Modelo Estándar de Control Interno MECI y el Sistema de Gestión de Calidad. A pesar de ello la Alcaldía cuenta de manera independiente con el Sistema de Gestión de Calidad, basado en la norma NTC ISO 9001:2008 Norma Técnica Colombiana y NTC GP 1000:2009 Norma Técnica De Calidad en la Gestión Pública; y el Modelo Estándar de Control Interno en su actualización a la versión MECI 1000:2014.[4]

Trazabilidad: Cualidad que permite que todas las acciones realizadas sobre la información o un sistema de tratamiento de la información sean asociadas de modo inequívoco a un individuo o entidad. (ISO/IEC 27000).

Vulnerabilidad: Debilidad de un activo o control que puede ser explotada por una o más amenazas. (ISO/IEC 27000).

[4] Alcaldía de Fusagasugá. Secretaria de Planeación, Sistema Integrado MECI-Calidad de la Alcaldía de Fusagasugá.

RESUMEN

En la actualidad el riesgo informático al que se expone las organizaciones, son tal vez una de las mayores preocupaciones de los empresarios. A medida que surge la innovación en nuevas tecnologías, surgen nuevos ataques informáticos que en ocasiones han logrado desestabilizar grandes compañías.

Al ser la información el activo más importante de la información, aun mayor para una entidad del estado, se debe realizar un análisis profundo de los riesgos a los que se ve expuesta y determinar cuáles son las medidas correctivas y preventivas que se deben realizar al interior de la organización, para garantizar los principios de la Seguridad de la Información: confidencialidad, integridad y disponibilidad.

Adicional y teniendo en cuenta que de acuerdo a la ley establecida para las Entidades Públicas, por reglamentación del ministerio de Tecnologías, se estableció la obligatoriedad de estas entidades en la implementación local de un Sistema General de Seguridad de la Información, basándose en lineamientos de Gobierno en Línea 2.0 y aplicándolo a través de metodología PHVA.

INTRODUCCIÓN

La Alcaldía Municipal de Fusagasugá es una entidad del estado, que tiene como principal actividad comercial prestar servicios a la comunidad, así como dar a conocer la oferta institucional según el Acuerdo 037 del 2012, con el objetivo que la población conozca y acceda a los beneficios brindados por el Gobierno Nacional y la Administración Municipal, para ejercer la participación ciudadana.

El Ministerio de Tecnologías de la Información y las Comunicaciones ha establecido dentro de la Ley 1341 de 2009 varios lineamientos entre ellos los relacionados con trámites y servicios en línea, así como también lo señala la estrategia de Gobierno en Línea, pero también ha diseñado un Modelo de Seguridad y Privacidad de la Información (MSPI) que busca que las entidades territoriales provean de sistemas de gestión de seguridad de la información (SGSI), teniendo en cuenta que dentro de la identificación de sus activos de información encontramos las sistemas de información y plataformas en línea, para lo cual la Administración Municipal de la Alcaldía de Fusagasugá debe fijar el compromiso institucional para dar aplicación e incluir la responsabilidad de todos niveles involucrados dentro de la entidad, de tal forma, que tengan claro los beneficios que se pueden obtener con una cultura organizacional enfocada a la seguridad, que permita basados en los riesgos informáticos identificados realizar una mejor gestión (lo cual incluye el análisis, la identificación de controles adecuados, su implementación, su medición y la mejora continua); de esta manera podrá contar con la aprobación y apoyo de los recursos necesarios a través de todas las etapas e instancias de los trámites y servicios en línea.

La Alcaldía de Fusagasugá, dentro de su Política Publica en Tecnologías de la Información y las Comunicaciones, aprobada mediante Acuerdo Municipal No. 044 de 2012, ha considerado dar cumplimiento dar cumplimiento a la Ley 1341 de 2009, lineamientos que ha dado el Ministerio de Tecnologías de la Información y las Comunicaciones, el Modelo de Seguridad y Privacidad de la Información y la Estrategia de Gobierno en línea en materia de Sistemas de Gestión de Seguridad de la información (SGSI), aplicando las fases del ciclo PHVA (Planear, Hacer, Verificar y Actuar), así como dar aplicación a los lineamientos del estándar NTC:ISO/IEC 27001, los cuales también se complementan con el Modelo Estándar de Control Interno (MECI) para las entidades públicas.

La Alcaldía de Fusagasugá también requiere del fortalecimiento de la infraestructura de tecnologías de la información para garantizar la responsabilidad y la orientación para preservar los pilares fundamentales de la seguridad de la

información como los son la CONFIDENCIALIDAD, INTEGRIDAD y DISPONIBILIDAD de la información y establecer un Modelo de Sistema de Gestión de Seguridad de la Información (SGSI) que le permita reunir la sostenibilidad y el conjunto de lineamientos, políticas, normas, procesos e Instituciones que proveen y promueven la puesta en marcha, supervisión, mejora y control, tal como lo señala el Modelo de Seguridad y Privacidad de la Información alineado con la Estrategia de Gobierno en Línea definida en manual GEL versión 3.0; teniendo en cuenta que la Oficina de Tecnologías de la Información y las Comunicaciones (Oficina TIC), brinda servicios de TI que deben ser gestionados y administrados, para lo cual se hace necesario contar con políticas, protocolos y procedimientos de seguridad de la información, que la entidad debe identificar por niveles de confidencialidad y custodia de la información pública, uso interno, restringido y reservado, en cumplimiento de la Ley 712 de 2015.

El Sistema de Desarrollo Administrativo centra su propósito en el mejoramiento permanente y planeado para la buena gestión y uso de los recursos y del talento humano en las entidades de la Administración Pública; es por ello que la Alcaldía de Fusagasugá cuenta con el Sistema de Gestión de la Calidad basado en la Norma Técnica de Calidad para la Gestión Pública NTC GP 1000:2009, para enfocar, dirigir y evaluar el desempeño institucional y el mejoramiento de la entidad. Adicional a esto la Alcaldía de Fusagasugá cuenta con el Sistema de Control Interno basado en el Modelo Estándar de Control Interno MECI 1000:2014, que orienta la configuración de estructuras de control de la planeación, la gestión, la evaluación y seguimiento para lograr que las entidades cumplan los objetivos institucionales propuestos y que se contribuya a la consecución de los fines esenciales del Estado, dentro de los que encontramos garantizar la seguridad y privacidad de la información.

1. PLANTEAMIENTO DEL PROBLEMA

1.1 ANTECEDENTES DEL PROBLEMA

En la actualidad la Oficina de Tecnologías de la Información y las Comunicaciones (Oficina TIC) de la Alcaldía del Municipio de Fusagasugá, no cuenta con un modelo de Seguridad General de Sistemas de la información, que le permita validar, supervisar, controlar y prevenir de ataques y delitos informáticos a los que puede ser objeto; no cuenta con un documento base que le permita garantizar la confidencialidad, integridad y disponibilidad de la información como uno de sus activos informáticos más importantes. Aun cuando la Ley 1341 de 2009, el Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC) y la Estrategia de Gobierno en línea establecen lineamientos para el Sistema de Gestión de Seguridad de la Información (SGSI) para las entidades públicas del orden territorial, la Alcaldía del Municipio de Fusagasugá no ha iniciado con la implementación del SGSI.

1.2 FORMULACIÓN DEL PROBLEMA

¿Cuenta la Alcaldía del Municipio de Fusagasugá, con un Modelo que le permita implementar un Sistema Gestión de Seguridad de la información y protocolos de Seguridad que contribuyan a la Oficina TIC a realizar una mejor gestión y control de los riesgos informáticos que han sido identificados por la entidad?.

1.3 DESCRIPCION O RESUMEN DEL PROBLEMA

La Alcaldía Municipal de Fusagasugá ha diseñado mediante su Modelo Estándar de Control Interno (MECI) y su Sistema de Gestión de Calidad, un Sistema Integrado de gestión y Calidad, mediante el cual ha realizado el análisis de riesgos informáticos; pero requiere dar solución a la gestión de los riesgos contando con una propuesta de un Modelo de Sistema de Gestión de Seguridad de la Información (SGSI) que pueda ser implementado junto con protocolos de seguridad que requiere la entidad para valorar y controlar los riesgos de acuerdo a la política de administración del riesgo que tenga establecida la organización. Como resultado del proyecto, la Oficina TIC de la Alcaldía de Fusagasugá podrá fortalecer la eficiencia gubernamental estableciendo políticas de seguridad, normas y reglas institucionales que formarán parte de las políticas de operación y acciones de seguridad de los procesos, además de dar cumplimiento a la Ley 1341 de 2009, lineamientos del Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC) y la Estrategia de Gobierno en Línea (GEL) en materia

de Sistemas de Gestión de Seguridad de la información (SGSI), basados en el Modelo de Sistema de Seguridad y Privacidad de la Información (MSPI) que ha fijado el

La entidad también podrá orientar la mejora continua del Sistema Integrado MECI-Calidad de la Alcaldía de Fusagasugá (SIMCAF) y la seguridad de la información de la entidad, aportando al cumplimiento de la normatividad vigente en Sistema de Gestión de Seguridad de la Información (SGSI) para las entidades públicas y parcialmente a futuros proyectos para certificarse con la norma ISO 27001.

2. JUSTIFICACION

En la actualidad el Centro Administrativo Municipal de la Alcaldía de Fusagasugá cuenta con una infraestructura tecnológica amplia, conformada por software, hardware, comunicaciones y más de 300 usuarios aproximadamente que utilizan equipos, tecnologías de la información, servicios tecnológicos como Internet, sistemas de información, plataformas tecnológicas en línea, entre otros; la infraestructura de TI (Tecnologías de la Información) es administrada por la Oficina TIC, por consiguiente, se considera importante que la entidad establezca acciones que garanticen la seguridad física y lógica de sus activos informáticos, protocolos y que le permita valorar los riesgos informáticos que han sido identificados bajo una política de administración del riesgo del Sistema de Gestión de Calidad y el Modelo Estándar de Control Interno (MECI), que permita emprender acciones de control y valoración del riesgo informático identificado y evaluado, con el fin contribuir a evitarlo, reducirlo, transferirlo, compartirlo o asumirlo.

Este proyecto se considera importante y prioritario ya que contribuye al fortalecimiento de los procesos, actividades y servicios que realiza la Oficina TIC de la Alcaldía de Fusagasugá, así como el cumplimiento de lineamientos del Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC), el Modelo de Seguridad y Privacidad de la Información (MSPI) que busca una vez implementado y con índice de madurez alto que la entidad inicie con el requerimiento del Sistema Administrativo de Seguridad de la Información para Gobierno en línea (SASIGEL), de esta manera se dará cumplimiento de los principios definidos en la Ley 1341 de 2009 y en la Estrategia de Gobierno en línea, que corresponden a la protección de la información del individuo y la credibilidad y confianza en Gobierno en línea. La Alcaldía Municipal de Fusagasugá contará con protocolos de seguridad y un Modelo para la implementación del Sistema Gestión de Seguridad de la información (SGSI), que estará alineado a la metodología del ciclo PHVA para realizar la implementación de un Sistema de Gestión de Seguridad de la Información que ha sido señalado en el manual de la estrategia de Gobierno en Línea (GEL) en su versión 3.0.

3. OBJETIVOS

3.1 OBJETIVO GENERAL

Entregar un Modelo para la implementación del Sistema de Gestión de Seguridad de la información y Protocolos de Seguridad Informática para la Oficina TIC de La Alcaldía Municipal de Fusagasugá, basados en la identificación previa de los riesgos informáticos por parte de la entidad.

3.2 OBJETIVOS ESPECÍFICOS

- Analizar los diferentes riesgos informáticos que actualmente se tienen identificados en la Oficina TIC de la Alcaldía de Fusagasugá.
- Establecer un modelo de Sistema Gestión de Seguridad de la información, con base en los riesgos informáticos identificados.
- Desarrollar un documento con los pasos para la implementación del modelo de Sistema de Gestión de Seguridad de la información, de acuerdo a los riesgos encontrados en la Oficina TIC de la Alcaldía de Fusagasugá.

4. ALCANCE

El alcance del proyecto inicia con el análisis de cada uno de los riesgos informáticos que han sido identificados por la Alcaldía de Fusagasugá, hasta el desarrollo de un documento con los pasos para la implementación del modelo de Sistema de Gestión de Seguridad de la información y Protocolos de Seguridad Informáticos, que le permitan a la Oficina TIC de la Alcaldía de Fusagasugá emprender acciones de control y valoración del riesgo informático identificado, así como el cumplimiento de la normatividad y lineamientos del Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC).

5. MARCO DE REFERENCIA

5.1. ESTADO DEL ARTE

5.1.1 Modelo de Seguridad Informática para Entidades Publica. Darly Ocampo de la Universidad Piloto de Colombia, en el artículo **Modelo de Seguridad de la Informac**ión para las Entidades Públicas del Estado Colombiano publicado en 2015[5], para optar por su grado de Especialista en Seguridad el cual se encuentra en la Biblioteca Virtual de la Universidad Piloto de Colombia, donde muestra la Legislación que lleva a que las diferentes Entidades Públicas del País, realicen la Implementación del Sistema General de Seguridad Informática, bajos los lineamientos establecidos por MinTIC en su programa "Gobierno en Línea". Muestra que dicha implementación se podrá realizar bajo el ciclo de vida PHVA (Planear, Hacer, Verificar y Actuar).

Finalmente explica el por qué, aunque el Decreto sugiere el uso de la NTC ISO/IEC 27001:2005, al haberse publicado la NTC ISO/IEC 27001:2013 es bueno que las entidades realicen la implementación basados en esta última, y en caso de que ya lo hubieran realizado o estén en el proceso, puedan realizar la respectiva transición y/o actualización.

5.1.2 Implementación del SGSI. En el año 2012, Johanna Buitrago, Diego Bonilla y Carol Murillo en su propuesta de Grado en la Universidad Escuela de Administración y Negocios Internacionales EAN titulada **Diseño de una metodología para la implementación del Sistema de Gestión de Seguridad de la Información - SGSI, en el sector de Laboratorios de Análisis Microbiológicos, basado en ISO 27001**[6], muestran los Riesgos más relevantes de su investigación y los métodos de control con los que se pueden tratar cada uno de estos, también sugieren que el Plan de verificación permitirá identificar si se está llevando a cabo el tratamiento correcto con cada uno de los riesgos y así poder tomar acciones preventivas y correctivas para los que no se estén tratando con su debida importancia.

Sugieren en su trabajo que la implantación del SGSI, se considera como un proceso dinámico, puesto que la implementación del mismo debe significar para la organización un objetivo en pro de la estabilidad y consolidación del Negocio. Así

[5] Universidad Piloto de Colombia: http://polux.unipiloto.edu.co:8080/00002024.pdf
[6] UNIVERSIDAD EAN: http://repository.ean.edu.co/bitstream/handle/10882/2692/MurilloCarol2012.pdf?sequence=1

mismo se deberán crear planes de acción con el fin de resolver los problemas que se presentan dentro de la organización.

5.1.3 Gestión de la Seguridad y Riesgo en TI. A través de su artículo publicado en la Universidad Piloto de Colombia en 2015 titulado **Gestión de la seguridad y el riesgo de TI**[7], Katherine Romero nos muestra la importancia de la Seguridad Informática en el mundo actual, no solo como el método de contrarrestar ataques, sino como el camino de mejora para cualquier organización. Una de las indicaciones que nos precisa es que para cualquier tipo de organización lo primero que se deberá implementar es el Gobierno de Tecnología, como plus para el negocio del que esta haga parte.

Ahonda en diferentes modelos y normas de Gestión de Riesgo en Seguridad Informática, hasta llegar finalmente a la NTC ISO/IEC 31000, de la cual nos muestra detalladamente las ventajas y herramientas que esta emplea a la hora de realizar el estudio de Riesgos y determinar cuál sería la mejor opción para poder implementar de manera correcta el Modelo de Seguridad Informática en cualquier organización.

5.1.4 Políticas de Seguridad Informática. En el trabajo de grado realizado en 2014 por el compañero Luis Patiño en la UNAD titulado **Propuesta de actualización, apropiación y aplicación de políticas de seguridad informática en una empresa corporativa, PROPOLSINECOR**[8], nos muestra como a través del análisis de Riesgo Informático de la empresa PROPOLSINECOR, la cual ya había implementado previamente su Sistema General de Seguridad Informática, presentaba déficit en las Políticas de la Seguridad.

A medida que avanza su investigación, pudo identificar las diferentes Políticas de Seguridad necesarias para la organización, buscando como resultado final el garantizar que cada uno de los procesos que contienen la información a salvaguardar puedan realizar su función de manera correcta.

5.2 MARCO CONCEPTUAL

5.2.1 Sistema de Información. "Un sistema de información (SI) puede ser cualquier combinación organizada de personas, hardware, software, redes de

[7]Universidad Piloto de Colombia: http://polux.unipiloto.edu.co:8080/00002222.pdf
[8]Universidad Nacional Abierta y a Distancia UNAD: http://repository.unad.edu.co/bitstream/10596/2742/1/12973210.pdf

comunicaciones y recursos de información que almacene, recupere, transforme y disemine información en la organización"

Las personas han confiado en los sistemas de información para comunicarse entre sí, mediante diferentes técnicas y medios desde los mismos orígenes de la civilización, ya sea a través de dispositivos físicos, instrucciones y procedimientos de procesamiento de la información, canales de comunicación o datos almacenados, y con sus diferentes presentaciones y grados de complejidad; hace parte misma de la esencia del hombre, ser recolector de conocimiento y razón, parte misma de su naturaleza, no siempre de forma tan sofisticada o eficiente, pero si, como elemento de la humanidad.

5.2.2 Sistema de Gestión de Seguridad de la Información (SGSI). Un SGSI es para una organización el diseño, implantación, mantenimiento de un conjunto de procesos para gestionar eficientemente la accesibilidad de la información, buscando asegurar la confidencialidad, integridad y disponibilidad de los activos de información minimizando a la vez los riesgos de seguridad de la información.[9]

5.2.3 ISO 27001. Es una norma internacional emitida por la Organización Internacional de Normalización (ISO) y describe cómo gestionar la seguridad de la información en una empresa. La revisión más reciente de esta norma fue publicada en 2013 y ahora su nombre completo es ISO/IEC 27001:2013. La primera revisión se publicó en 2005 y fue desarrollada en base a la norma británica BS 7799-2.

ISO 27001 puede ser implementada en cualquier tipo de organización, con o sin fines de lucro, privada o pública, pequeña o grande. Está redactada por los mejores especialistas del mundo en el tema y proporciona una metodología para implementar la gestión de la seguridad de la información en una organización.

También permite que una empresa sea certificada; esto significa que una entidad de certificación independiente confirma que la seguridad de la información ha sido implementada en esa organización en cumplimiento con la norma ISO 27001.

5.2.4 ISO 27004. ISO 27004 facilita una serie de mejores prácticas para poder medir el resultado de un SGSI basado en ISO 27001.El estándar concreta cómo configurar el programa de medición, qué parámetros medir, cuñando y cómo

[9] WIKIPEDIA, Sistema de gestión de la seguridad de la información, http://es.wikipedia.org/wiki/Sistema_de_gesti%C3%B3n_de_la_seguridad_de_la_informaci%C3%B3n

medirlos, y ayuda a las empresas a crear objetivos de rendimiento y criterios de éxito.

La medición de la seguridad aporta protección a los sistemas de la organización y da respuesta a las amenazas de la misma. A su vez expone que el tipo de medidas requeridas dependerá del tamaño y complejidad de la organización, de la relación coste beneficio y del nivel de integración de la seguridad de la información en los procesos de la propia organización.

La norma ISO27004 establece cómo se deben constituir estas medidas y cómo se deben documentar e integrar los datos obtenidos en el SGSI. Las etapas propuestas por ISO 27004 con el objetivo de medir la eficacia de la seguridad de la información son:

Selección procesos y objetos de medición: Las empresas deben definir lo que hay que medir y el alcance de la medida. Sólo se consideran en la medición los procesos bien documentados que son consistentes y repetibles. Objetos de medición puede ser el rendimiento de los controles o de procedimientos, el comportamiento del personal.

Definición de las líneas base: Los valores base que muestran el punto de referencia deben definirse para cada objeto que se está midiendo.

Recopilación de datos: Los datos deben ser dimensionales precisos y oportunos. Se pueden emplear técnicas automatizadas de recogida de datos para lograr una recolección estandarizada y presentar informes.

Desarrollo de un método de medición: Según ISO 27004, la secuencia lógica de operaciones se aplica en diversos atributos del objeto seleccionado para la medición. Se usan indicadores como fuentes de datos para mejorar el rendimiento de los programas de seguridad de la información.

Interpretación de los valores medidos: Mediante procesos y la tecnología para el análisis y la interpretación de los valores se deben identificar las brechas entre el valor inicial y el valor de medición real.

Comunicación de los valores de medición: Los resultados de medición del SGSI se comunicarán a las partes interesadas. Se puede hacer en forma de gráficos, cuadros de mando operacionales, informes o boletines de noticias.

La Plataforma Tecnológica ISOTools facilita la medición del rendimiento de los SGSI, siendo una herramienta simple y de fácil manejo.[10]

[10] ISO/IEC 27004 – Medición de la Seguridad de la Información, Disponible en: http://www.pmg-ssi.com/2014/01/isoiec-27004-medicion-de-la-seguridad-de-la-informacion/

5.3 MARCO LEGAL

5.3.1 Decreto 1151 de 2008. Decreto por el cual se establecen los lineamientos generales para la adopción de Gobierno en Línea para cada una de las Entidades de la Administración Publica en el territorio Nacional. Su objetivo principal es el de llevar a estas entidades a construir un estado más eficiente, transparente y participativo, dando a cada ciudadano las herramientas para conocer cada uno de los avances de su municipio, departamento o del país en general; así como la opción de que pueda obtener servicios a través de ellas.

5.3.2 Ley 1450 de 2011. Se creó con el fin de expedir el Plan Nacional de Desarrollo 2010 – 2014, dentro de esta en el Artículo 227. "Obligatoriedad de suministro de información." Parágrafo 3, establece que el Gobierno está en la obligación de garantizar al estado la implementación del Sistema General de Seguridad de la Información dando así el acceso a la información de manera segura y confiable y previniendo el uso adecuado de la misma.

5.3.3 Modelo de Seguridad y Privacidad de la Información – MinTIC. El Modelo de Seguridad y Privacidad de la Información fue diseñado como una estrategia de la Dirección de Estándares y Arquitectura de TI a través de la Subdirección de Seguridad y Privacidad de TI del Ministerio de Tecnologías de la Información y las comunicaciones (MinTIC), con el fin de reunir en este modelo el conjunto de lineamientos, políticas, normas, procesos e instituciones que proveen y promueven la puesta en marcha, supervisión, mejora y control de la implementación del modelo, así como a la implementación de la Estrategia de Gobierno en Línea, establecida en manual GEL; adicional a ello este modelo presenta la alineación con el Marco de Referencia de Arquitectura Empresarial para la Gestión de TI y la Estrategia de Gobierno en línea. También incluye la actualización del modelo de seguridad de la información para Gobierno en Línea (GEL), "Versión 2.0", plan de operación, modelo de madurez, entre otros.

De esta manera la entidad territorial en la construcción de un Estado más eficiente, más transparente y participativo, que preste los mejores servicios con la colaboración de toda la sociedad, mediante el aprovechamiento de las TIC, así mismo, trabajando en el fortalecimiento de la protección de la privacidad de los usuarios como parte de una estrategia de seguridad y privacidad en el país.

5.3.4 Modelo de Seguridad de la Información para la Estrategia de Gobierno en Línea 2.0 – MinTIC. En este documento el Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC), da a conocer las pautas de la Estrategia de Implementación del Sistema General de Seguridad de la Información (SGSI) en Entidades Públicas denominado Sistema Administrativo de Seguridad de la Información para Gobierno en línea – **SASIGEL**, aportando una guía paso a paso de las diferentes herramientas que se deben tener en cuenta para este fin, y mostrando como incorporar el ciclo PHVA en el proceso.

La adecuación de este Sistema ayudará al gobierno a realizar un seguimiento uniforme de las entidades Gubernamentales, y así poder determinar el avance de Infraestructura y Tecnológico con el que cuenta cada una de estas. Adicional aportara avance en la ejecución de Auditoria a cada una de estas.

6. MARCO METODOLOGICO

6.1 DISEÑO METODOLOGICO

El Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC) ha diseñado el Modelo de Seguridad y Privacidad de la Información (MSPI), el cual reúne el conjunto de lineamientos, políticas, normas, procesos e Instituciones que proveen y promueven la puesta en marcha, supervisión, mejora y control de la implementación de la Estrategia de Gobierno en Línea definida en manual de Gobierno en Línea (GEL) en su versión 3.0. El modelo está gestionado por el Sistema de Administración de Seguridad de la Información de Gobierno en línea (SASIGEL), y el modelo deber ser implementado en un sistema de gestión de seguridad de la información en cada entidad.

Teniendo en cuenta que la Alcaldía del Municipio de Fusagasugá es una entidad gubernamental del orden territorial y que la rige normatividad del Estado Colombiano, y de acuerdo a la metodologías usadas para Sistema de Gestión de Calidad que actualmente tiene implementado, se optó por utilizar la metodología del Ciclo PHVA (Planear, Hacer, Verificar y Actuar), conforme a lo establecido en el Sistema de Gestión de Seguridad de la Información (SGSI) para Gobierno en Línea que se encuentra alineada con la familia de estándares ISO/IEC 27000. Como resultado, la entidad contará con la alineación de su sistema, con los requisitos del Modelo de Seguridad y Privacidad de la Información (MSPI) y el manual Gobierno en Línea (GEL) versión 3.0 y entrará en el ciclo PHVA del SGSI. La metodología ha sido aprobada y apoyada por parte de los interesados en gestionar el proyecto, haciendo uso de la metodología propuesta se ejecutaran procesos y actividades con el fin de desarrollar el proyecto dentro de los tiempos, recursos, costos y estándares de calidad requeridos.

En este proyecto se adelantan estrategias para contribuir al fortalecimiento de los procesos, actividades y servicios que realiza la Oficina Tecnologías de la Información y las Comunicaciones (Oficina TIC), un modelo que le permite a la organización adelantar acciones que garanticen la seguridad de la información, implementar y/o ajustar los protocolos de seguridad señalados y establecer la política de seguridad para contribuir a la gestión de los riesgos informáticos identificados por la organización y asegurar la información.

Se optó por realizar como proyecto de grado esta monografía, teniendo en cuenta que el Ministerio de Tecnologías de la Información y las Comunicaciones

establece que las entidades públicas deben implementar un modelo de seguridad de la información alineado con la estrategia de Gobierno en Línea (GEL), sistemas de información, servicios tecnológicos y del uso y apropiación de los mismos. Un modelo de gestión que garantiza el valor estratégico de la capacidad y la inversión en tecnología realizada por el Estado, como una estrategia organizacional que incluye aspectos importantes como las Políticas de TI en cuanto a seguridad, información, acceso y uso; así como la Norma Técnica de Calidad para la Gestión Pública NTC-GP 1000:2009 y al Modelo Estándar de control interno MECI 1000:2014, entre otra normatividad concordante en seguridad de la información para las entidades públicas.

De otra parte la Estrategia de Gobierno en Línea (GEL) está definida en 6 componentes transversales en el Decreto 2693 de 2012, es considerada un eje estratégico del Buen Gobierno, porque procura un Estado más eficiente, más transparente y participativo que preste mejores servicios con la colaboración de toda la sociedad. En su elemento Transversal define que el estado debe entre otros aspectos implementar un sistema de gestión de Tecnologías de Información e implementar un Sistema de Gestión de Seguridad de la Información (SGSI).

El proyecto se ejecutó bajo las fases de la metodología del ciclo PHVA (Planear, Hacer, Verificar y Actuar), las cuales fueron ejecutadas de acuerdo a lo planteado en el cronograma de actividades.

6.1.1 Planear. Se definió en el ciclo PHVA la Planeación de todas las actividades del proyecto, el alcance, recursos comprometidos, así como la identificación de los interesados internos y externos que van a interactuar y ejercer alguna influencia sobre el resultado global del proyecto; así como el refinamiento de los objetivos, y el desarrollo de una línea de acción requerida para alcanzar dichos objetivos. También se analizaron los instrumentos normativos para apoyar el desarrollo del proyecto, el estado del arte, marco conceptual y normativo. Dentro de las actividades del proyecto se ejecutaron para la Fase Planear del ciclo PHVA las siguientes actividades:

- Análisis de Información
- Capacidades y recursos para el Proyecto
- Entrevistas con el personal de la Oficina TIC de la Alcaldía de Fusagasugá.
- Aplicación de encuestas a los funcionarios sobre Sistema de Gestión de Seguridad de la Información SGSI), política, protocolos de seguridad informática en la Alcaldía de Fusagasugá.
- Análisis de resultados de las encuestas aplicadas.

Identificación de Interesados: Interesados internos y externos que interactuaron y ejercieron alguna influencia sobre el resultado global del proyecto, así:

- Internos: Alcaldía de Fusagasugá
- Externos: Universidad Nacional Abierta y a Distancia - UNAD

6.1.2 Hacer. Se desarrollaron las actividades que en el ciclo PHVA que en el Hacer permitieron cumplir con los objetivos del proyecto y productos a entregar, así como el desarrollo de los protocolos de seguridad y el Modelo de implementación de un Sistema de Gestión de Seguridad de la Información (SGSI) para la Alcaldía de Fusagasugá, basados en la identificación de los riesgos informáticos suministrados por la organización, para lo cual se ejecutaron las siguientes actividades en Fase Hacer del ciclo PHVA:

- Análisis del Sistema Integrado de Gestión MECI-Calidad de la Alcaldía de Fusagasugá.
- Análisis del Proceso de Gestión TIC y el Sistema Gestión de Seguridad de la Información (SGSI).
- Análisis de la Administración del Riesgo Informático que han sido identificados por el proceso Gestión TIC de la Alcaldía de Fusagasugá.
- Selección de protocolos de seguridad requeridos por la Oficina TIC, de acuerdo a los riesgos informáticos.
- Modelo de Sistema Gestión de Seguridad de la Información (SGSI), en cumplimiento de la normatividad vigente para entidades públicas.

6.1.3 Verificar. Se coordinaron esfuerzos y se integraron actividades del proceso en la Fase Verificar del ciclo PHVA, en el que se efectuaron las revisiones y seguimiento de los protocolos de seguridad desarrollados y el Modelo de implementación de un Sistema de Gestión de Seguridad de la Información (SGSI) para la Alcaldía de Fusagasugá, en cumplimiento de la normatividad vigente y los objetivos del proyecto; así mismo se llevaron a cabo los ajustes requeridos

Se diseñó la ficha de control y seguimiento del proyecto, de tal forma que a medida que se avanzaba en cada actividad de acuerdo al cronograma fue posible generar la trazabilidad, hallazgos, evidencias y porcentaje de cumplimiento; esta herramienta de medición que permitió evaluar el avance de las actividades y generar acciones preventivas que aseguraron cumplir objetivos y plazos para el proyecto.

Dando cumplimiento al cronograma de actividades del proyecto, se ejecutaron para la Fase Verificar del ciclo PHVA las siguientes actividades:

- Validación de los protocolos de seguridad informática con el modelo Sistema Gestión de Seguridad de la Información (SGSI).
- Verificación de los protocolos de seguridad Informática estén alineados con los riesgos informáticos y el Sistema Gestión de Seguridad de la Información (SGSI).
- Ajustes requeridos en los protocolos de seguridad y en el modelo de Sistema Gestión de Seguridad de la Información (SGSI).
- Verificación del documento del proyecto con los productos entregables, de acuerdo a los objetivos planteados.

6.1.4 Actuar. Para la Fase Actuar del ciclo PHVA se generó como mejora continua para Sistema de Integrado de Gestión Mecí-Calidad de la Alcaldía de Fusagasugá, los resultados del proyecto (productos entregables), y el cumplimiento de la normatividad vigente en modelos de seguridad de la información. La entidad ahora cuenta con unos protocolos de seguridad y un Modelo que les permitirá analizar y viabilizar la implementación el Sistema de Gestión de Seguridad de la Información (SGSI) desarrollado en el proyecto, como parte de la gestión de los riesgos informáticos identificados por la entidad.

6.2 AREA DE CONOCIMIENTO

Gestión de la Seguridad Informática

6.3 AREA ESPECÍFICA

Gestión de Riesgo Informático

6.4 RECURSOS DISPONIBLES PARA EL PROYECTO

Recursos Humanos: Como primera medida se contó con la disposición, compromiso, dedicación y responsabilidad de las estudiantes, para realizar las actividades y tareas previstas para el proyecto, contando además con el apoyo del personal que hace parte de la Oficina de Tecnologías de la Información y las Comunicaciones (Oficina TIC) de la Alcaldía de Fusagasugá; y por otra parte se contó con el personal dispuesto a orientar el desarrollo del proyecto por parte de la

Universidad Nacional Abierta y a Distancia UNAD, asignado a tutores y la asesora del proyecto, referenciada en las portadas este documento.

Recursos Físicos: Se contó con la disponibilidad de infraestructura de TI que la Oficina de Tecnologías de la Información y las Comunicaciones (Oficina TIC) de la Alcaldía de Fusagasugá, autorizó pertinente para el desarrollo del proyecto. LA sede principal ubicada en la Calle 6 No.6-24 Centro Administrativo Municipal; también se contó con los espacios de residencia de cada una de las estudiantes, equipos de cómputo, impresoras, escáner, servicios de TI y teléfonos celulares para establecer comunicación entre las estudiantes.

Recursos Técnicos: Se hizo uso de las Tecnologías de la Información y las Comunicaciones, como servicios de Internet y en la nube.

Recursos Financieros: Cualquier costo de material u otros requeridos para el desarrollo del proyecto fue asumido con los recursos propios de las estudiantes.

Recursos Institucionales: UNAD, Alcaldía Municipal de Fusagasugá.

6.5 TECNICAS DE RECOLECCION DE INFORMACIÓN, POBLACION Y MUESTRA

TÉCNICAS DE RECOLECCIÓN DE INFORMACIÓN: Se utilizaron en el proyecto las siguientes técnicas para la recolección de información:

- *Revisión de Documentos:* La revisión de documentos permitió conocer la Alcaldía de Fusagasugá, así como revisar los documentos cualitativos y cuantitativos. Entre los documentos cualitativos se hallaron reportes, registros y formularios de captura de datos, y dentro los documentos cuantitativos se hallaron consultas, manuales de procedimiento y políticas.
- *Entrevistas*: Se diseñaron preguntas abiertas y cerradas para el personal de la Alcaldía de Fusagasugá.
- *Encuestas*: Se diseñaron cuatro (4) tipos de encuesta para obtener respuestas a interrogantes que fueron considerados importantes para el desarrollo del proyecto.

POBLACION: Funcionarios y Contratistas de las diferentes dependencias y oficinas de la Alcaldía de Fusagasugá.

MUESTRA: Para el desarrollo del proyecto se tomó como muestra aproximadamente el 10% de personas de cada grupo poblacional según la

encuesta o entrevista a aplicar, entre los que se encuentran funcionarios y contratistas de las dependencias y oficinas de la Alcaldía de Fusagasugá.

6.6 TECNICAS DE PROCESAMIENTO Y ANALISIS DE DATOS

Luego de la recolección de datos a través de encuestas o cuestionarios descritos, se dio comienzo a la fase esencial referida a la clasificación o agrupación de los datos con relación a cada variable, objetivo de estudio y su presentación conjunta.

Para el análisis de datos se tuvo en cuenta lo siguiente:

- *Validación y Edición:* En este proceso se verificaron las entrevistas realizadas de acuerdo a lo establecido. La meta de la validación fue exclusivamente detectar un fraude o falla del entrevistador en seguir las instrucciones claves para aplicar la entrevista o encuesta.
- *Codificación*: Se efectuó la verificación de errores del entrevistador y del entrevistado. El proceso de edición para las encuestas por escrito implicó una verificación manual de varios aspectos que se relacionaban con las respuestas, si estas fueron completas, si se presentaron patrones de salto o preguntas abiertas.
- *Introducción de datos:* Una vez validadas, editadas y codificadas las encuestas o cuestionarios, se procedió al proceso de introducción de datos, digitar los resultados obtenidos en un equipo de cómputo.
- *Tabulación y análisis estadísticos:* Los resultados de la encuesta fueron digitados de acuerdo a los datos y registros del entrevistador, y luego se tabularon los resultados de la encuesta.

TECNICAS: Se utilizaron las siguientes:

- *Tabla de frecuencia en un solo sentido:* La tabulación básica, que muestra el número de entrevistados e indican el porcentaje de aquellos que dieron cada posible respuesta a cada pregunta. Aquí se tuvo en cuenta el total de entrevistados, número de personas a quienes se hizo la pregunta en particular y número de personas que dieron respuesta a la pregunta.
- *Representación gráfica de los resultados:* Para las representaciones graficas de los datos y presentar los resultados se utilizaron las barras.

6.7 PRODUCTOS A ENTREGAR

Protocolos de seguridad informática y Modelo de Sistema de Gestión de Seguridad de la información (SGSI) para la Alcaldía Municipal de Fusagasugá.

7. FASE PLANEAR CICLO PHVA

7.1 ANÁLISIS INFORMACIÓN

El análisis realizado permitió identificar los proyectos de grado similares del orden nacional e internacional, como requisito del Estado del Arte e insumo de información primordial como antecedentes que aportan una guía fundamental para el desarrollo del actual proyecto. Adicional a ello fue el insumo para clarificar la normatividad que aplica para el proyecto y construir el marco legal y normativo.

También se solicitó información a la Oficina de Tecnologías de la Información y las Comunicaciones (Oficina TIC) de la Alcaldía de Fusagasugá, en aras de conocer y realizar un diagnóstico de la documentación de procedimientos, servicios de TI y activos informáticos. De esta manera de identificaron los protocolos requeridos para el modelo de seguridad informática.

7.2 CAPACIDADES Y RECURSOS DEL PROYECTO

El principal recurso del proyecto fue la información que dispone actualmente la Alcaldía de Fusagasugá, la disposición de la entidad para avanzar en el desarrollo del proyecto y la capacidad profesional de las estudiantes para dar cumplimiento al proyecto, para cual se contó con *Recursos Comprometidos* como los recursos materiales, físicos, financieros, e institucionales.

7.3 ENTREVISTA CON EL PERSONAL DE LA OFICINA TIC DE LA ALCALDÍA DE FUSAGASUGÁ

En la entrevista se dio a conocer al Jefe de la Oficina de Tecnologías de la Información y las Comunicaciones (Oficina TIC) de la Alcaldía de Fusagasugá y el parte del equipo de la Oficina TIC como el Líder de Proyectos, Líder de Soporte y Sistemas de Información y al Líder de Desarrollo e Innovación, todo lo relacionado con el proyecto, destacando los aspectos más importantes, así como el alcance y el recursos humano requerido por parte de la organización para que cumplir con los objetivos planteados.

Durante la reunión el Jefe de la Oficina TIC dio a conocer la estructura organizacional de la Alcaldía de Fusagasugá y manifestó que la Oficina de Tecnologías de la Información y las Comunicaciones (TIC) es una dependencia de orden directivo que depende directamente del Alcalde, también señaló que es la única Oficina de Tecnologías de la Información y las Comunicaciones de orden territorial en el departamento de Cundinamarca, lo que genera mayor

responsabilidad al ser un Municipio de cabecera en la provincia del Sumapaz, provincia que está conformada por 10 municipios en total.

También dio a conocer la importancia obtener un Modelo Guía para implementación de protocolos de seguridad informática y Sistema de Gestión de Seguridad de la información (SGSI) en la Alcaldía Municipal de Fusagasugá, ya que la entidad requiere una política de seguridad de la información, toda vez que la información es el activo más importante de la organización, adicional a ello porque es necesario dar cumplimiento a Modelo de Seguridad alineado con la Estrategia de Gobierno en Línea, como lineamientos de obligatoriedad para la entidades del orden nacional y territorial señalado por el Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC).

"En Colombia, las instituciones de seguridad se están vinculando a la Estrategia TI para aumentar la capacidad del Estado de enfrentar las amenazas informáticas, pues en el momento presenta grandes debilidades, pese a que existen iniciativas gubernamentales, privadas y de la sociedad civil que buscan contrarrestar sus efectos, no hay una coordinación interinstitucional apropiada. En 2011 en Colombia hubo más de 550 ataques exitosos a entidades del Estado, para 2013 los ataques se disminuyeron a +130."[11]

La Alcaldía de Fusagasugá, mediante el Acuerdo No. 044 de 2012, aprobó a través del Concejo Municipal la política pública *por medio del cual se crea la política pública de tecnologías de la información y las comunicaciones (TICS) "FUSAGASUGÁ DIGITAL: EJE DE LA REGIÓN INTELIGENTE",* mediante esta policía publica la Administración Municipal fomentará y facilitará el buen uso de las Tecnologías de la Información y Comunicación en la ciudadanía. El desarrollo de las estrategias de la política se fundamenta en los siguientes tres (3) aspectos como cadena de valor: Conectividad, Apropiación, Contenidos y Servicios; con cuatro líneas estratégicas Gobierno Digital, Educación Digital, Desarrollo Económico Digital y Turismo Digital. Para la ejecución de esta política pública la administración municipal promoverá, coordinará y/o ejecutará planes, programas y proyectos tendientes a garantizar el acceso, uso y apropiación de las Tecnologías de la Información y Comunicación en la educación, las empresas y la comunidad en general, incentivando el desarrollo de un Ecosistema Digital en el municipio (Infraestructura - Servicios - Aplicaciones - Usuarios).[12]

[11] MINTIC, Ministerio de Tecnologías de la Información y la Comunicaciones, Seguridad de TI, http://www.mintic.gov.co/gestionti/615/w3-propertyvalue-6206.html
[12] Oficina TIC, Alcaldía de Fusagasugá, http://fusagasugadigital.gov.co/descargas/acuerdoTIC.pdf

Figura 1. Organigrama Alcaldía de Fusagasugá

Fuente: Página web http://www.fusagasuga-cundinamarca.gov.co/publicaciones.php?id=37601

7.4 ENCUESTAS A LOS FUNCIONARIOS SOBRE SISTEMA DE GESTIÓN DE SEGURIDAD INFORMÁTICA (SGSI), POLÍTICA, PROTOCOLOS DE SEGURIDAD INFORMÁTICA EN LA ALCALDÍA DE FUSAGASUGÁ

Teniendo en cuenta la información recolectada en la entrevista, se diseñaron y aplicaron encuestas diferentes para algunas áreas importantes de la Alcaldía de Fusagasugá, como herramienta de medición y diagnóstico de los protocolos y políticas de seguridad en la organización; en la encuesta se tuvieron en cuenta criterios de apropiación, capacitación, difusión, conocimiento y perspectiva acerca de la implementación de políticas y protocolos de seguridad informática para la organización, así:

7.4.1 Muestra. Para la muestra se tomaron varias oficina o dependencias de la Alcaldía de Fusagasugá.

- Dirección de Gestión Humana, muestra 5 funcionarias. *Ver anexo 1. Encuestas gestión humana diligenciada en 5 folios.*
- Oficina de Control Interno, muestra 3 funcionarias. *Ver anexo 2. Encuestas gestión humana diligenciada en 5 folios.*
- Oficina TIC, muestra 10 funcionarios y contratistas. *Ver anexo 3. Encuestas gestión humana diligenciada en 5 folios.*
- Personal de la Alcaldía de Fusagasugá, muestra 30 de 265 personas. *Ver anexo 3. Encuestas gestión humana diligenciada en 5 folios.*

7.4.2 Resultado encuesta para personal de la Alcaldía de Fusagasugá. Se aplicó como herramienta de medición, una encuesta al personal de la Alcaldía de Fusagasugá, de acuerdo al siguiente objetivo.

Objetivo de la Encuesta: Identificar a través de la opinión de los trabajadores de la Alcaldía de Fusagasugá¸ las fortalezas y debilidades que se presentan actualmente dentro de la organización en cuanto a Seguridad de la Información.

Población estadística: 273 funcionarios de planta en los niveles asistencial, técnico, profesional y directivo.
Muestra: 30 funcionarios de planta en los diferentes niveles**.**
Fecha: Septiembre de 2015.

Tabla 1. Resultado encuesta aplicada a personal de la Alcaldía de Fusagasugá

ENUNCIADO	SI	NO	% Con ref. Muestra (30)
¿Considera adecuada la seguridad que se tiene en el correo corporativo de la organización?	**27**	3	90% SI
¿Considera suficiente el personal que actualmente se encuentra en la Oficina TIC de la organización?	**20**	10	66% SI
¿Conoce usted las normas de Seguridad Informática que tiene la Organización?	10	**20**	66% NO
¿Sabe a quién debe de reportar un incidente informático y de qué manera?	**27**	3	90% SI
¿Ha recibido capacitación y concientización sobre Seguridad Informática dentro de la organización?	6	**24**	80% NO
¿Cree que el nivel de Seguridad Informática dentro de la organización es el adecuado?	9	**21**	70% NO
¿Considera suficiente la Seguridad con la que cuenta el equipo que le ha sido asignado dentro de la organización?	11	**19**	63% NO
¿Al momento de su vinculación le fue entregado el manual de funciones del cargo y las políticas se Seguridad de la Información establecidas por la organización?	8	**22**	73% NO
¿Realiza copia de seguridad de la información que maneja en sus labores diarias de acuerdo a lo establecido en la organización?	10	**20**	66% NO
¿Maneja contraseñas Alfanuméricas para el acceso a la red?	**25**	5	83% SI
¿Le parece adecuado el tiempo de respuesta por parte de la Oficina TIC ante las incidencias técnicas reportadas?	**27**	3	90% SI

¿Es estable la conexión a la red de la organización?	11	**19**	63% NO
¿Conoce y aplica las normas establecidas por la organización Manual para el uso adecuado de la Infraestructura Tecnológica MA-GT-001?	9	**21**	70% NO
¿Cree usted que la organización debería invertir para la implementación de un Sistema de Gestión en Seguridad de la Información?	**26**	4	86% SI

Fuente: Anexo 4. Encuesta personal Alcaldía en pdf.

7.4.3 Resultado encuesta para personal de la Dirección de Gestión Humana. Se aplicó como herramienta de medición, una encuesta al personal de la Alcaldía de Fusagasugá, de acuerdo al siguiente objetivo.

Objetivo de la Encuesta: Identificar a través de la opinión de los trabajadores de la Alcaldía de Fusagasugá¸ las fortalezas y debilidades que se presentan actualmente dentro de la organización en cuanto a Seguridad de la Información.

Población estadística: 8 funcionarios de planta en los niveles asistencial, técnico, profesional y directivo.
Muestra: 5 funcionarios de planta en los diferentes niveles**.**
Fecha: Septiembre de 2015.

Tabla 2. Resultado encuesta aplicada a personal Dirección de Gestión Humana

ENUNCIADO	SI	NO	% Con ref. Muestra (5)
¿Considera adecuada la seguridad que se tiene en el correo corporativo de la organización?	**5**	0	100% SI
¿Conoce usted las normas de Seguridad Informática que tiene la Organización?	0	**5**	100% NO
¿Sabe a quién debe de reportar un incidente informático y de qué manera?	**4**	1	80% SI
¿Maneja contraseñas Alfanuméricas para el acceso a la red?	**5**	0	100% SI
¿Cree que el nivel de Seguridad de la información dentro de la organización es el adecuado?	**3**	2	60% SI
¿Le parece adecuado el tiempo de respuesta por parte de la Ofician TIC ante las incidencias técnicas reportadas?	**5**	0	100% SI
¿Es estable la conexión a la red de la organización?	2	**3**	60% NO
¿Considera suficientes las normas de Seguridad Informática dentro de organización?	2	**3**	60% NO

¿Existe un procedimiento de Selección del Personal y este cuenta con política de Seguridad de la Información?	0	**5**	100% NO
¿Al momento de la vinculación de personal se hace entrega del respectivo Manual de Funciones y Políticas de Seguridad de la Información establecidas por la organización?	1	**4**	80% NO
¿En la Capacitación de Inducción y Re inducción de personal se informa y ratifican las políticas de Seguridad de la Información establecidas por la organización?	0	**5**	100% NO
¿Dentro de los planes de capacitación anual de la organización se incluyen temas de Seguridad de la Información e Ingeniería Social para todo el personal?	0	**5**	100% NO
¿Dentro de los planes de capacitación anual de la organización se incluyen temas de Seguridad Informática y Certificaciones, para el personal de la Oficina TIC?	0	**5**	100% NO
¿Cree usted que la organización debería invertir para la implementación de un Sistema de Gestión en Seguridad de la Información?	**5**	0	100% SI

Fuente: Anexo 5. Encuesta Gestión Humana en pdf.

7.4.4 Resultado encuesta para personal de la Oficina de Control Interno. Se aplicó como herramienta de medición, una encuesta al personal de la Alcaldía de Fusagasugá, de acuerdo al siguiente objetivo.

Objetivo de la Encuesta: Identificar a través de la opinión de los trabajadores de la Alcaldía de Fusagasugá¸ las fortalezas y debilidades que se presentan actualmente dentro de la organización en cuanto a Seguridad de la Información.

Población estadística: 4 funcionarios de planta en los niveles asistencial, técnico, profesional y directivo.
Muestra: 3 funcionarios de planta en los diferentes niveles**.**
Fecha: Septiembre de 2015.

Tabla 3. Resultado encuesta aplicada a personal Oficina de Control Interno

ENUNCIADO	SI	NO	% Con ref. Muestra (3)
¿Considera adecuada la seguridad que se tiene en el correo corporativo de la organización?	**2**	1	66% SI
¿Conoce usted las normas de Seguridad Informática que tiene la Organización?	1	**2**	66% NO
¿Sabe a quién debe de reportar un incidente informático y de qué manera?	**2**	1	66% SI

¿Cree que el nivel de Seguridad de la información dentro de la organización es el adecuado?	**2**	1	66% SI
¿Le parece adecuado el tiempo de respuesta ante las incidencias técnicas del sistema por la Oficina TIC?	**3**	0	100% SI
¿Es estable la conexión a la red de la organización?	1	**2**	66% NO
¿Considera suficientes las normas de Seguridad informática dentro de organización?	0	**3**	100% NO
¿Existe dentro del Sistema Gestión de Calidad un procedimiento, manual u otro documento con política de Seguridad de la Información?	**2**	1	66% SI
¿Existe dentro del Modelo Estándar de Control Interno un procedimiento, manual u otro documento con política de Seguridad de la Información?	1	**2**	66% NO
¿Se encuentran identificados y valorados los Riesgos Informáticos que tiene la organización?	1	**2**	66% NO
¿La organización tiene establecido estrategias que permitan desarrollar e implementar políticas de Seguridad de la Información?	1	**2**	66% NO
¿Dentro del programa anual de auditorías internas de la organización se incluye el requerimiento de las normas en materia de Seguridad de la Información?	0	**3**	100% NO
¿Considera importante que el Sistema de Control Interno y Sistema de gestión de calidad de la organización deben incluir políticas de Seguridad de la información?	**3**	0	100% SI
¿Cree usted que la organización debería invertir para la implementación de un Sistema de Gestión en Seguridad de la Información?	**3**	0	100% SI

Fuente: Anexo 6. Encuesta Control Interno en pdf.

7.4.5 Resultado encuesta para personal de la Oficina TIC. Se aplicó como herramienta de medición, una encuesta al personal de la Alcaldía de Fusagasugá, de acuerdo al siguiente objetivo.

Objetivo de la Encuesta: Identificar a través de la opinión de los trabajadores de la Alcaldía de Fusagasugá¸ las fortalezas y debilidades que se presentan actualmente dentro de la organización en cuanto a Seguridad de la Información.

Población estadística: 14 servidores públicos en los niveles asistencial, técnico, profesional y directivo.
Muestra: 10 servidores públicos en los diferentes niveles**.**
Fecha: Septiembre de 2015.

Tabla 4. Resultado encuesta aplicada a personal Oficina TIC

ENUNCIADO	1 Muy Bajo	2 Bajo	3 Medio	4 Alto	5 Muy Alto	% Con ref. Muestra (10)
¿Qué tan adecuada es la seguridad que se tiene en el correo corporativo de la organización?			4	4	2	40% Medio 40% Alto
¿En qué nivel conoce usted las normas de Seguridad Informática que tiene la Organización?		2	6		2	60% Medio
¿Cuál considera que es el nivel de Seguridad de la información dentro de la organización?		4	3	3		40% Bajo
40¿Qué tan estable la conexión a la red de la organización?			4	2	4	40% Muy Alto 40% Medio
¿Cuál es el grado de infraestructura tecnológica con la que cuenta la organización, para garantizar la Seguridad de la Información?		4	5	1		50% Medio
¿Cómo considera la asignación de recursos para la implementación de Seguridad de la Información dentro de la organización?	3	2	3	1	1	30% Bajo 30% Medio
¿Qué tan satisfecho se siente con el plan de capacitación de la organización en cuanto a Seguridad de la Información?	2	2	3	3		30% Medio 30% Alto
¿Cuál es su nivel de conocimiento sobre Seguridad de la Información?			6	2	2	60% Medio
¿Qué tan suficientes son las normas de Seguridad dentro de organización?		2	6	2		60% Medio
¿Cuál es su nivel de conocimiento sobre Ingeniería Social?		5	1	2	2	50% Bajo
¿En qué nivel se encuentran identificados y valorados los Riesgos Informáticos que tiene la organización?		3	6		1	60% Medio
¿Con que frecuencia se realiza la implementación de proyectos que ayuden a mejorar la Seguridad de la Información dentro de la organización?		6	9	1		60% Bajo
¿Es satisfactorio el manejo de controles a los Riesgos Informáticos identificados en la organización?		5	3	2		50% Bajo
¿En qué grado considera que la política pública en TIC garantiza la seguridad de la información para la organización?		1	4	3	1	40% Media

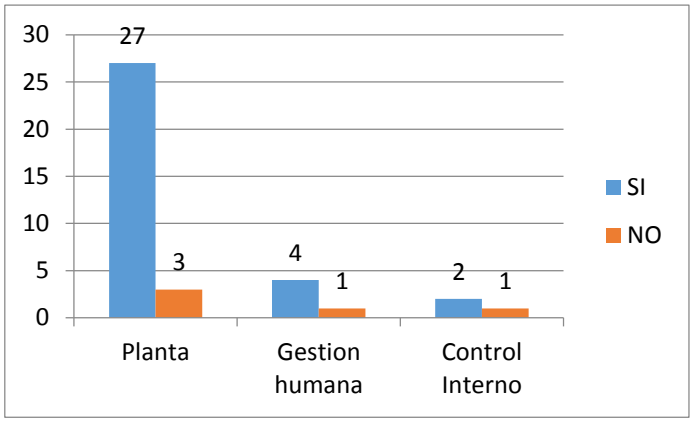
Fuente: Anexo 4. Encuesta Oficina TIC en pdf.

7.4.6 Análisis de resultados de las encuestas aplicadas. Luego de realizadas las encuestas a los diferentes dependencias de la Alcaldía Municipal de Fusagasugá, se ejecutó la respectiva tabulación y análisis de los resultados, exponiendo cuál es la tendencia de cada una de las preguntas. Para hacer un

censo general, se realizó la división de las mismas por cada pregunta comenzando por las que coincidían entre las áreas. Para esto se realiza la presentación de cada una de las preguntas que con las respuestas obtenidas:

A la pregunta **¿Sabe a quién debe de reportar un incidente informático y de qué manera?,** Se percibe que la mayor parte del personal de la Alcaldía conoce el conducto establecido por la Oficina TIC sobre el reporte de incidentes informáticos.

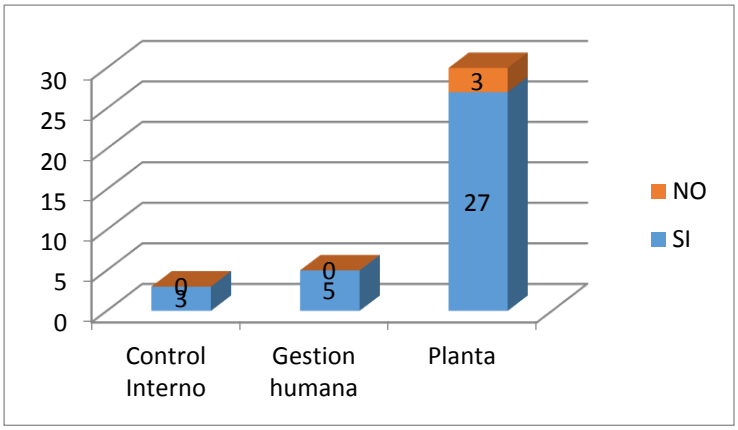
Figura 2. ¿Sabe a quién debe de reportar un incidente informático y de qué manera?



Fuente: El Autor

Para la Pregunta **¿Le parece adecuado el tiempo de respuesta por parte de la Ofician TIC ante las incidencias técnicas reportadas?,** La mayoría del personal de la Alcaldía siente que el tiempo de respuesta ante incidentes por parte de la Oficina de TIC es el adecuado.

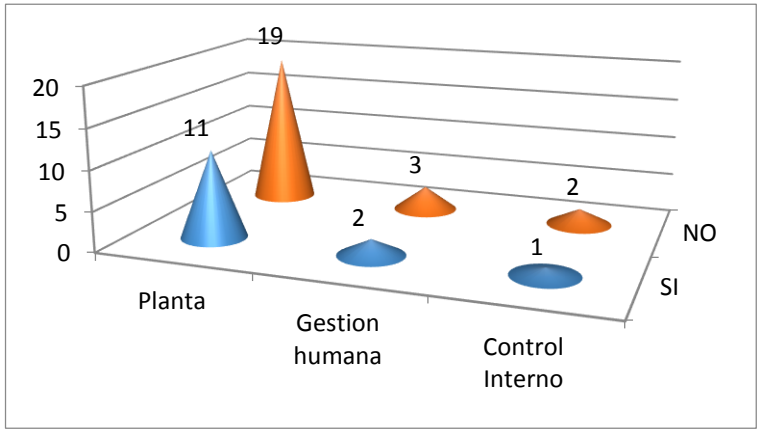
Figura 3. ¿Le parece adecuado el tiempo de respuesta por parte de la Ofician TIC ante las incidencias técnicas reportadas?



Fuente: El Autor

Para la pregunta **¿Es estable la conexión a la red de la organización?,** la mayor parte de los encuestados afirman que no es estable la conexión de la red, esto implica establecer mecanismos de seguridad que ayuden a mitigar estas fallas y que se pueda garantizar la continuidad de negocio.

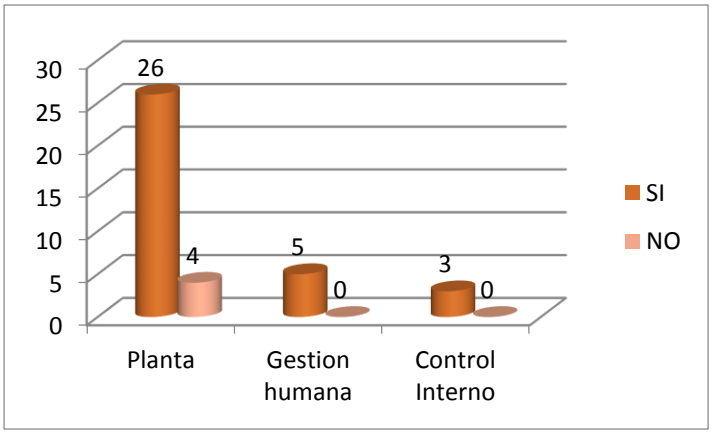
Figura 4. ¿Es estable la conexión a la red de la organización?



Fuente: El Autor

Para la pregunta **¿Cree usted que la organización debería invertir para la implementación de un Sistema de Gestión en Seguridad de la Información?,** El personal reitera que siente la falta de un sistema de seguridad de la Información.

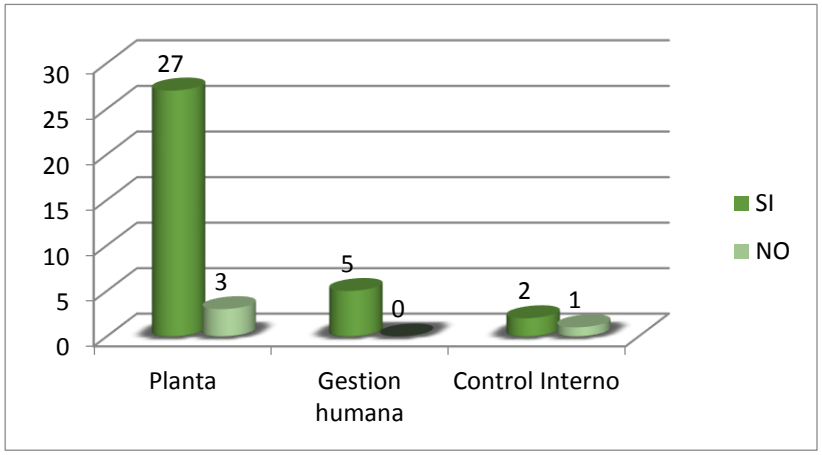
Figura 5. ¿Cree usted que la organización debería invertir para la implementación de un Sistema de Gestión en Seguridad de la Información?



Fuente: El Autor

Para la pregunta **¿Considera adecuada la seguridad que se tiene en el correo corporativo de la organización?,** el personal en general se siente satisfecho con la seguridad que se ha establecido para el manejo del correo corporativo el cual se encuentra contratado con Google.

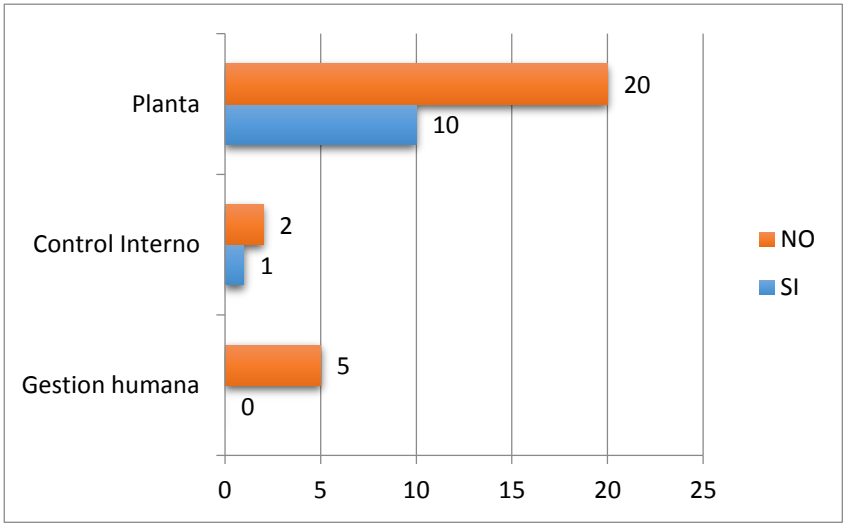
Figura 6. ¿Considera adecuada la seguridad que se tiene en el correo corporativo de la organización?



Fuente: El Autor

Para la Pregunta **¿Conoce usted las normas de Seguridad Informática que tiene la Organización?**, Se rarifica que uno de los puntos con mayor déficit es que el personal de la Alcaldía desconoce las normas de Seguridad Informática que están establecidas hasta el momento.

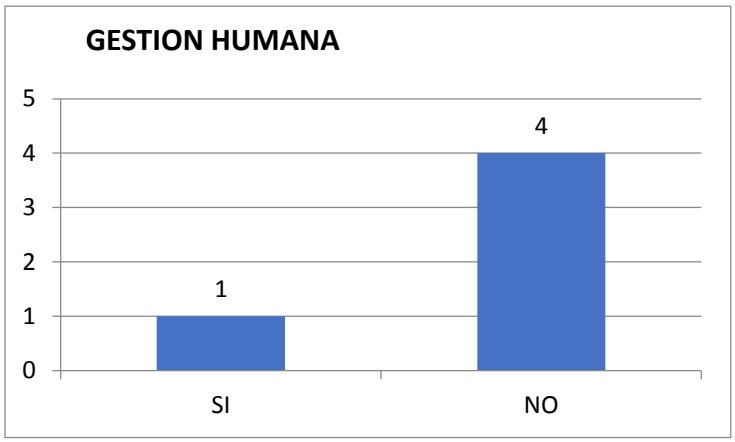
Figura 7. ¿Conoce usted las normas de Seguridad Informática que tiene la Organización?



Fuente: El Autor

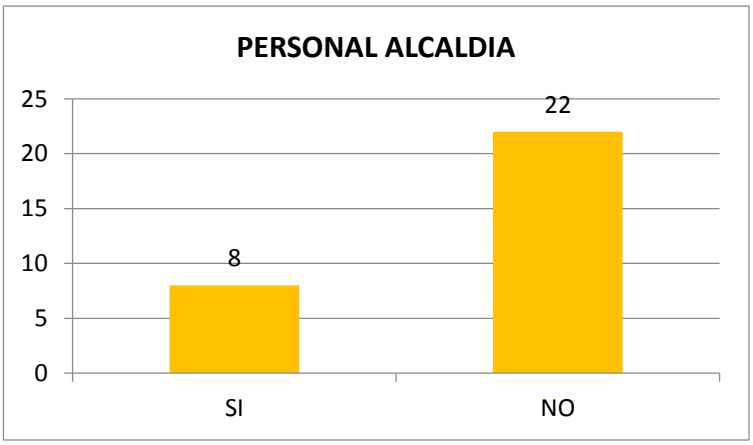
Para la pregunta **¿Al momento de la vinculación de personal se hace entrega del respectivo Manual de Funciones y Políticas de Seguridad de la Información establecidas por la organización?**, VS la pregunta **¿Al momento de su vinculación le fue entregado el manual de funciones del cargo y las políticas se Seguridad de la Información establecidas por la organización?**, Se puede evidenciar que en ambos casos la tendencia es que el área de Gestión Humana no realiza la entrega del respectivo manual de funciones al momento de las vinculaciones, generándose riesgo operativo, pues el personal no tiene claras las funciones y políticas de seguridad por las que se rige el cargo asignado.

Figura 8. ¿Al momento de la vinculación de personal se hace entrega del respectivo Manual de Funciones y Políticas de Seguridad de la Información establecidas por la organización?



Fuente: El Autor

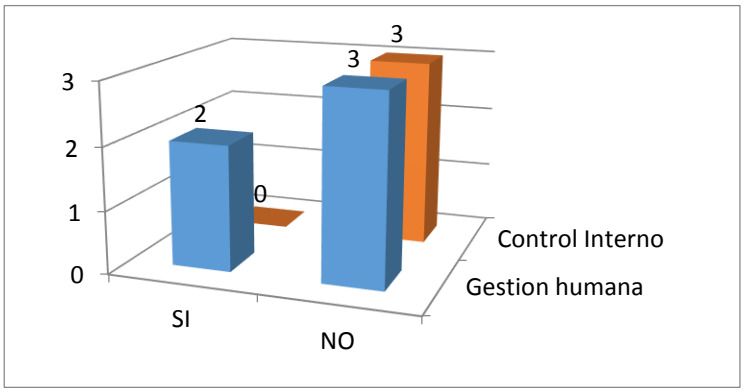
Figura 9. ¿Al momento de su vinculación le fue entregado el manual de funciones del cargo y las políticas se Seguridad de la Información establecidas por la organización?



Fuente: El Autor

Para la pregunta **¿Considera suficientes las normas de Seguridad Informática dentro de organización?,** las áreas de Control Interno y Gestión Humana consideran en su mayoría que existe un déficit en las normas que se encuentran implementadas en el momento.

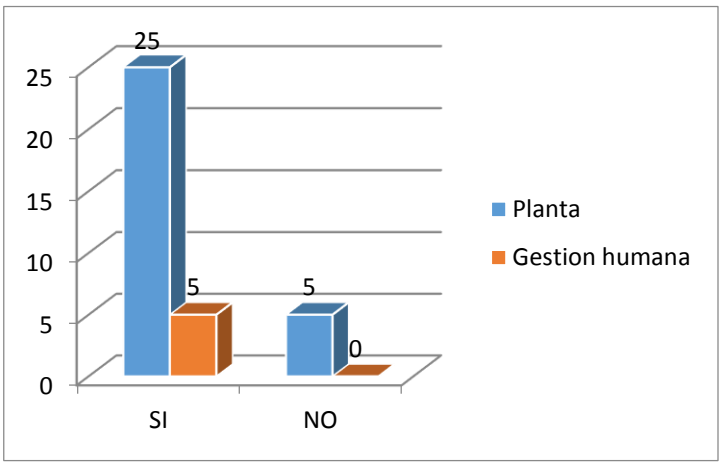
Figura 10. ¿Considera suficientes las normas de Seguridad Informática dentro de organización?



Fuente: El Autor

Para la Pregunta **¿Maneja contraseñas Alfanuméricas para el acceso a la red?,** La mayoría del personal encuestado afirma que si cuenta con contraseñas Alfanuméricas dentro de la red, sin embargo no existe una política implementada que realice el control y valide que en verdad se encuentren creadas de manera segura.

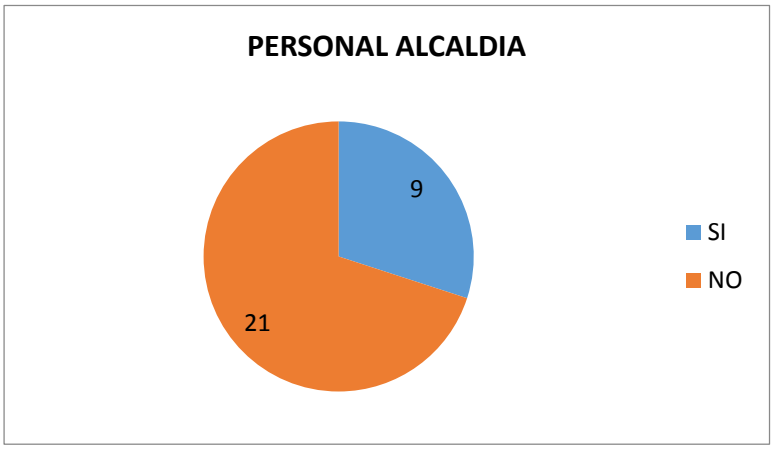
Figura 11. ¿Maneja contraseñas Alfanuméricas para el acceso a la red?



Fuente: El Autor

Para la pregunta **¿Conoce y aplica las normas establecidas por la organización Manual para el uso adecuado de la Infraestructura Tecnológica MA-GT-001?,** sigue prevaleciendo el déficit de no realizar la debida capacitación o socialización de los diferentes esquemas de Seguridad de Información que se han establecido dentro de la Alcaldía.

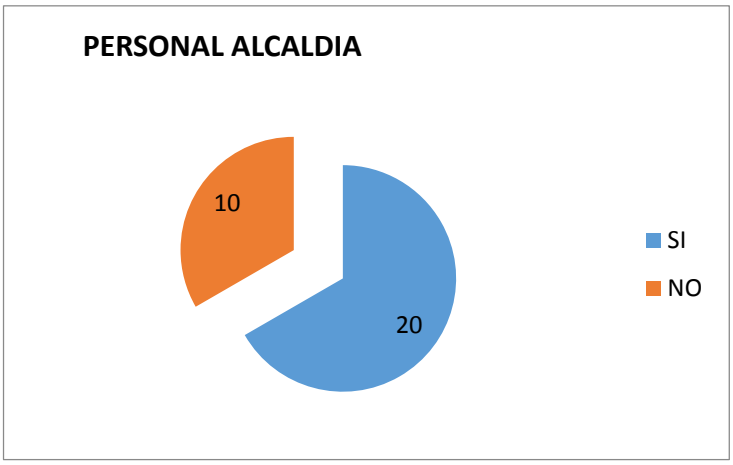
Figura 12. ¿Conoce y aplica las normas establecidas por la organización Manual para el uso adecuado de la Infraestructura Tecnológica MA-GT-001?



Fuente: El Autor

Para la pregunta **¿Considera suficiente el personal que actualmente se encuentra en la Oficina TIC de la organización?**, para la muestra de Personal de Alcaldía a la que se le aplico la encuentra prevalece la respuesta Si, considerándose suficiente el personal de la oficina TIC.

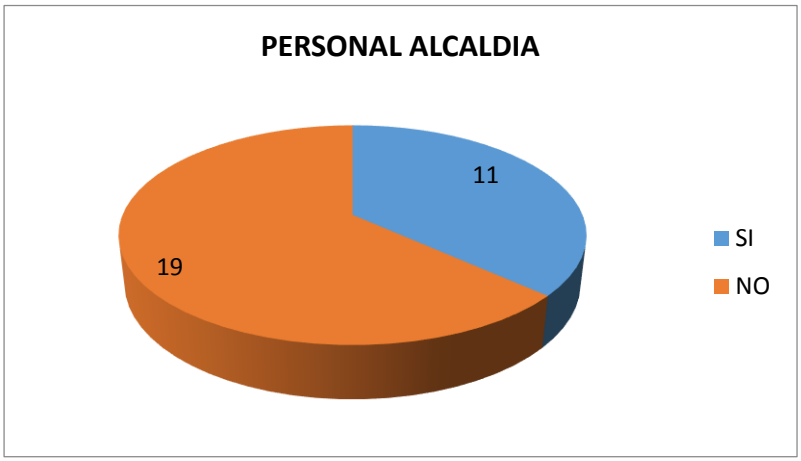
Figura 13. ¿Considera suficiente el personal que actualmente se encuentra en la Oficina TIC de la organización?



Fuente: El Autor

Para la pregunta **¿Considera suficiente la Seguridad con la que cuenta el equipo que le ha sido asignado dentro de la organización?,** para la muestra de Personal de Alcaldía a la que se le aplico la encuentra prevalece la respuesta No, por lo cual surge la necesidad de establecer mejoras a la seguridad que se encuentra actualmente en los equipos.

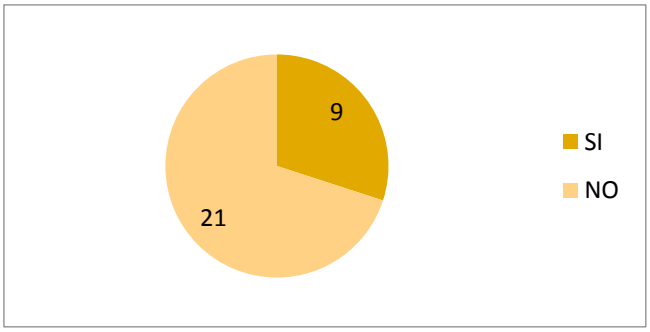
Figura 14. ¿Considera suficiente la Seguridad con la que cuenta el equipo que le ha sido asignado dentro de la organización?



Fuente: El Autor

Para la pregunta **¿Cree que el nivel de Seguridad Informática dentro de la organización es el adecuado? ,** para la muestra de Personal de Alcaldía a la que se le aplico la encuentra prevalece la respuesta No, identificándose que el personal sabe que se necesitan implementar muchas más medidas de Seguridad para respaldar la información.

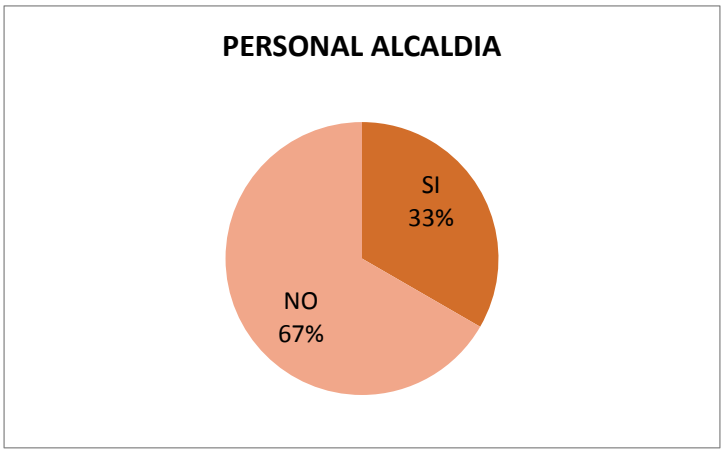
Figura 15. ¿Considera suficiente la Seguridad con la que cuenta el equipo que le ha sido asignado dentro de la organización?



Fuente: El Autor

Para la pregunta **¿Realiza copia de seguridad de la información que maneja en sus labores diarias de acuerdo a lo establecido en la organización?,** la mayor parte del personal de planta afirma que no realiza copia alguna de la información.

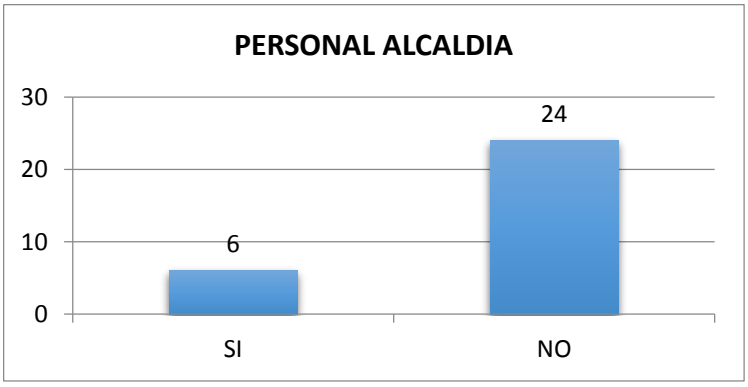
Figura 16. ¿Considera suficiente la Seguridad con la que cuenta el equipo que le ha sido asignado dentro de la organización?



Fuente: El Autor

Para la pregunta **¿Ha recibido capacitación y concientización sobre Seguridad Informática dentro de la organización?**, Se puede evidenciar que el personal de la Alcaldía es consciente de que no ha sido capacitado en los temas de Seguridad de la Información y desconoce el riesgo del mal manejo de la información al que se está sometiendo la Alcaldía.

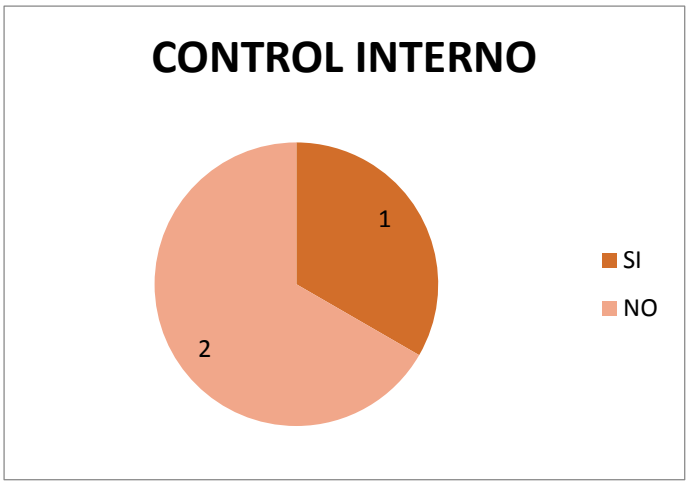
Figura 17. ¿Ha recibido capacitación y concientización sobre Seguridad Informática dentro de la organización?



Fuente: El Autor

Para la Pregunta **¿La organización tiene establecido estrategias que permitan desarrollar e implementar políticas de Seguridad de la Información?**, Se carece de propuestas de políticas de Seguridad por parte de las áreas encargadas para la Seguridad de la Información.

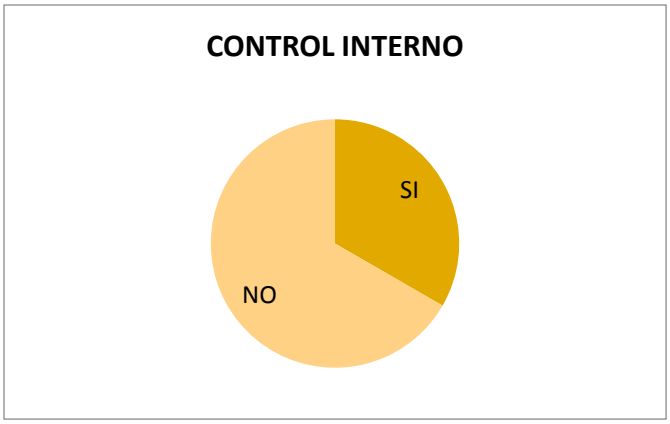
Figura 18. ¿La organización tiene establecido estrategias que permitan desarrollar e implementar políticas de Seguridad de la Información?



Fuente: El Autor

A la pregunta **¿Se encuentran identificados y valorados los Riesgos Informáticos que tiene la organización?,** Se identifica que Control Interno no tiene la identificación y respectiva valoración de los diferentes riesgos a los que actualmente se encuentra expuesta la Alcaldía.

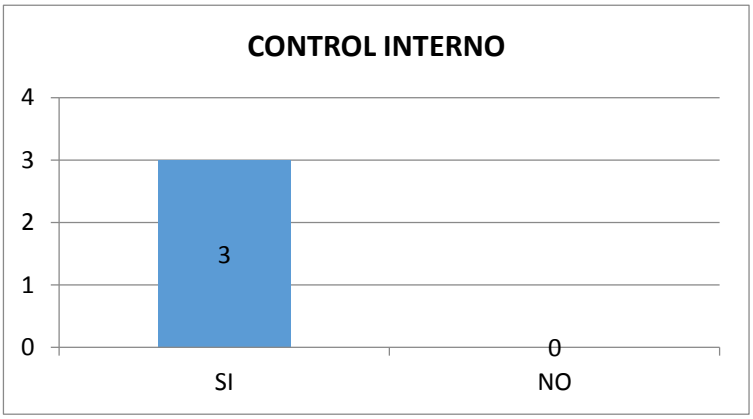
Figura 19. ¿Se encuentran identificados y valorados los Riesgos Informáticos que tiene la organización?



Fuente: El Autor

Para la pregunta **¿Considera importante que el Sistema de Control Interno y Sistema de gestión de calidad de la organización deben incluir políticas de Seguridad de la información?**, Se evidencia que el Área de Control Interno reconoce la necesidad de implementar políticas de Seguridad para los sistemas que se manejan dentro del área.

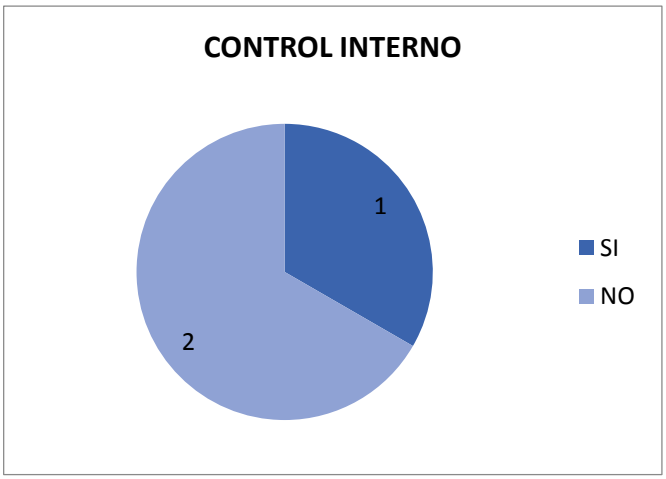
Figura 20. ¿Considera importante que el Sistema de Control Interno y Sistema de gestión de calidad de la organización deben incluir políticas de Seguridad de la información?



Fuente: El Autor

Para la pregunta **¿Existe dentro del Modelo Estándar de Control Interno un procedimiento, manual u otro documento con política de Seguridad de la Información?**, La falta de políticas en Seguridad de la Información, puede ocasionar incidentes de gran magnitud y que pueden llevar a un desequilibrio de la organización como tal.

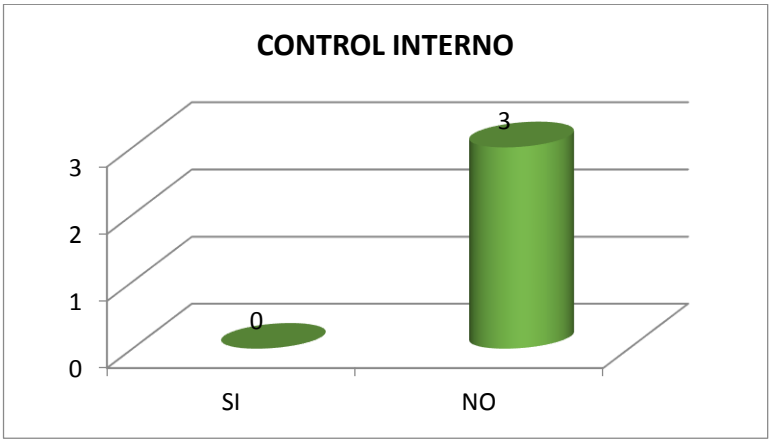
Figura 21. ¿Existe dentro del Modelo Estándar de Control Interno un procedimiento, manual u otro documento con política de Seguridad de la Información?



Fuente: El Autor

Para la pregunta **¿Dentro del programa anual de auditorías internas de la organización se incluye el requerimiento de las normas en materia de Seguridad de la Información?**, El área de Control Interno reconoce el hecho de que hasta el momento los temas concernientes a Seguridad de la información no hacen parte de las auditorias que ellos adelantan, esto explica el hecho de que muchos de los riesgos a los que se expone la Alcaldía a la fecha no han sido identificados, valoras y/o tratados.

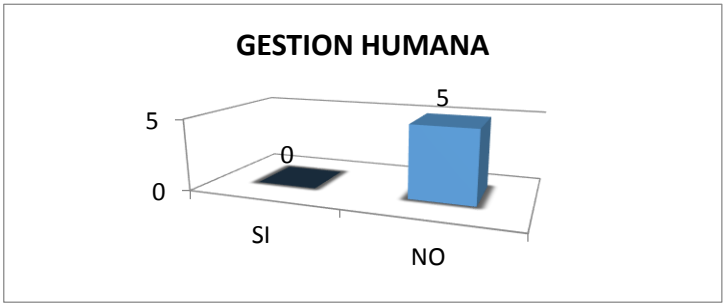
Figura 22. ¿Dentro del programa anual de auditorías internas de la organización se incluye el requerimiento de las normas en materia de Seguridad de la Información?



Fuente: El Autor

Para la pregunta **¿Dentro de los planes de capacitación anual de la organización se incluyen temas de Seguridad de la Información e Ingeniería Social para todo el personal?,** el área de Gestión humana reconoce el que no se está llevando a cabo ningún tipo de capacitación donde se instruya al personal sobre cómo resguardar la información dentro y fuera del trabajo y a su vez de incentivar al cuidado de esta.

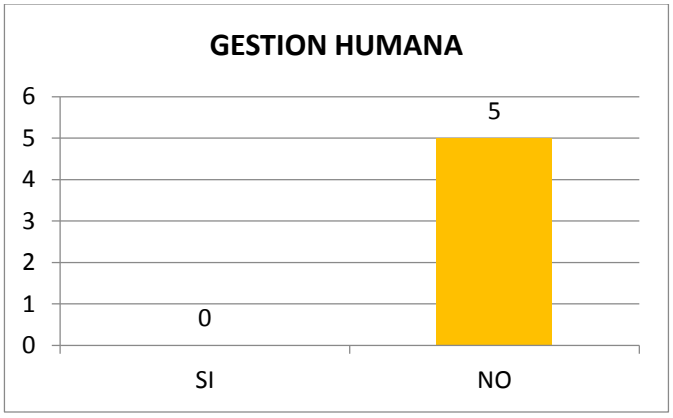
Figura 23. ¿Dentro del programa anual de auditorías internas de la organización se incluye el requerimiento de las normas en materia de Seguridad de la Información?



Fuente: El Autor

Para la pregunta **¿Dentro de los planes de capacitación anual de la organización se incluyen temas de Seguridad Informática y Certificaciones, para el personal de la Oficina TIC?**¸una vez se ve el déficit de capacitación, mas con la oficina de TIC, los cuales dentro de sus funciones está el implementar y supervisor las normas de Seguridad de la Información.

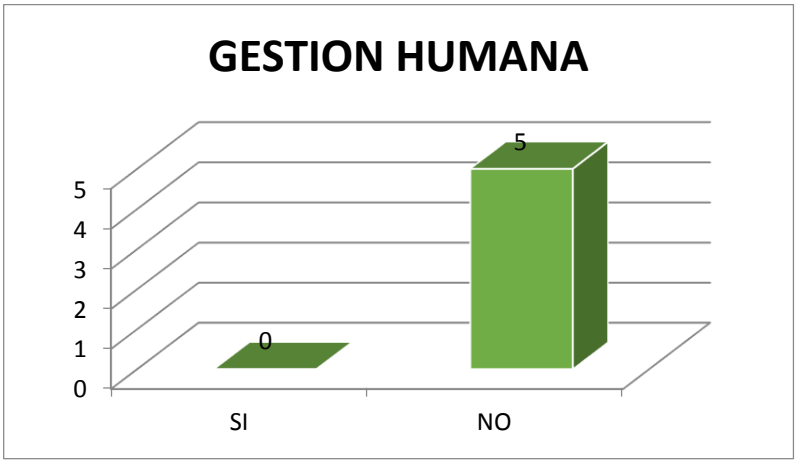
Figura 24. ¿Dentro de los planes de capacitación anual de la organización se incluyen temas de Seguridad Informática y Certificaciones, para el personal de la Oficina TIC?



Fuente: El Autor

Para la pregunta **¿En la Capacitación de Inducción y Re inducción de personal se informa y ratifican las políticas de Seguridad de la Información establecidas por la organización?**, El desconocimiento de las políticas de Seguridad de la información por parte de los funcionarios, genera un riesgo latente de Fraude dentro de la Alcaldía.

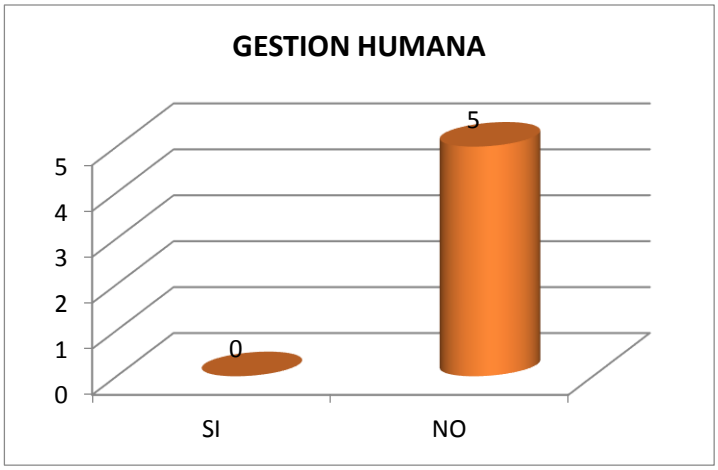
Figura 25. ¿En la Capacitación de Inducción y Re inducción de personal se informa y ratifican las políticas de Seguridad de la Información establecidas por la organización?



Fuente: El Autor

Para la pregunta **¿Existe un procedimiento de Selección del Personal y este cuenta con política de Seguridad de la Información?**, Se puede identificar otro gran riesgo al que se ve expuesta la Alcaldía por falta de tener establecidos los pasos y lineamientos al momento de contratación de personal.

Figura 26. ¿Existe un procedimiento de Selección del Personal y este cuenta con política de Seguridad de la Información?



Fuente: El Autor

8. FASE HACER CICLO PHVA

8.1 ANÁLISIS DEL SISTEMA INTEGRADO MECI-CALIDAD DE LA ALCALDÍA DE FUSAGASUGÁ

La Alcaldía del Municipio de Fusagasugá cuenta con un Sistema Integrado MECI-Calidad para dar cumplimiento a la normatividad Norma Técnica de Calidad para la Gestión Pública NTC-GP 1000:2009 y el Modelo Estándar de Control Interno MECI 1000:2014, lineamientos para las entidades públicas del orden nacional, departamental y territorial. Bajo este entendido se diseñó el Sistema de Gestión de Calidad y ha establecido el Manual de Calidad MA-DI-001 en su versión 2, aprobada el 06 de Junio de 2014, documento que da a conocer lo siguiente:

- Principios que orientan nuestra gestión de calidad
- Misión
- Política de calidad (cómo se aplica)
- Objetivos de calidad
- Alcance Sistema de Gestión de Calidad
- Mapa de procesos (17 procesos)
- Exclusiones del sistema de Gestión de calidad

- Procedimientos obligatorios de la norma
  - ✓ CONTROL DE DOCUMENTOS (4.2.3 ISO 9001 – NTCGP 1000)
  - ✓ CONTROL DE REGISTROS (4.2.4 ISO 9001 – NTCGP 1000)
  - ✓ AUDITORÍAS INTERNAS (8.2.2 ISO 9001 – NTCGP 1000)

- Tratamiento de producto y/o servicio no conforme (8.3 ISO 9001 – NTCGP 1000)
- Descripción de procesos, responsabilidad y autoridad del Sistemas de Gestión de Calidad S.G.C
- Comité de coordinación del Sistema de Control Interno MECI y del Sistema de Gestión de Calidad
- Representante de la Dirección
- Sistema Integrado de Gestión MECI-Calidad de la Alcaldía de Fusagasugá (SIMCAF)
- Equipo técnico MECI-Calidad (EMCAF)
- Líderes de proceso
- Definición de clientes de la Alcaldía de Fusagasugá

- Caracterizaciones de los procesos (17 procesos)
  - ✓ Uno (1) Estratégico
  - ✓ Nueve (9) misionales
  - ✓ Seis (6) apoyo
  - ✓ Uno (1) evaluación

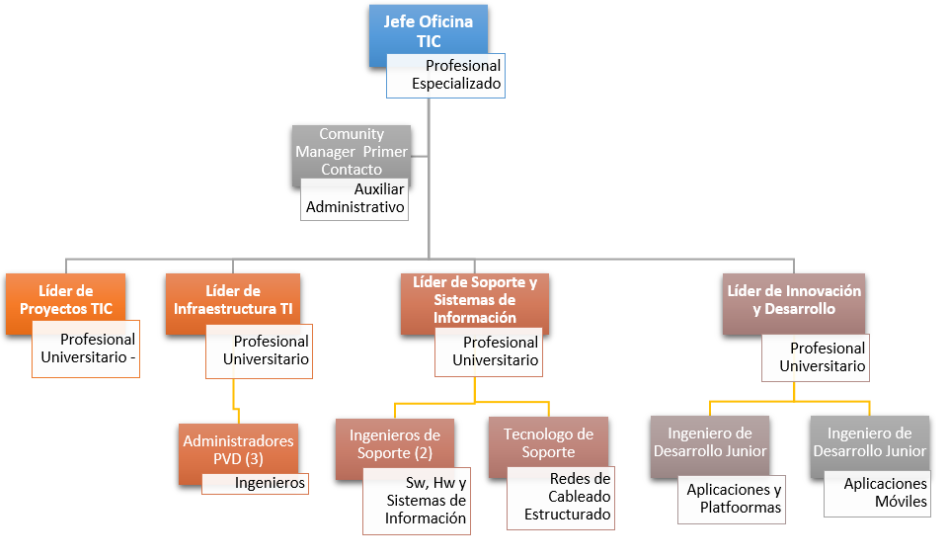
Figura 27. Mapa de procesos

Fuente: Manual de Calidad MA-DI-001

8.2 ANÁLISIS DEL PROCESO DE GESTIÓN TIC Y SISTEMA GESTIÓN DE SEGURIDAD INFORMÁTICA (SGSI)

La Oficina de Tecnologías de la Información y las Comunicaciones (Oficina TIC), en cumplimiento de la Norma Técnica de Calidad para la Gestión Pública NTC-GP 1000:2009 y en el Modelo Estándar de Control Interno MECI 1000:2014 el proceso Gestión TIC es de tipo apoyo, y las áreas que intervienen es la Oficina de Tecnologías de la Información y Comunicaciones (TIC).

Figura 28. Organigrama Interno Oficina TIC



Fuente: Oficina TIC

La estructura está conformada por catorce (14) personas, cinco (5) personas de planta, nueve (9) OPS y una (1) pasante del SENA. En total doce (12) profesionales en Ingeniera de Sistemas, un (1) Tecnólogo y un (1) Auxiliar Administrativo.

Descripción de la Oficina TIC: La Oficina de Tecnologías de la Información y Comunicaciones (TIC), dentro de su proceso de apoyo GESTION TIC del Sistema de Gestión de Calidad (SGC), y según su caracterización CA-GT-001 esta es su descripción:

Objetivo: Implementar las Tecnologías de la Información y las Comunicaciones mediante la innovación y nuevos desarrollos tecnológicos, como también el mantenimiento y soporte a la infraestructura tecnológica (software, hardware y comunicaciones) de la Alcaldía Municipal de Fusagasugá para garantizar la prestación de sus servicios misionales, estratégicos y de apoyo.

Alcance: El proceso comprende desde el establecimiento de planes, proyectos y políticas en materia TIC, para el desarrollo y la innovación de nuevos productos tecnológicos, la administración de la infraestructura tecnológica con servicios de mantenimiento y soporte técnico, hasta la implementación y apropiación de nuevas tecnologías en la Alcaldía Municipal de Fusagasugá, que se encuentran a cargo de la Oficina TIC.

Actividades: Enmarcadas en la metodología DEMING ciclo PHVA, planear, hacer, verificar y actuar.

P: Identificar las necesidades y recopilar información para los planes y proyectos TIC's.
H: Elaborar plan anual de adquisiciones, plan de mantenimiento a la infraestructura tecnológica y proyectos TIC.
H: Administrar la infraestructura tecnológica (software, hardware y comunicaciones) a cargo de la Oficina TIC's.
H: Brindar servicio de soporte técnico y diagnostico a la infraestructura tecnológica.
H: Administrar y custodiar las copias de seguridad.
H: Actualizar el inventario de la infraestructura tecnológica (software, hardware y comunicaciones).
H: Desarrollar, innovar y apropiar nuevas TIC.
V: Medir el desempeño del proceso a través de cumplimiento de actividades de seguimiento.
A: Mejorar continuamente el proceso mediante la aplicación de acciones correctiva, preventivas y de mejora.

Figura 29. Caracterización Proceso Gestión TIC

12.12 GESTIÓN DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES

	12.12 CARACTERIZACIÓN PROCESO GESTIÓN DE TECNOLOGIAS DE LA INFORMACIÓN Y LAS COMUNICACIONES (TIC)	Código: CA-GT-001 Fecha de aprobación: 13 de Junio de 2014 Versión: 1

Proceso: GESTIÓN DE TECNOLOGIAS DE LA INFORMACIÓN Y LAS COMUNICACIONES (TIC) **Tipo de Proceso:** APOYO

Objetivo del proceso: Implementar las Tecnologías de la Información y las Comunicaciones mediante la innovación y nuevos desarrollos tecnológicos, como también el mantenimiento y soporte a la infraestructura tecnológica (software, hardware y comunicaciones) de la Alcaldía Municipal de Fusagasugá para garantizar la prestación de sus servicios misionales, estratégicos y de apoyo.

Líder del Proceso: JEFE OFICINA TIC

Alcance El proceso comprende desde el establecimiento de planes, proyectos y políticas en materia TIC, para el desarrollo y la innovación de nuevos productos tecnológicos, la administración de la infraestructura tecnológica con servicios de mantenimiento y soporte técnico, hasta la implementación y apropiación de nuevas tecnologías en la Alcaldía Municipal de Fusagasugá, que se encuentran a cargo de la Oficina TIC's.

PROVEEDOR	ENTRADA		ACTIVIDADES	SALIDA	CLIENTE
Gobierno Nacional y Territorial Todos los procesos Organismos de Control y Vigilancia Los ciudadanos	Normatividad Solicitud de requerimientos Informes de auditorías No conformidades	P	Identificar las necesidades y recopilar información para los planes y proyectos TIC's.	Plan anual de adquisiciones, plan de mantenimiento a la infraestructura tecnológica y proyectos TIC. Administrar la infraestructura tecnológica) a cargo de la Oficina TIC's. Prestación de servicio de soporte técnico y diagnósticos. Plan de copias de seguridad y reporte de custodia. Informes y formatos de inventario actualizado de hardw are y softw are. Desarrollo, innovación y apropiación de nuevas TIC como plataformas, infraestructura y sistemas de información. Indicadores, encuestas internas de satisfacción del servicio y PQR's (peticiones, quejas y reclamos). Planes de mejoramiento y Administración del riesgo.	Todos los procesos Organismos de Control y Vigilancia Los ciudadanos
		H	Baborar plan anual de adquisiciones, plan de mantenimiento a la infraestructura tecnológica y proyectos TIC.		
		H	Administrar la infraestructura tecnológica (softw are, hardw are y comunicaciones) a cargo de la Oficina TIC's.		
		H	Brindar servicio de soporte técnico y diagnostico a la infraestructura tecnológica.		
		H	Desarrollar e implementar las estrategias GEL.		
		H	Administrar y custodiar las copias de seguridad.		
		H	Actualizar el inventario de la infraestructura tecnológica (softw are, hardw are y comunicaciones).		
		H	Desarrollar, innovar y apropiar nuevas TIC.		
		V	Medir el desempeño del proceso a través de cumplimiento de actividades de seguimiento.		
		A	Mejorar continuamente el proceso mediante la aplicación de acciones correctiva, preventivas y de mejora		

RELACIÓN DE ANEXOS

Anexo 1- Requisitos del Proceso Anexo 2- Ficha Técnica de Indicadores Anexo 3- Lista Maestra de Documentos Anexo 4-Tabla de Retención Documental Anexo 5- Mapa de Riesgos Anexo 6- Matriz de Seguimiento (Actividades y Recursos del Proceso)

Fuente: Manual de Calidad MA-DI-001

La Oficina TIC durante la vigencia 2014 diseño y envió al Comité MECI-Calidad para aprobación los documentos necesarios para evidenciar la ejecución de las

actividades del proceso de GESTION TIC, de acuerdo a lo aprobado por el Sistema de Gestión de Calidad (SGC), y aplica la Ley General de Archivo conforme a las Tablas de retención documental y Manual de imagen corporativa.

FORMATOS:

- FO-GT-001 FORMATO HOJA DE VIDA TIC.
- FO-GT-002 FORMATO DE SOLICITUD SERVICIO DE SOPORTE (Apoyado por el Sistema de Información de Reporte de Incidencias Técnicas - SIRIT)
- FO-GT-003 FORMATO DE SOPORTE Y DIAGNOSTICO TECNICO.
- FO-GT-004 FORMATO DE SERVICIO DE SOPORTE.
- FO-GT-005 MANTENIMIENTO DE SOFTWARE Y HARDWARE EQUIPOS DE CÓMPUTO.
- FO-GT-006 FORMATO PLAN ANUAL DE MANTENIMIENTO PREVENTIVO.
- FO-GT-007 SOLICITUD DE SERVICIO Y/O ACCESO A LA RED LAN, INTRANET, INTERNET, SOFTWARE Y OTROS.
- FO-GT-008 FORMATO DE REQUERIMIENTO INTERNO FUNCIONAL Y DOCUMENTAL DE SOFTWARE.
- FO-GT-009 FORMATO REGISTRO DE PRUEBAS FUNCIONALES.
- FO-GT-010 FORMATO PROTOCOLO COPIA DE SEGURIDAD DE INFORMACION.
- FO-GT-011 FORMATO PARA ENTRADA Y/O SALIDA DE EQUIPOS TECNOLOGICOS.
- FO-GT-012 FORMATO DE SOLICITUD DE SERVICIO DE ASESORIA TIC's.

PROCEDIMIENTOS:

- PR-GT-001 PROCEDIMIENTO SERVICIO DE SOPORTE TECNICO.
- PR-GT-002 PROCEDIMIENTO PROYECTOS TIC.

MANUAL:

- MA-GT-001 MANUAL PARA EL USO ADECUADO DE LA INFRAESTRUCTURA TECNOLOGICA.

PROTOCOLO:

- PT-GT-001 PROTOCOLO DE SERVICIOS INFORMÁTICOS Y COMPROMISO DE CONFIDENCIALIDAD SOBRE TRATAMIENTO DE DATOS

MAPA DE RIESGOS:

- FO-DI-031 CONTEXTO ESTRATEGICO
- FO-DI-032 IDENTIFICACION DEL RIESGO

- FO-DI-033 ANALISIS DEL RIESGO
- FO-DI-034 VALORACIÓN DEL RIESGO
- FO-DI-035 MAPA DE RIESGOS

Sistema de Gestión de Seguridad de la Información (SGSI)

El análisis, planeación, implementación y cronograma de actividades secuencial y lógico para proponer el Modelo Guía para implementación de protocolos de seguridad informática y Sistema de Gestión de Seguridad de la información (SGSI) en la Alcaldía Municipal de Fusagasugá.

Para el modelo un Sistema de Gestión de Seguridad de la Información (SGSI), fue necesario tener en cuenta y entender cómo aplicar los requerimientos de la norma ISO 27001:2013, iniciando con el entendimiento de la organización, realizando un diagnóstico de seguridad de la información, identificando las principales vulnerabilidades y amenazas, aplicando una metodología para la gestión de riesgos de seguridad de la información, planeación de los planes de tratamiento de riesgos y generación del marco documental del Sistema de Gestión de Seguridad de la Información para la Alcaldía de Fusagasugá.

Es importante señalar, que el Modelo Guía para implementación de protocolos de seguridad informática y Sistema de Gestión de Seguridad de la información (SGSI), representa para la Alcaldía Municipal de Fusagasugá, una alternativa para garantizar que los procesos puedan gestionar de manera eficientemente la accesibilidad de la información, asegurando la confidencialidad, integridad y disponibilidad de los activos de información, de tal forma que se a la vez se minimicen los riesgos de seguridad de la información. También obedece a una solución que permita continuar con el mejoramiento del SGSI, para que siga siendo eficiente durante un largo tiempo adaptándose a los cambios internos de la organización, así como los factores externos del entorno.

El modelo de operación de MinTIC definido en el Modelo de Seguridad y Privacidad de la Información (MSPI), establece cinco (5) fases o componentes que comprenden los objetivos, metas y herramientas que permiten que la seguridad y privacidad de la información como un sistema de gestión sostenible dentro de las entidades territoriales:

- Componente Diagnostico
- Componente Planificación
- Componente Implementación

- Componente Gestión y/o evaluación de desempeño
- Componente Mejora Continua

8.3 REVISIÓN DE LA ADMINISTRACIÓN DEL RIESGO INFORMÁTICO PROCESO GESTIÓN TIC

La Oficina TIC de la Alcaldía de Fusagasugá, suministro para el proyecto los riesgos informáticos del proceso GESTION TIC, en cumplimiento de la Norma Técnica de Calidad para la Gestión Pública NTC-GP 1000:2009 y en el Modelo Estándar de Control Interno MECI 1000:2014. Estos riesgos han sido aprobados y documentados por el Comité MECI-Calidad, aplicando la *Guía de administración del riesgo del Departamento Administrativo de la Función Pública (DAFP).* El ICONTEC a través de la norma NTC-ISO 31000 actualizó la norma NTC5254 base para el documento de la Guía de administración del riesgo del DAFP.

El proceso GESTION TIC define para riesgos informáticos los siguientes formatos, que pueden ser visualizados en el *Anexo No. 8. Administración del Riesgo Gestión TIC.*

- FO-DI-031 CONTEXTO ESTRATEGICO: Donde se describen siete (7) factores externos y siete (7) internos, con cada una de sus causas.

- FO-DI-032 IDENTIFICACION DEL RIESGO: Aquí se identifican catorce (14) riesgos, causas, descripción y consecuencias potenciales.

- FO-DI-033 ANALISIS DEL RIESGO: Se establece para cada riesgo la calificación en probabilidad e impacto, tipo de impacto, evaluación y las medidas de respuesta *(reducir, evitar, transferir o compartir el riesgo).*

- FO-DI-034 VALORACIÓN DEL RIESGO: Se identifican los controles para los riesgos que posteriormente serán evaluados de acuerdo a la política de administración del riesgo, para establecer en la valoración el tipo control probabilidad o impacto, puntaje herramientas para ejercer el control, puntaje para seguimiento y control y puntaje final.

- FO-DI-035 MAPA DE RIESGOS: Donde se encuentra el resumen de la gestión del riesgo.

Dando cumplimiento al objetivo del proyecto, con los protocolos de seguridad y el Modelo Guía para implementación de protocolos de seguridad informática y Sistema de Gestión de Seguridad de la información (SGSI), se pretende contribuir a las medidas de respuesta y controles sobre los riesgos informáticos identificados por la Oficina TIC, de tal manera que en la valoración el puntaje obtenido dé como resultado del análisis de riesgo que las acciones tomadas pueden garantizar en un porcentaje el logro de los objetivos de la entidad o el cumplimiento de su función.

La Oficina TIC debe verificar que los controles existentes contribuyan a evitar, compartir o mitigar los diferentes riesgos identificados, y como parte de esa acción preventiva o correctiva se encuentran los productos entrégales en el este proyecto.

El análisis de resultados de las encuestas aplicadas en la Alcaldía de Fusagasugá, suministran datos importantes que pueden señalar a la organización que es necesarios analizar y evaluar la posibilidad de identificar nuevos riesgos.

También es necesario que la Oficina TIC solicite la política de administración pública, para exigir una valoración de los riesgos dentro de los periodos establecidos.

En resumen el análisis de los riesgos del proceso de GESTION TIC es el siguiente:

Tabla 5. Análisis del riesgo proceso Gestión TIC

	ANÁLISIS DEL RIESGO	**CODIGO: FO-DI-033**
	PROCESO DE DIRECCIONAMIENTO ESTRATEGICO	**VERSION: PRUEBA**
ELABORO: Profesional Universitario	**REVISÓ: Jefe Oficina TIC's**	**APROBÓ: Comité Meci-Calidad, Alcalde**

PROCESO	**PROCESO DE GESTIÓN DE TECNOLOGIAS DE LA INFORMACION Y LAS COMUNICACIONES (TIC)**
OBJETIVO	Implementar las Tecnologías de la Información y las Comunicaciones mediante la innovación y nuevos desarrollos tecnológicos, como también el mantenimiento y soporte a la infraestructura tecnológica (software, hardware y comunicaciones) de la Alcaldía Municipal de Fusagasugá para garantizar la prestación de sus servicios misionales, estratégicos y de apoyo.

RIESGO	CALIFICACIÓN		TIPO DE IMPACTO	EVALUACIÓN	MEDIDAS DE RESPUESTA
	Probabilidad	Impacto			
Fallas o suspensión en la prestación de servicios de energía eléctrica.	5	4	Operativo 5	Zona de Riesgo Extrema	Transferir el riesgo al proceso de Apoyo Gestión Administrativa y misional Planificación y desarrollo Integral del riesgo
Daños y pérdidas en equipos tecnológicos por catástrofes naturales.	2	5	Operativo 5	Zona de Riesgo Extrema	Evitar y compartir el riesgo con el proceso de Gestión rural ambiental y del riesgo
Fallas en la prestación de los servicios de tecnologías de la información y las comunicaciones (internet y telefonía).	5	3	Operativo 5, Credibilidad o Imagen 4	Zona de Riesgo Extrema	Reducir el riesgo
Atentados contra la confidencialidad, la integridad y la disponibilidad de los datos y de los sistemas informáticos.	2	4	Confidencialidad de la información 1, Operativo 4	Zona de Riesgo Alta	Reducir el riesgo
Atentados informáticos y otras infracciones.	2	4	Confidencialidad de la información 1, Operativo 4	Zona de Riesgo Extrema	Evitar el riesgo
Acciones terroristas y de orden público.	2	4	Operativo 5	Zona de Riesgo Alta	Evitar y compartir el riesgo con el proceso misional Convivencia y Seguridad Ciudadana
Inadecuada o insuficiente infraestructura TIC actualizada.	3	2	Operativo 4	Zona de Riesgo Moderada	Reducir y compartir el riesgo con el proceso de apoyo Hacienda Pública
Inadecuada o insuficiente infraestructura TIC de respaldo o backup.	3	2	Operativa 4	Zona de Riesgo Moderada	Reducir y compartir el riesgo con el proceso de apoyo Hacienda Pública
Insuficiente infraestructura tecnológica para suplir la demanda de servicios requeridos por los funcionarios.	3	2	Operativa 4	Zona de Riesgo Moderada	Transferir el riesgo al proceso de apoyo Gestión Administrativa
Desconocimiento de la infraestructura tecnológica implementada.	3	3	Operativa 4, Credibilidad o Imagen 2.	Zona de Riesgo Alta	Evitar el riesgo
Administración inadecuada de la infraestructura tecnología.	3	4	Operativa 4, Credibilidad o Imagen 1.	Zona de Riesgo Extrema	Evitar el riesgo
Equipos desactualizados o con inconvenientes en su funcionamiento.	4	3	Operativa 4	Zona de Riesgo Alta	Transferir el riesgo al proceso de apoyo Gestión Administrativa

Disponibilidad de recursos financieros para la compra y suministro de equipos, servicios de mantenimiento, internet, y/o actualización de la infraestructura tecnológica.	3	3	Operativa 4	Zona de Riesgo Alta	Transferir el riesgo al proceso de Direccionamiento Estratégico, Hacienda Pública y Gestión Administrativa
Daño total o parcial de infraestructura tecnológica.	4	3	Operativa 4	Zona de Riesgo Alta	Reducir el riesgo

Fuente: Alcaldía de Fusagasugá

La Alcaldía de Fusagasugá tiene identificado un total de catorce (14) riesgos informáticos para el proceso GESTION TIC, la totalidad de los mismos tienen un tipo de impacto operativo, tres (3) de credibilidad o imagen corporativa y dos (2) relacionado con un impacto en la confidencialidad de la información. De otra parte, en la evaluación de estos riesgos, cinco (5) se encuentran en zona de riesgo extrema, seis (6) en zona de riesgo alto y tres (3) en zona de riesgo moderado; representando un necesidad urgente a la Alcaldía de Fusagasugá para implementar protocolos de seguridad informática y un modelo de Sistema de Gestión de Seguridad de la Información (SGSI), que le permitan fortalecer los procesos, actividades laborales y servicios que realiza la Oficina TIC de la Alcaldía de Fusagasugá, y dentro de la gestión del riesgo emprender acciones de control y valoración, con el fin contribuir a que el riesgo se pueda evitar, reducir, transferir, compartir o asumir, conforme al política de administración del riesgo de la entidad, mejorar continuamente y disminuir de la probabilidad de ocurrencia, así como asegurar que el impacto sea menor.

8.4 PROTOCOLOS DE POLITICAS DE SEGURIDAD DE LA INFORMACIÓN

Luego de la validación de los riesgos que se encuentran identificados, junto con los que se identifican gracias al resultado de las encuestas aplicadas, se definen los protocolos que definen y regulan las políticas de seguridad de la información dentro de la Alcaldía Municipal de Fusagasugá en los diferentes ámbitos. La Política TIC que se expone a continuación es un planteamiento sobre el tratamiento de la seguridad de la información que se convertirán posteriormente en protocolos específicos con la implementación y seguimiento que se realice a estas, así como con la concienciación que se realice al personal sobre las buenas prácticas en Seguridad de la Información y en la capacitación del personal de la Oficina TIC y de Control Interno para la prevención, detección y respuesta de la información ante incidentes de seguridad.

8.4.1 Generales

a) Todo funcionario o usuario con acceso a la información, aplicaciones o sistemas de la Alcaldía Municipal de Fusagasugá, tiene la obligación de adoptar todas las medidas de control establecidas, así como los ordenamientos legales aplicables para la protección de la información o sistemas a los que tenga acceso, preservando su naturaleza confidencial y evitando su transferencia, modificación, destrucción o divulgación a entidades no autorizadas.
b) La infraestructura tecnológica y la información de la Alcaldía Municipal de Fusagasugá (sistemas, aplicaciones, programas, y en general todos los recursos de cómputo e información que reside o se transmite a través de ellos, PC, escritorios, portátiles, teléfonos celulares, Blackberry, table PC o ipad) son propiedad de la Alcaldía Municipal de Fusagasugá, por tanto ningún funcionario puede copiar, duplicar, transmitir o divulgar dicha información, el conocimiento de la misma debe ser únicamente para fines del cumplimiento de sus funciones.
c) El usuario de red y la contraseña asignados para el acceso a los sistemas, aplicaciones y en general a los recursos de cómputo e información, son personales, intransferibles y confidenciales; por tanto el titular de la misma es responsable por el uso que se haga de ella, así como de la información y provecho que a través de ella obtenga, para sí o para terceros y de los daños y perjuicios que se ocasionen sin menoscabo de las responsabilidades y sanciones de naturaleza civil y penal que resulten.
d) Cada funcionario debe tener solamente un usuario de red a su nombre, el cual se asignara por la Alcaldía Municipal de Fusagasugá.
e) El acceso a los sistemas de cómputo y aplicaciones de la Alcaldía Municipal de Fusagasugá que se haga mediante el usuario distinto al asignado para el desempeño de sus funciones, se considera como un uso no autorizado de información confidencial.
f) Se considera una falta grave, la introducción, tráfico o envío de información (cadenas de cartas), el desarrollo, almacenamiento, uso (ejecución) de programas, aplicaciones u otros mecanismos que puedan dañar, alterar o impactar en el desempeño de los componentes de software de una computadora o sistema de cómputo o comunicaciones propiedad de la Alcaldía Municipal de Fusagasugá, con el fin de molestar a otros usuarios, infiltrarse en un sistema, y en general, intentar violar los estándares de seguridad definidos para la Alcaldía Municipal de Fusagasugá por parte de la Oficina TIC.
g) La infraestructura de sistemas, aplicaciones y en general los recursos de cómputo e información de la Alcaldía Municipal de Fusagasugá, debe ser utilizada únicamente para los fines del propios de la entidad. En virtud de

ello, no debe ser usada para provecho personal, tales como entretenimiento, grupos de conversación, juegos recreativos, entre otros.

h) En ningún caso, los usuarios de red pueden ser reasignados o puestos a nombre de otras personas. Los usuarios de la Alcaldía Municipal de Fusagasugá no deben establecer redes de área local, conexiones remotas a redes internas o externas, intercambio de información con otros equipos de cómputo utilizando el protocolo de transferencia de archivos (FTP), u otro tipo de protocolo para la transferencia de información empleando la infraestructura de red de la Alcaldía de Fusagasugá, sin la previa autorización por escrito de la Oficina de Tecnologías de la Información y las Comunicaciones.
i) El funcionario debe obligarse a impedir fugas de información confidencial o secreta o evitar la sustracción o utilización indebida de la documentación e información clasificada o confidencial a la cual tiene acceso y que le corresponde custodiar por razón de su cargo o función.
j) Los funcionarios de la Alcaldía Municipal de Fusagasugá, se obligan con toda información clasificada como confidencial a: administrarla, guardarla, custodiarla y conservarla bajo la más estricta reserva.
k) No se permite utilizar programas, herramientas o mecanismos de mensajería instantánea (chats internos o públicos) para el envío y recepción de información confidencial.
l) No se permite utilizar programas, herramientas o mecanismos que pudieran analizar información confidencial en los dispositivos.
m) Al imprimir información confidencial de cualquiera de la Alcaldía Municipal de Fusagasugá, el usuario debe proteger la información contra robo y acceso no autorizado.
n) El usuario final debe recoger sus listados confidenciales en el menor tiempo posible, no dejándolos olvidados en impresoras, salas de reuniones, entre otros y no utilizándola como papel reciclable. Esto es aplicable también a los usuarios informáticos.
o) Está prohibida la definición y asignación de usuarios genéricos para uso compartido (usuarios que no están a cargo de un funcionario).
p) La transmisión de archivos vía FTP es restringida en la Alcaldía Municipal de Fusagasugá. En caso de excepciones se debe hacer el análisis correspondiente y avalarlo por la Oficina TIC.
q) Todos los funcionarios están obligados a bloquear su terminal de trabajo cuando se ausenten de su puesto. En caso de inactividad por más de 5 minutos, estas se bloquearan automáticamente.
r) La ejecución de operaciones no autorizadas al cargo específico que desempeña se considera falta grave y es sancionada disciplinariamente.
s) La Alcaldía Municipal de Fusagasugá establece los procedimientos necesarios para controlar los permisos de acceso, la consulta y la administración de las carpetas y archivos ubicados en la red de servidores.

t) La Oficina de TIC en la Alcaldía Municipal de Fusagasugá no garantiza que los archivos que se transfieren por la red de Internet estén libres de virus, gusanos, caballos de troya o demás códigos de infección.
u) Está prohibido compartir carpetas de los discos duros de los equipos propios o unidad “C”, entre usuarios.
v) El servicio de acceso a internet se autoriza a funcionarios y terceros que requieran dicho acceso para el cabal ejercicio de sus funciones.
w) Cualquier intento de acceso exitoso o no exitoso a páginas fuera de las autorizadas se considera una falta grave y se aplica las sanciones establecidas en el régimen disciplinario correspondiente.
x) La Oficina de TIC en la Alcaldía Municipal de Fusagasugá establece los estándares y procedimientos necesarios para control de reportes de acceso y actividad en internet.
y) La autorización para inspección y monitoreo del uso de internet se presume desde el momento de asignación de acceso.
z) Bajo la confirmación y autorización del Gestor de Recursos Humanos de que un funcionario con un cargo diferente a los anteriormente autorizados, tenga acceso a formularios por que se encuentre reemplazando a un cargo de éstos, se autoriza tener el cargo en este aplicativo.

8.4.2 Aplicaciones

a) Las aplicaciones que contengan componentes de seguridad (encripción, claves de acceso, identificación del PIN, bases de datos de autenticaciones, entre otros), deben estar avaladas por la Oficina TIC de la Alcaldía Municipal de Fusagasugá.
b) Cada funcionario debe estar matriculado con un solo perfil de la plataforma unificada de sistemas y poseer los accesos adicionales al sistema, de acuerdo con el cargo que desempeña.
c) Para aquellas aplicaciones que no son administradas por la Oficina TIC de la Alcaldía Municipal de Fusagasugá, el alta, baja y modificación de usuarios debe ser solicitado por medio de un correo electrónico del Jefe Inmediato.
d) Los usuarios no deben modificar las configuraciones generales y especialmente aquellas específicas de seguridad establecidas en las aplicaciones o sistemas operativos. En caso de problemas en su operativa habitual siempre deben ponerse en contacto con soporte o asistencia técnica.
e) Se deben desactivar las opciones que permiten la ejecución de macros en aplicaciones ofimáticas sin pedir expresamente la autorización del usuario. Además, siempre que se autorice la ejecución de macros, se debe estar completamente seguro de la procedencia, fiabilidad e integridad de los contenidos del documento en que dichas macros se encuentran.

8.4.3 Manejo de Claves

a) La clave debe ser de ocho (8) caracteres alfanuméricos diferente a la utilizada en los últimos tres meses.
b) El sistema valida el no uso de las últimas trece (13) contraseñas o password utilizadas para así evitar problemas de seguridad. Si se utiliza una clave repetida el sistema bloquea al usuario.
c) El password de cualquier sistema o aplicación debe permitir el cambio de clave obligatoriamente cada 30 días y al tercer intento fallido de password debe bloquearse de manera permanente.
d) La vigencia de la contraseña o clave es de treinta (30) días calendario para la red de la Alcaldía Municipal de Fusagasugá. Transcurrido este tiempo el sistema obliga el cambio de clave, pero si el usuario no ingresa pasado este período de tiempo, el sistema revoca la clave del usuario. En pro de aumentar la seguridad de la información presente en los diferentes requerimientos de acceso a los servidores de aplicaciones, bases de datos y repositorios bajo protocolos específicos, no se podrán usar contraseñas antiguas y la complejidad de la misma dependerá de las reglas que la Oficina de Tecnologías de la Información y las Comunicaciones brindará en la inducción.
e) En caso de existir una razón justificada del no uso del sistema (licencia, incapacidad, vacaciones, permiso, entre otros), el Jefe Inmediato deberá informar a la Oficina TIC de la Alcaldia Municipal de Fusagasuga, para que se realice el respectivo Bloqueo del Usuario de red durante el tiempo en que el funcionario se encuentre fuera de su labor.

8.4.4 Segmentación de Redes

a) La Alcaldía Municipal de Fusagasugá, deberá realizar la segmentación lógica y física de los servidores de la capa de presentación ubicados en una DMZ protegida por Firewall, respecto a los servidores de aplicativos ubicados en una zona interna, la comunicación entre los segmentos debe realizarse mediante protocolos seguros tipo HTTPS con certificados digitales de tipo OV.
b) El servidor de Base de Datos que se utiliza para la Alcaldía Municipal de Fusagasugá se debe ubicar en un sistema distinto al de ejecución de la aplicación, habilitando únicamente la comunicación con el servidor de aplicaciones donde se aloje la aplicación.

8.4.5 Servidores para Prestar el Servicio

a) Todas las reglas que se den de alta en los firewalls de la Alcaldía Municipal de Fusagasugá deberán estar con el respectivo detalle indicando claramente a qué servicio se refieren, siempre que sea técnicamente posible documentarlas.
b) Los servidores deben cumplir con políticas de militarización de sistema operativo, teniendo en cuenta que la Alcaldía Municipal de Fusagasugá deberá tener establecido un procedimiento de actualización.

8.4.6 Hardware

a) Cualquier daño o pérdida de los equipos que manejan información de la Alcaldía Municipal de Fusagasugá deberán ser reportados al área encargada. La intervención directa de personal no autorizado para reparar el equipo debe estar expresamente prohibida. La empresa debe proporcionar personal interno o externo para la solución del problema reportado.
b) Todo el hardware o software que adquiera la Alcaldía Municipal de Fusagasugá debe conseguirse a través de canales de compra estándares y confiables. A su vez estos deberán ser registrados al fabricante y contar con el respectivo contrato de mantenimiento.

8.4.7 Acceso Lógico y Físico

a) Todos las computadoras multiusuarios y los equipos de comunicaciones propiedad de la Alcaldía Municipal de Fusagasugá deben estar ubicadas en lugares asegurados para prevenir alteraciones y usos no autorizados.
b) Los medios de respaldo como cintas, discos y documentos, se deben ubicar en áreas restringidas y/ó en sitios con acceso únicamente a personas autorizadas.
c) La Alcaldía Municipal de Fusagasugá debe establecer un modelo de autenticación multifactorial el cual estará definido y condicionado al resultado de un análisis de riesgos.
d) El control de acceso a recursos se articulará siempre en base a la asignación de los usuarios de acuerdo a las funciones que estos desempeñan dentro de la Alcaldía Municipal de Fusagasugá. Nunca se deberán asignar permisos de acceso directos a recursos para usuarios concretos.

8.4.8 Respaldo y continuidad del negocio

a) Todas las estaciones de trabajo se deben equipar con unidades suplementarias de energía eléctrica (UPS), filtros eléctricos, supresores de picos de corriente y en lo posible, eliminadores de corriente estática. Se integrará un sistema de administración de energía extra en la Alcaldía Municipal de Fusagasugá pueda garantizar con la Secretaria de Infraestructura la disponibilidad de la información en los diferentes servidores de la compañía, esto evitará que el sistema analizador de tráfico instalado pierda secciones por interrupción de energía.
b) Cada uno de los equipos de cómputo, comunicaciones y demás equipos de soporte, deberá realizársele un mantenimiento preventivo y periódico, previniendo que el riesgo a fallas se mantenga en una probabilidad de ocurrencia baja.
c) Los planes de contingencia y de recuperación de sistemas deben ser actualizados y probados regularmente con el fin de asegurar la eficacia de los planes y por ende la Estrategia de Continuidad que se ha establecido. Cada prueba debe documentarse y sus resultados y las acciones de mejora deben comunicarse a la alta dirección.

8.4.9 Accesos de los Usuarios

a) Las Estaciones de trabajo, Servidores y Aplicativos que se tengan al interior de la Alcaldía Municipal de Fusagasugá deben ser protegidos mediante usuario y contraseña. Se debe establecer una caducidad específica para la contraseña, la cual será asignada inicialmente de forma confidencial y segura al usuario, quien debe realizar cambio en el primer logon, además, tendrá una longitud mínima de 8 caracteres y será alfanumérica.
b) Para la sesión de usuario se debe contar con un timeout de 5 minutos, una vez se exceda este tiempo la sesión se bloqueara.
c) Debe quedar registrado en el log los logins/logoff con sus correspondientes horarios y los cambios de contraseña de todos los usuarios del sistema/aplicación.
d) Los usuarios son responsables de todas las actividades llevadas a cabo con su código de identificación de usuario y sus claves personales.
e) Cada usuario deberá contar con su respectivo código para acceder a los sistemas de información, la generación de usuarios genéricos deberá estar restringida.
f) Toda clave de acceso debe estar personalizada, lo cual implica que la clave Administrador del sistema debe ser usada solo en situaciones predeterminadas.

g) La cuenta administrador NUNCA debe ser utilizada para actividades cotidianas, debe permanecer en custodia.
h) Se limitará el otorgamiento de privilegios administrativos para instalación, configuración, monitorización o soporte por parte de personal ajeno al personal designado para tal fin.
i) Para prevenir infecciones por virus informáticos, los usuarios de tecnologías de la información, deben evitar hacer uso de cualquier clase de software que no haya sido proporcionado y validado por la Oficina de Tecnologías de la Información y las Comunicaciones.
j) Se considera una falta grave el que los usuarios instalen cualquier tipo de programa (software) en sus computadores, estaciones de trabajo, servidores, o cualquier equipo conectado a la red de la Alcaldía Municipal de Fusagasugá, que no esté autorizado por la Oficina de Tecnologías de la Información y las Comunicaciones.
k) Los empleados que requieran de la instalación de software o aplicativos que no sean de propiedad de la Alcaldía Municipal de Fusagasugá, deberán justificar su uso y solicitar su autorización a la Oficina de Tecnologías de la Información y las Comunicaciones, a través de un documento firmado por el titular Jefe Inmediato, indicando el equipo de cómputo donde se instalará el software y el período que permanecerá dicha instalación, siempre y cuando el dueño del software presente la factura de compra de dicho software o normatividad que rigen su uso, esto con el fin de tener control sobre todos y cada uno de los programas instalados en la Alcaldía Municipal de Fusagasugá.

8.4.10 Parches de Seguridad

a) Los puestos de trabajo dedicados, servidores y aplicativos de la Alcaldía Municipal de Fusagasugá, deberán estar siempre a último nivel de parches, tanto de S.O. como de productos.
b) Se deberá definir los procedimientos y la política de actualización de parches de seguridad para la Alcaldía Municipal de Fusagasugá.

8.4.11 Tratamiento de Documentación Impresa

a) La documentación en papel no debe de ser accesible por personal no autorizado. Se evitará dejar documentos en las impresoras y fotocopiadoras, así como en sitios de paso o de atención al público.
b) Si la función no lo requiere, queda prohibida la impresión física de documentos que contenga información de la Alcaldía Municipal de Fusagasugá.

8.4.12 Control de la Información

a) Todo funcionario que utilice los recursos de los Sistemas, tiene la responsabilidad de velar por la integridad, confidencialidad, disponibilidad confiabilidad de la información que maneje, especialmente si dicha información ha sido clasificada como crítica.

8.4.13 Vinculación de Personal

a) La contratación y vinculación de personal en la Alcaldía Municipal de Fusagasugá, debe ser un proceso donde se garantice la idoneidad del perfil requerido y sean realizadas todas las consultas respecto a trayectoria y experiencia laboral, verificando las referencias de anteriores funcionarios, así como las respectivas investigaciones de seguridad (antecedentes penales, entre otros).
b) Toda contratación de personal en la Alcaldía Municipal de Fusagasugá deberá contener acuerdo de confidencialidad, copia del mismo deberá ser puesto a disposición del Banco cuando éste así lo requiera.
c) Todas las personas que cumplan con los requisitos básicos exigidos por la entidad deben ser evaluadas frente al perfil del cargo a cubrir en cuanto a conocimientos y competencias.
d) El informe de selección es de carácter estrictamente confidencial y debe ser firmado por el Gestor de Selección.
e) Un contrato de aprendizaje no debe ser mayor a dos (2) años.
f) La solicitud de personal debe hacerse en un plazo no mayor a 15 días contados a partir de la fecha en que el cargo queda vacante.
g) Para el cubrimiento de vacantes se debe dar prioridad a los funcionarios que se encuentran en ese momento a disposición de la Alcaldía Municipal de Fusagasugá.
h) Si al interior de la Alcaldía Municipal de Fusagasugá no se halla el recurso más idóneo para cubrir la vacante, la vinculación de un candidato externo debe de ser aprobada por la Vicepresidencia Ejecutiva de Recursos Humanos.
i) Los procesos de selección aprobados tienen una vigencia de un año.
j) Se deben considerar varias solicitudes, con el fin de tener oportunidad de comparar y elegir entre varios candidatos.
k) En ningún caso la duración del contrato de los recursos temporales podrá exceder el año, ni renovarse por el mismo o diferente período.

8.4.14 Personal de Contrato y/o terceros

a) Para los funcionarios externos de la Alcaldía Municipal de Fusagasugá, es responsabilidad del Jefe Directo, y/o el delegado en su equipo que realice las actividades de administración del contrato, diligenciar el formulario solicitud acceso a la red solicitando la creación, modificación o retiro de un recurso externo, indicando el perfil asignado y el área a que debe ser asignado. Este formulario es remitido a la Oficina TIC de la Alcaldía Municipal de Fusagasugá realizado el trámite correspondiente.
b) El Jefe directo debe velar por la correcta solicitud de perfiles del recurso y la confidencialidad e integridad de la información administrada por el mismo, la cual debe ser necesaria para el desempeño de sus funciones dentro en la Alcaldía Municipal de Fusagasugá.
c) El usuario externo debe cumplir todas las políticas y normativas de seguridad emitidas por la Alcaldía Municipal de Fusagasugá, compartidas por el jefe inmediato del recurso.
d) Desde el momento en que el usuario externo es conocedor de su nueva clave en el sistema, es su responsabilidad personalizar y realizar las modificaciones posteriores de acuerdo con las reglas establecidas por la Alcaldía Municipal de Fusagasugá.
e) Todo funcionario externo, debe utilizar clave de acceso única y debidamente auditada, con las facultades y privilegios requeridos para desempeñar su función.
f) Los usuarios que no ingresen a la red por un período mayor a sesenta (60) días, son eliminados
g) El jefe inmediato del recurso externo debe vigilar que cumpla con las políticas, estándares, normativa y lineamientos de seguridad de la Alcaldía Municipal de Fusagasugá, debe tomar las medidas necesarias para hacer que se cumplan y reportar a sus superiores, a Recursos Humanos y a Oficina TIC de cualquier incidente que afecte a la seguridad de los sistemas.

8.4.15 Copyright

a) La realización de copias no autorizadas de software o material bajo protección de copyright está expresamente prohibida, tanto mediante el uso de los Sistemas de la Alcaldía como si el material está licenciado o es propiedad de la Alcaldía Municipal de Fusagasugá.

8.4.16 Pruebas de seguridad

a) Está expresamente prohibida la recogida de información sobre configuraciones de redes, sistemas, software base, aplicativos y controles internos o mecanismos de seguridad asociados a los mismos tanto para aquellos pertenecientes a la Alcaldía Municipal de Fusagasugá para los ajenos a los mismos, salvo los efectuados por motivos de trabajo por las diferentes áreas en las que es parte de su responsabilidad como la Oficina TIC, Control Interno y Auditoría.
b) Están expresamente prohibidos los intentos de acceso no autorizado mediante monitorización de tráfico de datos, y las pruebas de vulnerabilidades o deficiencias de seguridad en los Sistemas de Información tanto para aquellos pertenecientes a la Alcaldía Municipal de Fusagasugá, salvo los aprobados por la Oficina TIC, Control Interno y Auditoría.
c) No se considerará acceso no autorizado la monitorización de tráfico necesaria e imprescindible para la resolución de incidencias siempre que sea efectuada por los departamentos técnicos responsables y bajo las normas y procedimientos de seguridad específicos que puedan estar establecidos.

8.4.16 Escritorio Limpio

a) Todos los funcionarios internos y externos que presten servicios a la Alcaldía Municipal de Fusagasugá, adoptarán una política de escritorio limpio con el objeto de prevenir el acceso no autorizado a activos de información cuando estos fuesen desatendidos. De esta manera se evitará la manipulación, pérdida o daño de información que se encuentre en soporte electrónico o en papel.
b) Es responsabilidad de todo usuario guardar los soportes electrónicos y documentos en papel cuando se tenga conocimiento de largos periodos de tiempo lejos del escritorio, como en la hora de almuerzo, reuniones en otras locaciones y al final de la jornada de trabajo, entre otros.
c) Todo usuario deberá guardar bajo llave aquellos soportes que contengan documentos clasificados como Confidencial o de Uso Interno de la Alcaldía Municipal de Fusagasugá, durante su ausencia.
d) Todo usuario deberá mantener un entorno de trabajo ordenado para evitar la pérdida de soportes de información, ya sea en formato electrónico o en papel.

8.4.17 Uso correcto de contraseñas

Los funcionarios de la Alcaldía Municipal de Fusagasugá deben:

a) Escoger contraseñas que no sean triviales para impedir que terceras personas puedan suplantarles con éxito.
b) No escribir las contraseñas salvo en los casos en que existan procedimientos de seguridad establecidos para salvaguarda de las mismas.
c) No utilizar mecanismos de recuerdo de contraseña o similares ofrecidos por determinados sistemas o aplicaciones comerciales.
d) Cambiar las contraseñas periódicamente con la frecuencia que se haya determinado para los distintos sistemas y aplicaciones, al menos cada 30 días y siempre que por configuración de los sistemas o aplicaciones se solicite expresamente.
e) No utilizar las mismas contraseñas en sistemas de la Alcaldía Municipal de Fusagasugá en sistemas ajenos al mismo.

8.4.18 Hardware

a) Los usuarios no deben añadir, eliminar o modificar los elementos que configuran el hardware de sus equipos. En caso de nuevas necesidades o problemas en su operativa habitual siempre deben ponerse en contacto con soporte o asistencia técnica.

8.4.19 Activación y actualización de programas antivirus

a) tener instalados en sus puestos ni interferir en los procesos de actualización automática de los mismos.
b) En los casos en los que organizativamente se establezca, habitualmente por imposibilidad técnica de automatización, el usuario deberá proceder a actualizar el antivirus siguiendo los procedimientos que para el caso se establezcan.

8.4.20 Creación o propagación intencionada

a) Queda estrictamente prohibido el uso de redes, sistemas o equipos de la Alcaldía Municipal de Fusagasugá para la creación, ejecución o propagación intencionada de virus o código malicioso.
b) Es responsabilidad de cada funcionario de la Alcaldía Municipal de Fusagasugá asegurarse de que el personal subcontratado a su cargo

conoce la presente Normativa y que cumple con aquellas disposiciones que requieran de aprobación o supervisión previa al inicio de su trabajo.

c) Los usuarios de la Alcaldía Municipal de Fusagasugá que hagan uso de los equipos de cómputo, deben conocer y aplicar las medidas para la prevención de código malicioso como pueden ser virus, gusanos y troyanos. El usuario puede acudir a la Oficina de Tecnologías de la Información y las Comunicaciones, para solicitar asesoría.

8.4.21 Correo electrónico

a) La dirección del buzón de mensajería interna de la Alcaldía Municipal de Fusagasugá, es creado únicamente por el administrador del sistema contratado por la Oficina TIC.
b) Está estrictamente prohibido realizar afirmaciones que produzcan pánico general, cualquiera sea su intención (económico, social, político o natural).
c) Todo correo debe tener la siguiente información básica como firma: Nombres y apellidos completos, cargo que ocupa, dependencia a la cual pertenece dentro de la Alcaldía, nombre completo de la Alcaldía, dirección de correo electrónico corporativo, indicativo de país, número de teléfono, extensión, ciudad y país, código postal y actual emblema de la Alcaldía Municipal de Fusagasugá.
d) Es prohibida la utilización de este medio para el envío de mensajes de tipo religioso, humorístico, de azar o cualquier otro que no aporte a la eficiencia, productividad y eficacia en el cumplimiento de las funciones y responsabilidades de cada cargo.
e) Está prohibido el uso indebido de la extensión o el nombre de dominio en la dirección electrónica.
f) El servicio de correo electrónico corporativo es un instrumento o herramienta de trabajo, cuya propiedad corresponde a la Alcaldía Municipal de Fusagasugá y cuyo uso se vincula a la existencia de la relación laboral.
g) La administración del buzón especial es exclusiva de la dependencia asignada y su responsabilidad de uso, operatividad y backup, será del funcionario-usuario asignado por el responsable de la dependencia para este fin.
h) Se restringirá el ingreso de archivos anexos en los correos electrónicos que tengan extensiones consideradas como peligrosas.
i) El correo institucional es de uso privativo y solo con fines laborales.
j) Los usuarios deben tratar los mensajes de correo electrónico y archivos adjuntos como información que es propiedad de la Alcaldía Municipal de Fusagasugá. Los mensajes de correo electrónico deben ser manejados como una comunicación privada y directa entre emisor y receptor.
k) Los usuarios podrán enviar información reservada y/o confidencial exclusivamente a personas autorizadas y en el ejercicio estricto de sus

funciones y atribuciones, a través del correo institucional que le proporcionó la Oficina de Tecnologías de la Información y las Comunicaciones.

8.4.22 Internet

a) Está estrictamente prohibido el uso del servicio de internet para realizar negocios personales o transacciones financieras electrónicas, salvo los expresamente autorizados por la Alcaldía Municipal de Fusagasugá.
b) La Alcaldía Municipal de Fusagasugá establecerá los estándares y procedimientos necesarios para control de reportes de acceso y actividad en internet.
c) Es prohibido, salvo aprobación expresa, el uso o habilitación de módems, adaptador o cualquier dispositivo externo de almacenamiento y/o transmisión de datos.
d) La autorización para inspección y monitoreo del uso de Internet se presume desde el momento de asignación de acceso.
e) Queda expresamente prohibido el encadenamiento de proxies externos a la Alcaldía Municipal de Fusagasuga para la navegación por Internet.
   La Alcaldía Municipal de Fusagasugá dispondrá de programas antivirus de obligatoria ejecución al momento de recepción de archivos externos por cualquier vía y en cualquier estación de trabajo móvil o fija.
f) Pro aplicabilidad el consumo de recursos viene ligado con el buen uso de las páginas y su contenido, en el caso de páginas de videos y juegos se aplicaran las políticas descritas en el literal anterior que sugieren el buen uso y utilización de la red.
g) La utilización de páginas web inapropiadas dentro de la organización facilitan al desorden de los usuarios en pro de la calidad y el desempeño que se puede lograr, además de esto facilita la infección por adware y virus que adicionarían vulnerabilidades de seguridad de la información a la Alcaldía Municipal de Fusagasugá.
h) La navegación estará restringida exclusivamente para las labores empresariales y las conexiones que lo requieran, si existiera una página bloqueada a la que sea necesario entrar se deberá solicitar la Oficina de Tecnologías de la Información y las Comunicaciones, la debida autorización.
i) El acceso a internet provisto a los usuarios de la Alcaldía Municipal de Fusagasugá es exclusivamente para las actividades relacionadas con las necesidades del puesto y función que desempeña. En caso de daño a la imagen de la institución se procederá de acuerdo a lo que determine la Alta dirección.
j) La asignación del servicio de internet, deberá solicitarse mediante el procedimiento establecido por la Oficina de Tecnologías de la Información y

las Comunicaciones. Esta solicitud deberá contar con el visto bueno del Jefe Inmediato.

k) Todos los accesos a internet tienen que ser realizados a través de los canales de acceso provistos por la Oficina de Tecnologías de la Información y las Comunicaciones.
l) Los usuarios con acceso a Internet de la Alcaldía Municipal de Fusagasugá tienen que reportar todos los incidentes de seguridad informática la Oficina de Tecnologías de la Información y las Comunicaciones, inmediatamente después de su identificación, indicando claramente que se trata de un incidente de seguridad informática.

8.4.23 Retención y archivo de datos.

a) Mantener la integridad y disponibilidad de la información y de los servicios de procesamiento de información.
b) Estas son políticas que aplican a la Alta Dirección, Secretarios, Jefes de Oficina, Asesores, funcionarios, trabajadores oficiales y contratistas, y en general a todos los usuarios de la información que cumplan con los propósitos generales de la Alcaldía Municipal de Fusagasugá.
c) La retención de archivos debe establecer cuánto tiempo se deben mantener almacenados los archivos en cada una de las Secretarias u oficina de la Alcaldía Municipal de Fusagasugá, de acuerdo a las tablas de retención documental.
d) Las reglas y los principios generales que regulan la función archivística, se encuentran definidos por la Ley, la cual es aplicable a la administración en sus diferentes niveles producidos en función de su misión y naturaleza.
e) La ley prevé el uso de las tecnologías de la información y las comunicaciones en la administración, conservación de archivos y en la elaboración e implantación de programas de gestión de documentos.

8.4.24 Respaldo y restauración de información

a) La información de cada sistema debe ser respaldada regularmente sobre un medio de almacenamiento como CD, DVD, Discos Duros, etc.
b) Los administradores de los servidores, los sistemas de información o los equipos de comunicaciones, son los responsables de definir la frecuencia de respaldo y los requerimientos de seguridad de la información (codificación) y el administrador del sistema de respaldo, es el responsable de realizar los respaldos periódicos.
c) Todas las copias de información crítica deben ser almacenadas en un área adecuada y con control de acceso.

d) Las copias de respaldo se guardaran únicamente con el objetivo de restaurar el sistema luego de un virus informático, defectos en los discos de almacenamiento, problemas de los servidores o computadores, materialización de amenazas, catástrofes y por requerimiento legal.
e) Un plan de emergencia debe ser desarrollado para todas las aplicaciones que manejen información crítica; el dueño de la información debe asegurar que el plan es adecuado, frecuentemente actualizado y periódicamente probado y revisado.
f) Ningún tipo de información institucional puede ser almacenada en forma exclusiva en los discos duros de las estaciones de trabajo; por lo tanto, es obligación de los usuarios finales realizar las copias en las carpetas destinadas para este fin.
g) Deben existir al menos una copia de la información de los discos de red, la cual deberá permanecer fuera de las instalaciones de la Alcaldía Municipal de Fusagasugá. La restauración de copias de respaldo en ambientes de producción debe estar debidamente aprobada por el propietario de la información.
h) Semanalmente los administradores de infraestructura de la Alcaldía Municipal de Fusagasugá, verificarán la correcta ejecución de los procesos de backup, suministrarán las cintas requeridas para cada trabajo y controlarán la vida útil de cada cinta o medio empleado.
i) El Oficina de Tecnologías de la información y las Comunicaciones debe mantener un inventario actualizado de las copias de respaldo de la información y los aplicativos o sistemas de la Alcaldía Municipal de Fusagasugá
j) Los medios que vayan a ser eliminados deben surtir un proceso de borrado seguro1 y posteriormente serán eliminados o destruidos de forma adecuada.
k) Es responsabilidad de cada dependencia mantener depurada la información de las carpetas virtuales para la optimización del uso de los recursos de almacenamiento que entrega la Alcaldía Municipal de Fusagasugá a los usuarios.
a) Los usuarios de la Alcaldía Municipal de Fusagasugá deberán respaldar de manera periódica la información sensible y crítica que se encuentre en sus computadores personales o estaciones de trabajo para así garantizar la integridad de la misma, si es necesario deben solicitar asesoría de la Oficina de Tecnologías de la Información y las Comunicaciones, para evitar el robo de identidad.

8.4.25 Seguridad del centro de datos, de cableado o cuartos de equipos tecnológicos.

a) No se permite el ingreso al centro de datos, de cableado o cuartos de equipos, al personal que no esté expresamente autorizado. Se debe llevar un control de ingreso y salida del personal que visita estos sitios. En los centro de datos, de cableado o cuartos de equipos debe disponerse de una planilla para el registro, la cual debe ser diligenciada en lapicero de tinta al iniciar y finalizar la actividad a realizar.
b) El Área de Información y Sistemas debe garantizar que el control de acceso al centro de datos, de cableado o cuartos de equipos de Alcaldía Municipal de Fusagasugá, en lo posible deben contar con dispositivos electrónicos de autenticación o sistema de control biométrico.
c) La Oficina de Tecnologías de la Información y las Comunicaciones deberá garantizar que todos los equipos de los centro de datos, de cableado o cuartos de equipos, cuenten con un sistema alterno de respaldo de energía.
d) La limpieza y aseo centro de datos, de cableado o cuartos de equipos estará a cargo de la Secretaria General – Servicios Generales y debe efectuarse en presencia de un funcionario del Oficina de Tecnologías de la Información y las Comunicaciones de la Alcaldía de Fusagasugá.
e) El personal de limpieza debe ser ilustrado con respecto a las precauciones mínimas a seguir durante el proceso de limpieza. Debe prohibirse el ingreso de personal de limpieza con maletas o elementos que no sean estrictamente necesarios para su labor de limpieza y aseo.

8.4.26 Uso de discos de red o carpetas virtuales.

a) Para que los usuarios tengan acceso a la información ubicada en los discos de red, el Jefe Inmediato deberá enviar un correo autorizando el acceso y permisos, correspondientes al rol y funciones a desempeñar Oficina de Tecnologías de la Información y las Comunicaciones de la Alcaldía de Fusagasugá. Los usuarios tendrán permisos de escritura, lectura o modificación de información en los discos de red, dependiendo de sus funciones y su rol.
b) La información institucional que se trabaje en las estaciones cliente de cada usuario debe ser trasladada periódicamente a los discos de red por ser información institucional.
c) La información almacenada en cualquiera de los discos de red debe ser de carácter institucional.
d) Está prohibido almacenar archivos con contenido que atente contra la moral y las buenas costumbres de la entidad o las personas, como pornografía, propaganda racista, terrorista o cualquier software ilegal o malicioso, ya sea

en medios de almacenamiento de estaciones de trabajo, computadores de escritorio o portátiles, tablets, celulares inteligentes, etc. o en los discos de red.

e) Se prohíbe extraer, divulgar o publicar información de cualquiera de los discos de red o estaciones de trabajo, sin expresa autorización de su Jefe inmediato.
f) Se prohíbe el uso de la información de los discos de red con fines publicitarios, de imagen negativa, lucrativa o comercial.
g) La responsabilidad de generar las copias de respaldo de la información de los discos de red, está a cargo de la Oficina de Tecnologías de la Información y las Comunicaciones de la Alcaldía de Fusagasugá.
h) La responsabilidad de custodiar la información en copias de respaldo controladas, fuera de las instalaciones de la Alcaldía de Fusagasugá, estará a cargo de la Oficina de Tecnologías de la Información y las Comunicaciones de la Alcaldía de Fusagasugá.
i) Las claves, archivos y equipos compartidos en las compañías se prestan para realizar delitos informáticos directos, con la publicación de una clave (ya sea a una persona de confianza o no) esta pierde el valor de privada y es una puerta abierta a los delincuentes informáticos.
j) Las claves son personales e intransferibles, los empleados de la Alcaldía Municipal de Fusagasugá serán responsables por los actos ocasionados desde una cuenta o equipo especifico, en caso de que se demuestre lo contrario el usuario deberá sustentar los actos ocurridos.
k) El usuario que tenga bajo su resguardo algún equipo de cómputo será responsable de su uso y custodia; en consecuencia, responderá por dicho bien, se implementarán documentos en los que se valide la información de los empleados con relación a sus equipos.

8.4.27 Uso de impresoras, servicio de Impresión y documentos físicos

a) Los documentos que se impriman en las impresoras de la Alcaldía de Fusagasugá deben ser de carácter institucional.
b) Es responsabilidad del usuario conocer el adecuado manejo de los equipos de impresión (escáner y fotocopiado) para que no se afecte su correcto funcionamiento.
c) Ningún usuario debe realizar labores de reparación o mantenimiento de las impresoras. En caso de presentarse alguna falla, esta se debe reportar a la Oficina de Tecnologías de la Información y las Comunicaciones de la Alcaldía de Fusagasugá.
d) La documentación en papel no debe de ser accesible por personal no autorizado. Se evitará dejar documentos en las impresoras y fotocopiadoras, así como en sitios de paso o de atención al público.

e) Si la función no lo requiere, queda prohibida la impresión física de documentos que contenga información de la Alcaldía Municipal de Fusagasugá.

8.4.29 Seguridad aplicables contra virus, gusanos y troyanos.

Los virus, gusanos y troyanos son elementos maliciosos en una red conocidos generalmente como malware, los cuales pueden ser implantados de forma manual en un sistema o de manera automática mediante una replicación de correos electrónicos, programas en dispositivos de almacenamiento masivo o ejecuciones en segundo plano de un software encriptado.

Para la disminución de riesgos y vulnerabilidades que generan los diferentes tipos de malware mencionados se recomienda la implementación de las siguientes políticas de seguridad de la información en la Alcaldía Municipal de Fusagasugá:

a) Los usuarios de la Alcaldía Municipal de Fusagasugá deberán utilizar los mecanismos institucionales para proteger la información que reside y utiliza la infraestructura de la organización.
b) Se deberán proteger y proceder con la correcta administración de la información reservada o confidencial que por necesidades de la organización deba ser almacenada o transmitida, ya sea dentro de la red interna de la Alcaldía Municipal o hacia redes externas hacia los servidores empresariales, el servidor de bases de datos que responde a las consultas externas es prioridad.
c) Para garantizar la correcta utilización del software de firewall y antivirus la Alcaldía Municipal de Fusagasugá establece que por lo menos una vez cada tres meses capacitará al personal en temas de seguridad informática.

8.5 SELECCIÓN DE PROTOCOLOS DE SEGURIDAD REQUERIDOS POR LA OFICINA TIC, DE ACUERDO A LOS RIESGOS INFORMÁTICOS

Una vez se analizaron los riesgos, fue necesario verificar cuales serían los protocolos que ayudaran en la gestión del riesgo informático a generar medidas de respuesta que permitan valorar los riesgos nuevamente y clasificarlos en un impacto y evaluación baja. De acuerdo a los veintinueve (29) protocolos de políticas de seguridad de la información se seleccionaron así:

Tabla 6. Selección de protocolos de seguridad requeridos por la Oficina TIC, de acuerdo a los riesgos informáticos

RIESGO	CALIFICACIÓN		TIPO DE IMPACTO	EVALUACIÓN	MEDIDAS DE RESPUESTA	SELECCIÓN DE PROTOCOLOS
	Probabilidad	Impacto				
Fallas o suspensión en la prestación de servicios de energía eléctrica.	5	4	Operativo 5	Zona de Riesgo Extrema	Transferir el riesgo al proceso de Apoyo Gestión Administrativa y misional Planificación y desarrollo Integral del riesgo	**Respaldo y continuidad del negocio**
Daños y pérdidas en equipos tecnológicos por catástrofes naturales.	2	5	Operativo 5	Zona de Riesgo Extrema	Evitar y compartir el riesgo con el proceso de Gestión rural ambiental y del riesgo	
Fallas en la prestación de los servicios de tecnologías de la información y las comunicaciones (internet y telefonía).	5	3	Operativo 5, Credibilidad o Imagen 4	Zona de Riesgo Extrema	Reducir el riesgo	
Atentados contra la confidencialidad, la integridad y la disponibilidad de los datos y de los sistemas informáticos.	2	4	Confidencialidad de la información 1, Operativo 4	Zona de Riesgo Alta	Reducir el riesgo	**Respaldo y continuidad del negocio** **Pruebas de seguridad** **Creación o propagación intencionada** **Control de la Información** **Uso correcto de contraseñas** **Manejo de Claves** **Vinculación De Personal** **Acceso Lógico y Físico**
Atentados informáticos y otras infracciones.	2	4	Confidencialidad de la información 1, Operativo 4	Zona de Riesgo Extrema	Evitar el riesgo	
Acciones terroristas y de orden público.	2	4	Operativo 5	Zona de Riesgo Alta	Evitar y compartir el riesgo con el proceso misional Convivencia y Seguridad Ciudadana	

Inadecuada o insuficiente infraestructura TIC actualizada.	3	2	Operativo 4	Zona de Riesgo Moderada	Reducir y compartir el riesgo con el proceso de apoyo Hacienda Pública	**Asignación de recursos presupuestales** **Respaldo y continuidad del negocio** **Pruebas de seguridad**
Inadecuada o insuficiente infraestructura TIC de respaldo o backup.	3	2	Operativa 4	Zona de Riesgo Moderada	Reducir y compartir el riesgo con el proceso de apoyo Hacienda Pública	
Insuficiente infraestructura tecnológica para suplir la demanda de servicios requeridos por los funcionarios.	3	2	Operativa 4	Zona de Riesgo Moderada	Transferir el riesgo al proceso de apoyo Gestión Administrativa	
Desconocimiento de la infraestructura tecnológica implementada.	3	3	Operativa 4, Credibilidad o Imagen 2.	Zona de Riesgo Alta	Evitar el riesgo	**Vinculación De Personal** **Acceso Lógico y Físico** **Parches de Seguridad**
Administración inadecuada de la infraestructura tecnología.	3	4	Operativa 4, Credibilidad o Imagen 1.	Zona de Riesgo Extrema	Evitar el riesgo	
Equipos desactualizados o con inconvenientes en su funcionamiento.	4	3	Operativa 4	Zona de Riesgo Alta	Transferir el riesgo al proceso de apoyo Gestión Administrativa	**Pruebas de seguridad**
Disponibilidad de recursos financieros para la compra y suministro de equipos, servicios de mantenimiento, internet, y/o actualización de la infraestructura tecnológica.	3	3	Operativa 4	Zona de Riesgo Alta	Transferir el riesgo al proceso de Direccionamiento Estratégico, Hacienda Pública y Gestión Administrativa	**Asignación de recursos presupuestales**
Daño total o parcial de infraestructura tecnológica.	4	3	Operativa 4	Zona de Riesgo Alta	Reducir el riesgo	**Asignación de recursos presupuestales** **Respaldo y continuidad del negocio**

Fuente: Alcaldía de Fusagasugá

8.6 MODELO DE SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN (SGSI)

La Alcaldía de Fusagasugá, dentro de su Política Publica en Tecnologías de la Información y las Comunicaciones, aprobada mediante Acuerdo Municipal 044 de 2012, ha considerado dar cumplimiento a la Ley 1341 de 2009, lineamientos del Ministerio de Tecnologías de la Información y las Comunicación, Modelo de Seguridad y Privacidad de la Información, y la Estrategia de Gobierno, para lo

cual aplicará el Modelo de Sistemas de Gestión de Seguridad de la información (SGSI), aplicar las fases del ciclo PHVA, así como el estándar NTC:ISO/IEC 27001 que se complementa con el Modelo Estándar de Control Interno (MECI) para las entidades públicas.

La Administración municipal ha proyectado dentro de su Política Publica en TICs "FUSAGASUGÁ DIGITAL: EJE DE LA REGIÓN INTELIGENTE", mediante la cual fomenta y facilita a la ciudadanía el buen uso de las Tecnologías de la Información y Comunicación en la ciudadanía. En la actualidad la Alcaldía de Fusagasugá ha demostrado un gran impacto, desde la creación mediante Decreto No. 273 de 2015, se convirtió en la primera Oficina de Tecnologías de la Información y las Comunicaciones del Departamento, situación que ha facilitado la gerencia en cuanto a la infraestructura, los servicios, las aplicaciones y los usuarios en el marco de un ecosistema digital; es por ello que surge la necesidad de reconocer la seguridad informática como un factor primordial para la apropiación de las TIC; la constante evolución de los mercados; y la dinámica de las entidades, para lo cual la Alcaldía de Fusagasugá y en cumplimiento de lineamientos del Ministerio de Tecnologías de la Información y las Comunicaciones (MinTic).

8.6.1 Modelo de Seguridad y Privacidad de la Información (MSPI). La Alcaldía de Fusagasugá proyecta que una vez implementado del Sistema de Gestión de Seguridad de la Información (SGSI) tomando como referencia el Modelo de Seguridad y Privacidad de la Información de MinTic, puede cumplir con los principios definidos en la Ley 1341 de 2009 y en la Estrategia de Gobierno en línea, para lo cual la entidad ya contará un Modelo de Sistema Gestión de Seguridad de la información (SGSI) alineado a la metodología del ciclo PHVA que también se aplican en el manual de Gobierno en línea 3.0, así como políticas, protocolos y procedimientos de seguridad adecuados que garanticen la responsabilidad y la orientación para preservar los pilares fundamentales de la seguridad de la información:

- **Confidencialidad:** La información debe ser accesible sólo a aquellas personas autorizadas.
- **Integridad:** La información y sus métodos de procesamiento deben ser completos y exactos.
- **Disponibilidad:** La información y los servicios deben estar disponible cuando se le requiera.[13]

[13] Modelo de Seguridad de la Información para la Estrategia de Gobierno en línea 2.0, MinTic http://css.mintic.gov.co/ap/gel4/images/Modelo_Seguridad_Informacion_2_01.pdf

Basados en lo anterior, la Administración Municipal ha fijado el compromiso institucional para dar aplicación al Sistema de Gestión de Seguridad de la Información (SGSI) por parte de todos niveles involucrados dentro de la entidad, de tal forma que tengan claro los beneficios que se pueden obtener con una cultura organizacional enfocada a la seguridad, que permita basados en los riesgos informáticos identificados realizar una mejor gestión (lo cual incluye el análisis, la identificación de controles adecuados, su implementación, su medición y mejora continua), sea aprobada y apoyada con los recursos necesarios a través de todas las etapas e instancias del sistema.

El Modelo de Sistema de Gestión de Seguridad de la Información (SGSI) que se plantea reúne la sostenibilidad y el conjunto de Lineamientos, Políticas, Normas, Procesos e Instituciones que proveen y promueven la puesta en marcha, supervisión, mejora y control tal como lo señala el Modelo de Seguridad y Privacidad de la Información (MSPI) alineado con la Estrategia de Gobierno en Línea definida en manual GEL 3.0.

8.6.2 Fases del Modelo de Operación de Seguridad y Privacidad de la Información (MOSPI). El Modelo de Seguridad y Privacidad de la Información diseñado por MinTic se encuentra alineado con el Marco de Referencia de Arquitectura Empresarial para la Gestión de TI y la Estrategia de Gobierno en línea, adicional a ello incluye la actualización del modelo de seguridad de la información para gobierno en línea, “versión 2.0”, plan de operación, modelo de madurez, entre otros; por consiguiente es tenido en cuenta para el Modelo de Sistema de Gestión de Seguridad de la Información de la Alcaldía de Fusagasugá.

El modelo de operación establece cinco (5) fases o componentes que comprenden los objetivos, metas y herramientas que permiten que la seguridad y privacidad de la información como un sistema de gestión sostenible dentro de las entidades territoriales:

- Componente Diagnostico
- Componente Planificación
- Componente Implementación
- Componente Gestión y/o evaluación de desempeño
- Componente Mejora Continua

Figura 30. Marco de Seguridad y Privacidad de la Información

Fuente: Modelo de Privacidad y Seguridad de la información - MinTic

Dentro de la ciclo PHVA (Planear, Hacer, Verifica y Actuar) para el modelo de implementación del Sistema de Gestión de Seguridad de la información (SGSI) podemos clasificar las fases del modelo de seguridad y privacidad de la información como:

- **PLANEAR:** Componente de Diagnóstico y Planificación
- **HACER:** Componente de Implementación
- **VERIFICAR:** Componente de gestión y/o evaluación de desempeño
- **ACTUAR:** Componente mejora continua

8.6.3 Componente de Diagnostico (Ciclo PHVA: Planear). Este componente pretende que la Alcaldía de Fusagasugá determine herramientas que le permitan evaluar el nivel de madurez de seguridad y privacidad de la información de la entidad, para lo cual debe producir documentos con el resultado de la etapa de diagnóstico.

Tabla 7. Componente de Diagnostico MOSPI

Modelo Sistema de Gestión de Seguridad de la Información (SGSI)			
COMPONENTE DE DIAGNOSTICO - CICLO PHVA (Planear)			
No.	**Metas del Modelo de Seguridad y Privacidad de la Información**	**Entregables Alcaldía de Fusagasugá**	**Estado Actual frente al requerimiento del Modelo de Seguridad y Privacidad de la Información**
1	Determinar el estado actual de la gestión de seguridad y privacidad de la información al interior de la Entidad, teniendo en cuenta la infraestructura de red de comunicaciones (IPv4/IPv6). Para lo cual MinTic sugiere Ver, guía para el aseguramiento del protocolo IPv6.	Documento con el resultado de la autoevaluación realizada a la Entidad, de la gestión de seguridad y privacidad de la información e infraestructura de red de comunicaciones (IPv4/IPv6), revisado y aprobado por la alta dirección y Sistema Integrado de Gestión MECI-Calidad de la Alcaldía de Fusagasugá.	PENDIENTE: Aun no se encuentra elaborado el documento de resultados de la autoevaluación realizada a la entidad para la información e infraestructura de red de comunicaciones (IPv4 e IPv6).
2	Identificar el nivel de madurez de seguridad y privacidad de la información en la Entidad. Para lo cual MinTic sugiere Ver Guía para la encuesta de diagnóstico del Modelo de Seguridad de la Información.	Documento con el resultado de la herramienta de la encuesta, revisado, aprobado y aceptado por la alta dirección y Sistema Integrado de Gestión MECI-Calidad de la Alcaldía de Fusagasugá.	Durante el desarrollo del proyecto de grado se aplicaron encuestas básicas para evidenciar la necesidad de diseñar un modelo de sistema de gestión de Seguridad de la Información, y se realizó el análisis y resultado de los datos. PENDIENTE: La Alcaldía de Fusagasugá debe aplicar encuestas de diagnóstico que abarque más temas relacionados con el nivel de madurez de seguridad y privacidad de la información.
3	Realizar pruebas que permitan a la Entidad medir la efectividad de los controles existentes.	Documento con el resultado de la estratificación de la entidad, aceptado y aprobado por la dirección.	Actualmente la Alcaldía de Fusagasugá cuenta con algunos manuales, protocolos, procedimientos y formatos relacionados con las actividades del proceso de apoyo denominado GESTIÓN TIC del Sistema Integrado de Gestión MECI-Calidad, PENDIENTE: Utilizar mecanismos de medición que permitan medir la efectividad de los controles existentes en temas de seguridad y privacidad de la información, así como los procedimientos establecidos para los actividades y servicios TIC que se brindan en la organización.

Fuente: Modelo de Operación Seguridad y Privacidad de la Información, e información de la Alcaldía de Fusagasugá

8.6.4 Componente de Planeación (Ciclo PHVA: Planear). Este componente pretende que la Alcaldía de Fusagasugá, defina la estrategia metodológica, que permita establecer el alcance, objetivos, procesos y procedimientos, pertinentes a la gestión del riesgo y mejora de seguridad de la información; este resultado le permitirá dar cumplimiento con las metas propuestas del MSPI.

Tabla 8. Componente de Planificación MOSPI

Modelo Sistema de Gestión de Seguridad de la Información (SGSI)			
COMPONENTE DE PLANEACIÓN - CICLO PHVA (Planear)			
No.	**Metas del Modelo de Seguridad y Privacidad de la Información**	**Entregables Alcaldía de Fusagasugá**	**Estado Actual frente al requerimiento del Modelo de Seguridad y Privacidad de la Información**
1	Objetivos, alcance y límites del Modelo de Seguridad y Privacidad de la Información (MSPI).	Documento con el alcance y límites de la seguridad de la información, debidamente aprobado y socializado al interior de la Entidad, por la alta dirección y el Sistema Integrado de Gestión MECI-Calidad de la Alcaldía de Fusagasugá.	Actualmente se tiene aprobado el MA-GT-001 Manual para el uso adecuado de la infraestructura tecnológica y el PT-GT-001 Protocolo de servicios informáticos y compromiso de confidencialidad sobre tratamiento de datos. PENDIENTE: Adelantar un documento con lo requerido para el Sistema de Gestión de Seguridad y Privacidad de la Información, políticas y protocolos de seguridad basados en el Modelo de Privacidad y Seguridad de la Información de MinTIC: documento que debe ser aprobado mediante Acto administrativo por la Entidad, la alta dirección y el Sistema Integrado de Gestión MECI-Calidad de la Alcaldía de Fusagasugá.
2		Acto administrativo a través del cual se crea o se modifica las funciones del comité gestión institucional (ó el que haga sus veces), en donde se incluyan los temas de seguridad de la información en la entidad, revisado y aprobado por la alta Dirección y el Sistema Integrado de Gestión MECI-Calidad de la Alcaldía de Fusagasugá.	
3	Políticas de seguridad y privacidad de la información. Para lo cual MinTic sugiere Ver, guía de políticas de seguridad y privacidad de la información.	Documento con las políticas de seguridad y privacidad de la información, debidamente aprobadas y socializadas al interior de la Entidad, por la alta Dirección y el Sistema Integrado de Gestión MECI-Calidad de la Alcaldía de Fusagasugá.	PENDIENTE: La Alcaldía de Fusagasugá aún no cuenta con dichas políticas, pero uno de los productos generados por el proyecto de grado son los protocolos y/o políticas de seguridad de la información, las cuales aportaran un adelantó significativo para la Entidad, pueden mejorarse y adicionarse de acuerdo a la necesidad para su aprobación.
4	Procedimientos de control documental del Modelo de Seguridad y Privacidad de la Información (MSPI).	Formatos de procesos y procedimientos, debidamente definidos, establecidos y aprobados por el comité que integre los sistemas de gestión institucional, en este caso el Sistema Integrado de Gestión MECI-Calidad de la Alcaldía de Fusagasugá.	A pesar que la Alcaldía de Fusagasugá cuenta con algunos manuales, protocolos, procedimientos y formatos relacionados con las actividades del proceso de apoyo denominado GESTIÓN TIC del Sistema Integrado de Gestión MECI-Calidad, tiene PENDIENTE: adelantar los formatos, procesos y procedimientos de control para la seguridad y la privacidad de la información con su respectiva aprobación.

5	Inventario de activos de información. Para lo cual MinTic sugiere Ver, Guía de clasificación de activos de información.	Documento de inventario de activo de información, revisado y aprobado por la alta Dirección y el Sistema Integrado de Gestión MECI-Calidad de la Alcaldía de Fusagasugá.	Actualmente la entidad adelanta el proyecto de inventario e identificación de activos informáticos de software, hardware, sistemas de información y plataformas tecnológicas, usuarios, redes y equipos telemáticos, apoyados de unos formatos estandarizados. PENDIENTE: Aprobar los formatos e inventario existente y diseñar el formato de identificación de activos de información estableciendo los niveles de confidencialidad y custodia de la información pública, uso interno, restringido y reservado, de acuerdo a la Ley 712 de 2015.
6	Acciones para tratar riesgos y oportunidades de seguridad de la información. Debe incluir Identificación y valoración de riesgos de (Metodología, Reportes) y Tratamiento de riesgos (Selección de controles). Para lo cual MinTic sugiere Ver, guía de gestión del riesgo.	Documento con el informe de análisis de riesgos, matriz de riesgos, plan de tratamiento de riesgos y declaración de aplicabilidad, revisado y aprobado por la alta Dirección y el Sistema Integrado de Gestión MECI-Calidad de la Alcaldía de Fusagasugá.	La Alcaldía de Fusagasugá para la gestión de los riesgos de los procesos misionales, apoyo, estratégicos y de evaluación del Sistema Integrado MECI-Calidad ha tomado como referencia la Guía de Administración de Riesgos del Departamento Administrativo de la Función Pública (DAFP). A pesar que el proceso de GESTION TIC ya tiene identificado algunos riesgos queda PENDIENTE: analizar y gestionar los riesgos y oportunidades de seguridad de la información, con su respectiva aprobación.
7	Asignación de recurso humano, comunicación de roles y responsabilidades de seguridad y privacidad de la información. Toma de conciencia.	Documento con el plan de comunicación, sensibilización y capacitación, con los respectivos soportes, revisado y aprobado por la alta Dirección y el y el Sistema Integrado de Gestión MECI-Calidad de la Alcaldía de Fusagasugá.	Por el momento la Alcaldía de Fusagasugá no cuenta con planes de capacitación, sensibilización y comunicación en temas de seguridad y privacidad de la información, tal como se evidencio en el análisis y resultados de las encuestas aplicadas a la entidad durante el desarrollo del proyecto de grado, por consiguiente queda PENDIENTE: Establecer un plan de comunicación y sensibilización de seguridad y privacidad de la información, así como incluir dentro de los planes de capacitación temas como ingeniera social, tratamiento, seguridad y privacidad de la información. Dar a conocer la normatividad en Colombia frente al uso de las TIC y delitos informáticos como: Decreto 1377 de 2013, Ley Estatutaria 1581 de 2012, Ley 1474 de 2011, Ley 1273 de 2009, Ley Estatutaria 1266 de 2008, Ley 734 de 2002, Ley 599 de 2000 y Ley 52 de 1999.
8	Plan y estrategia de transición de IPv4 a IPv6. Ver, Guía de transición de IPV4 a IPv6 para Colombia, circular 0002 del 6 de julio 2011.	Documento con el plan y estrategia de transición de IPv4 a IPv6, revisado y aprobado por la alta Dirección.	PENDIENTE: Aun no se encuentra elaborado el plan de transición de la información e infraestructura de red de comunicaciones de IPv4 a IPv6. Debe elaborarse y ser aprobado.

Fuente: Modelo de Operación Seguridad y Privacidad de la Información, e información de la Alcaldía de Fusagasugá

8.6.5 Componente de Implementación (Ciclo PHVA: Hacer). Este componente le permitirá a la Alcaldía de Fusagasugá llevar acabo la implementación del componente de planificación del Modelo de Seguridad y Privacidad de la Información (MSPI), teniendo en cuenta los aspectos más relevantes en los procesos de implementación del MSPI. Para desarrollar la estrategia por parte de la Alcaldía de Fusagasugá se deben ejecutar las actividades necesarias para el cumplimiento de las metas definidas, para lograr la implementación y puesta en marcha del MSPI en la Entidad, con el fin de abarcar dentro de esta gestión los procesos de la Entidad de manera organizada y planificada teniendo en cuenta el contexto de la Alcaldía de Fusagasugá.

Tabla 9. Componente de Implementación MOSPI

Modelo Sistema de Gestión de Seguridad de la Información (SGSI)			
COMPONENTE DE IMPLEMENTACIÓN - CICLO PHVA (Hacer)			
No.	**Metas del Modelo de Seguridad y Privacidad de la Información**	**Entregables Alcaldía de Fusagasugá**	**Estado Actual frente al requerimiento del Modelo de Seguridad y Privacidad de la Información**
1	Planificación y control operacional.	Documento con la estrategia de planificación y control operacional, revisado y aprobado por la alta Dirección y el y el Sistema Integrado de Gestión MECI-Calidad de la Alcaldía de Fusagasugá.	PENDIENTE: Elaborar plan o estrategia de planificación y control operacional para la seguridad de la información, tomando como referencia la guía de controles y seguridad de MinTIC para el Modelo.
2	Implementación de controles. Ver, Guía de Controles y seguridad de la información.		
3	Implementación del plan de tratamiento de riesgos. Ver, Guía de gestión del riesgo.	Documento con el informe del plan de tratamiento de riesgos, que incluya la implementación de controles de acuerdo con lo definido en la declaración de aplicabilidad, revisado y aprobado por la alta Dirección y el Sistema Integrado de Gestión MECI-Calidad de la Alcaldía de Fusagasugá.	La Alcaldía de Fusagasugá para la gestión del proceso GESTION TIC del Sistema Integrado MECI-Calidad ha tomado como referencia la Guía para tratamiento de riesgos de seguridad de la información, y si lo desea puede alinearlos con la Guía de Administración de Riesgos del Departamento Administrativo de la Función Pública (DAFP). PENDIENTE: Elaborar el plan de tratamiento de riesgos para seguridad de la información.
4	Implementación del plan y estrategia de transición de IPv4 a IPv6. Ver, Guía de transición de IPV4 a IPv6 para Colombia, circular 0002 del 6 de julio 2011.	Indicadores de gestión del MSPI, revisado y aprobado por la alta Dirección. Documento con el informe de la implementación del plan y la estrategia de transición de IPv4 a IPv6, revisado y aprobado por la alta Dirección y el Sistema Integrado de Gestión MECI-Calidad de la Alcaldía de Fusagasugá.	PENDIENTE: Elaborar plan o estrategia de transición del IPv4 a IPv6, y formular los indicadores de gestión que permitan medir la efectividad del modelo de seguridad y privacidad de la información.
5	Indicadores de gestión del Modelo de Seguridad y Privacidad de la Información (MSPI). Ver, Guía de indicadores de la gestión para la seguridad de la información.		

Fuente: Modelo de Operación Seguridad y Privacidad de la Información, e información de la Alcaldía de Fusagasugá

8.6.6 Componente de Evaluación de desempeño (Ciclo PHVA: Verificar). Este componente le permitirá a la Alcaldía de Fusagasugá, evaluar el desempeño y la eficacia del Modelo de Seguridad y Privacidad de la Información (MSPI), a través de instrumentos que permita determinar la efectividad de la implantación del MSPI. Para esta medición se deben tomar los indicadores definidos en el componente de implementación para llevar a cabo el plan de seguimiento, evaluación y análisis del MSPI.

Tabla 10. Componente de Evaluación y Desempeño MOSPI

Modelo Sistema de Gestión de Seguridad de la Información (SGSI)			
COMPONENTE DE EVALUACIÓN Y DESEMPEÑO - CICLO PHVA (Verificar)			
No.	**Metas del Modelo de Seguridad y Privacidad de la Información**	**Entregables Alcaldía de Fusagasugá**	**Estado Actual frente al requerimiento del Modelo de Seguridad y Privacidad de la Información**
1	Plan de seguimiento, evaluación y análisis del MSPI.	Documento con el plan de seguimiento, evaluación, análisis y resultados del MSPI, revisado y aprobado por la alta Dirección y el Sistema Integrado de Gestión MECI-Calidad de la Alcaldía de Fusagasugá.	PENDIENTE: La Alcaldía de Fusagasugá debe establecer el plan de seguimiento, evaluación, análisis y resultados del Modelo de Seguridad y Privacidad de la Información, estableciendo la frecuencia de medición y datos gerenciales para la organización.
2	Auditoria Interna.	Documento con el plan de auditorías internas y resultados, de acuerdo a lo establecido en el plan de auditorías, revisado y aprobado por la alta Dirección y el Sistema Integrado de Gestión MECI-Calidad de la Alcaldía de Fusagasugá.	PENDIENTE: La Alcaldía debe incluir dentro del plan de auditorías internas que viene realizando hace 2 años para MECI y CALIDAD, la auditoria para el Sistema de Gestión de Seguridad de la Información, capacitar a los treinta (30) auditores internos en la norma ISO/IEC 27001, 27002 y demás concordantes. El plan de auditoria y capacitación debe ser aprobado. En lo posible certificar los auditores en la norma.
3	Evaluación del plan de tratamiento de riesgos.	Resultado del seguimiento, evaluación y análisis del plan de tratamiento de riesgos, revisado y aprobado por la alta Dirección y el Sistema Integrado de Gestión MECI-Calidad de la Alcaldía de Fusagasugá.	PENDIENTE: La Alcaldía de Fusagasugá debe establecer el plan de tratamiento de riesgos para el sistema de gestión de seguridad de la información, para ello puede aplicar la guía de gestión de riesgos del Modelo de Seguridad y Privacidad de la Información de MinTIC.

Fuente: Modelo de Operación Seguridad y Privacidad de la Información, e información de la Alcaldía de Fusagasugá

8.6.5 Componente de Mejora Continua (Ciclo PHVA: Actuar). Este componente le permitirá a la Alcaldía de Fusagasugá, consolidar los resultados obtenidos del componente de evaluación de desempeño, para diseñar el plan de mejoramiento continuo de seguridad y privacidad de la información, que permita realizar el plan de implementación de las acciones correctivas identificadas para el MSPI.

Tabla 11. Componente de Mejora Continua MOSPI

Modelo Sistema de Gestión de Seguridad de la Información (SGSI)			
COMPONENTE DE MEJORA CONTINUA - CICLO PHVA (Actuar)			
No.	**Metas del Modelo de Seguridad y Privacidad de la Información**	**Entregables Alcaldía de Fusagasugá**	**Estado Actual frente al requerimiento del Modelo de Seguridad y Privacidad de la Información**
1	Plan de seguimiento, evaluación y análisis para el MSPI.	Documento con el plan de seguimiento, evaluación y análisis para el MSPI, revisado y aprobado por la alta Dirección y el Sistema Integrado de gestión MECI-Calidad de la Alcaldía de Fusagasugá.	PENDIENTE: La Alcaldía de Fusagasugá debe tener en cuenta los resultados del plan de seguimiento, evaluación y análisis del Sistema de Gestión de Seguridad de la información para establecer el plan de mejoramiento del sistema que permita garantizar la seguridad y privacidad de la información conforme a lo requerido por la entidad y el modelo establecido por MinTIC con el marco legal y normativo que lo regula.
2	Auditoria Interna.	Documento con el consolidado de las auditorías realizadas de acuerdo con el plan de auditorías, revisado y aprobado por la alta Dirección y el Sistema Integrado de gestión MECI-Calidad de la Alcaldía de Fusagasugá.	PENDIENTE: La Alcaldía de Fusagasugá debe tener en cuenta los resultados del informe de auditoría final realizado al Sistema de Gestión de Seguridad de la información, con el fin de determinar los aspectos favorables (fortalezas), débiles (oportunidades de mejora) y las NO CONFORMIDADES, para lo cual debe establecer el plan de mejoramiento del sistema que permita garantizar el cumplimiento de los requisitos de la norma ISO/IEC 27001, 27002 y demás.
3	Comunicación de resultados y plan de mejoramiento.		
4	Revisión y aprobación por la alta Dirección.		

Fuente: Modelo de Operación Seguridad y Privacidad de la Información, e información de la Alcaldía de Fusagasugá

8.6.7 Controles para el Modelo de Seguridad y Privacidad de la Información. Teniendo en cuenta los lineamientos del Modelo de Seguridad y Privacidad de la Información, a continuación se a conocer los controles que se deben tener en cuenta la Alcaldía de Fusagasugá.

Tabla 12. Controles del Modelo de Seguridad y Privacidad de la Información

NIVEL	Controles Modelo de Seguridad y Privacidad de la Información
Inicial	**8. GESTIÓN DE ACTIVOS** 8.2 Clasificación de la Información
Gestionado	**5. POLITICA DE SEGURIDAD** 5.1 Directrices de la Dirección en seguridad de la información. **6. ASPECTOS ORGANIZATIVOS DE LA SEGURIDAD DE LA INFORMACIÓN** 6.1 Organización interna. 6.2 Dispositivos para movilidad y teletrabajo. **8. GESTIÓN DE ACTIVOS** 8.1 Responsabilidad sobre los activos. **12. SEGURIDAD EN LA OPERATIVA.** 12.2 Protección contra código malicioso. 12.3 Copias de seguridad. 12.6 Gestión de la vulnerabilidad técnica. **16. GESTIÓN DE INCIDENTES EN LA SEGURIDAD DE LA INFORMACIÓN.** 16.1 Responsabilidades y procedimientos. **17. ASPECTOS DE SEGURIDAD DE LA INFORMACION EN LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO.** 17.1.1 Planificación de la continuidad de la seguridad de la información.
Definido	**7. SEGURIDAD LIGADA A LOS RECURSOS HUMANOS.** 7.1 Antes de la contratación. 7.2 Durante la contratación. 7.3 Cese o cambio de puesto de trabajo. **9. CONTROL DE ACCESOS.** 9.1 Requisitos de negocio para el control de accesos. 9.3 Responsabilidades del usuario. **11. SEGURIDAD FÍSICA Y AMBIENTAL** 11.1 Áreas seguras 11.2 Seguridad de los equipos. **12. SEGURIDAD EN LA OPERATIVA.** 12.1 Responsabilidades y procedimientos de operación. 12.5 Control del software en explotación. **13. SEGURIDAD EN LAS TELECOMUNICACIONES.** 13.1 Gestión de la seguridad en las redes. 13.2 Intercambio de información con partes externas. **14. ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE LOS SISTEMAS DE INFORMACIÓN.** 14.1 Requisitos de seguridad de los sistemas de información. 14.2 Seguridad en los procesos de desarrollo y soporte. 14.3 Datos de prueba. **16. GESTIÓN DE INCIDENTES EN LA SEGURIDAD DE LA INFORMACIÓN.** 16.2 Notificación de los eventos de seguridad de la información. 16.1.3 Notificación de puntos débiles de la seguridad. 16.1.7 Recopilación de evidencias. **17. ASPECTOS DE SEGURIDAD DE LA INFORMACION EN LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO.** 17.1.2 Implantación de la continuidad de la seguridad de la información. **15. RELACIONES CON SUMINISTRADORES** 15.1 Seguridad de la información en las relaciones con suministradores. 15.2 Gestión de la prestación del servicio por suministradores.
Gestionado Cuantitativamente	**9. CONTROL DE ACCESOS.** 9.2 Gestión de acceso de usuario. 9.4 Control de acceso a sistemas y aplicaciones **10. CIFRADO** 10.1 Controles Criptográficos **12. SEGURIDAD EN LA OPERATIVA.** 12.7 Consideraciones de las auditorías de los sistemas de información. 12.4 Registro de actividad y supervisión. **16. GESTIÓN DE INCIDENTES EN LA SEGURIDAD DE LA INFORMACIÓN.** 16.1.4 Valoración de eventos de seguridad de la información y toma de decisiones. 16.1.5 Respuesta a los incidentes de seguridad. **18. CUMPLIMIENTO.** 18.1 Cumplimiento de los requisitos legales y contractuales.

Optimizado	**18. CUMPLIMIENTO** 18.2 Revisiones de la seguridad de la información. **16. GESTIÓN DE INCIDENTES EN LA SEGURIDAD DE LA INFORMACIÓN.** 16.1.6 Aprendizaje de los incidentes de seguridad de la información. **17. ASPECTOS DE SEGURIDAD DE LA INFORMACION EN LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO**. Verificación, revisión y evaluación de la continuidad de la seguridad de la información.

Fuente: Modelo de Seguridad y Privacidad de la Información - MinTIC

8.6.8 Sujetos Obligados del Orden Territorial a cumplir con MPSI. El Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC), a través del Modelo de Seguridad y Privacidad de la Información (MPSI), ha establecido cuales son los sujetos del orden nacional y territorial para el cumplimiento de esta política de seguridad; para el caso de la Alcaldía de Fusagasugá es un Municipio del orden territorial de categoría 2, por consiguiente, y según la clasificación los sujetos obligados a cumplir con el modelo la organización estaría enmarcada en la clasificación B.

A. Gobernaciones de categoría Especial y Primera; alcaldías de categoría Especial, y demás sujetos obligados de la administración publica en el mismo nivel.
B. Gobernaciones de categoría segunda, tercera y cuarta; alcaldías de categoría primera, segunda y tercera y demás sujetos obligados de la Administración Pública en el mismo nivel.
C. Alcaldías de categoría cuarta, quinta y sexta y demás sujetos obligados de la Administración Pública en el mismo nivel.

Para las entidades agrupadas en A, B y C los plazos serán los siguientes:

Figura 31. Plazo para entidades agrupadas en A, B y C para cumplir con MPSI

Componente/Año	Entidades A (%)					
	2015	2016	2017	2018	2019	2020
TIC para ser servicios	70%	90%	100%	Mantener 100%	Mantener 100%	Mantener 100%
TIC para Gobierno abierto	80%	95%	100%	Mantener 100%	Mantener 100%	Mantener 100%
TIC para la Gestión	20%	45%	80%	100%	Mantener 100%	Mantener 100%
Seguridad y Privacidad de la Información	**35%**	**50%**	**80%**	**100%**	**Mantener 100%**	**Mantener 100%**

Fuente: Modelo de Seguridad y Privacidad de la Información - MinTIC

9. FASE VERIFICAR CICLO PHVA

9.1 VALIDAR LA PROPUESTA DE PROTOCOLOS DE SEGURIDAD INFORMÁTICA CON EL MODELO SISTEMA GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN (SGSI)

El modelo de Sistema de Gestión de Seguridad de la Información (SGSI) para la Alcaldía de Fusagasugá, se encuentra basado en el Modelo de Seguridad y Privacidad de la Información de MinTIC, alineado a la metodología del ciclo PHVA que también se aplican en el manual de Gobierno en línea 3.0.

9.2 VERIFICAR QUE LOS PROTOCOLOS DE SEGURIDAD INFORMÁTICA ESTÉN ALINEADOS CON LOS RIESGOS INFORMÁTICOS, GOBIERNO DE TI Y SISTEMA GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN (SGSI)

Los protocolos de seguridad propuestos para la Alcaldía de Fusagasugá, cumplen con el resultado del análisis de información realizado, estableciendo controles de seguridad adecuados que garanticen la responsabilidad y la orientación para preservar los pilares fundamentales de la seguridad de la información confidencialidad, integridad y disponibilidad de la información.

9.3 AJUSTES REQUERIDOS EN LOS PROTOCOLOS DE SEGURIDAD Y EN EL MODELO DE SISTEMA GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN (SGSI)

Los protocolos de seguridad propuestos para la Alcaldía de Fusagasugá, fueron ajustados de tal manera que contribuyan como una acción de control para la valoración de los riesgos informáticos que ha identificado la organización.

9.4 INFORME FINAL DEL PROYECTO, PRODUCTOS ENTREGABLES

Los productos entregar: los protocolos de seguridad informática y el Modelo de Sistema de Gestión de Seguridad de la información (SGSI) para la Alcaldía Municipal de Fusagasugá.

10. FASE ACTUAR CICLO PHVA

10.1 ENTREGAR A LA OFICINA TIC PROTOCOLOS DE SEGURIDAD Y MODELO DE SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN (SGSI) QUE CONTRIBUYEN A LA MEJORA CONTINUA DEL PROCESO DE GESTIÓN TIC Y LA ADMINISTRACIÓN DE SUS RIESGOS.

Los productos a entregar del presente trabajo de grado, serán entregados a la Oficina de Tecnologías de la Información y las Comunicaciones de la Alcaldía de Fusagasugá, entre ellos están los protocoles de seguridad y el Modelo de Sistema de Gestión de Seguridad de la Información, conforme al Modelo de Seguridad y Privacidad de la Información por parte del Ministerio de Tecnologías de la Información las Comunicaciones.

11. RECOMENDACIONES

- En base con los hallazgos de la información recolectada a lo largo del Proyecto, se recomienda que el área de Control Interno realice una verificación de los Riesgos Informáticos a los que actualmente se tienen al interior de la Alcaldía Municipal de Fusagasugá los cuales se deben clasificar posteriormente.
- Aunque la entidad cuenta con normativa vigente en cuanto a la Seguridad de la Información se recomienda la implementación de Protocolos para las políticas de Seguridad que se deben dictar desde cada uno de los ámbitos que se requieran, con el fin de proveer directrices estrictas en cuanto al manejo de la Información que se encuentra al interior de la Alcaldía Municipal de Fusagasugá.
- La implementación de lineamientos robustos en cuanto al manejo de la información para los funcionarios internos y externos de la Alcaldía Municipal de Fusagasugá, elevara el nivel de protección para posibles ataques a los que actualmente se encuentra expuesta.
- Incluir dentro de los planes de capacitación los temas de los temas de Seguridad, privacidad y confidencialidad de la información, e ingeniería social. La capacitación debe tener como alcance desde el inicio de su vinculación y durante la permanencia de los servidores públicos; de esta manera se garantiza una mayor concienciación del tema y su aplicación para el desarrollo de sus funciones y actividades laborales.
- El manejo de campañas de sensibilización y estrategias de comunicación interna sobre Seguridad, tratamiento y niveles de confidencialidad de la Información para los servidores públicos de la Alcaldía, ayudara a mitigar y prevenir posibles fugas o robo de información a los que actualmente se encuentra expuesta la entidad.
- La implementación del Sistema General de Seguridad de la Información en la Alcaldía Municipal de Fusagasugá ayudara a la Institución a linearse a la normativa emitida por el Ministerio de las TIC para Gobierno en Línea 3.0.
- Diseñar dentro del Sistema de Gestión de Seguridad de la Información el Plan de continuidad del negocio, señalada por Modelo de Seguridad y Privacidad de la información MPSI como Guía para la preparación de las TIC para la continuidad del negocio de MinTIC.
- Establecer una Declaración de Aplicabilidad (*SoA)*, con el propósito de estimar las acciones necesarias que de acuerdo al riesgo identificado y analizado que permitan mitigar, transferir, compartir y aceptar el riesgo; en este documento se deben registrar los controles de seguridad que son aplicables (necesarios), los cuales deben ser verificados para comprobar si se encuentran operando o no.

BIBLIOGRAFIA

Agedum Sistema de Información. (2015). *Diseño e implementación de un S.G.S.I. ISO 27001*. Obtenido de http://www.agedum.com/Dise%C3%B1oeimplementaci%C3%B3ndeunSGSIISO27001/tabid/91/Default.aspx

Alcaldía de Fusagasugá. (Septiembre de 2015). *Fusagasugá Digital - Oficina TIC*. Obtenido de www.fusagasugadigital.gov.co

Alberto G., A. (2014). *Implantación de la ISO 27001:2005 Sistema de Gestión de Seguridad de la Información*. Obtenido de http://www.iso27000.es/download/Implantacion_del_ISO_27001_2005.pdf

Alcaldía de Fusagasugá. (2014). *Caracterización proceso de apoyo Gestion TIC (CA-GT-001).* Fusagasugá: Sistema Integrado Meci-Calidad de la Alcaldía de Fusagasugá (SIMCAF).

Alcaldía de Fusagasugá. (Septiembre de 2014). *Gestión TIC . proceso de apoyo - Sistema Integrado Meci-Calidad de la Alcaldía de Fusagasugá.* Recuperado el Mayo de 2015, de Drive, oficina TIC

Alcaldía de Fusagasugá. (6 de Junio de 2014). *Manual de Calidad.* Obtenido de http://www.fusagasuga-cundinamarca.gov.co/publicaciones.php?id=42617

Alcaldía de Fusagasugá. (Septiembre de 2015). *Portal Web Municipio de Fusagasugá*. Obtenido de www.fusagasuga-cundinamarca.gov.co

Alpala P., L. O. (11 de Septiembre de 2014). *Propuesta de actualización, apropiación y aplicación de políticas de seguridad informática en una empresa corporativa, PROPOLSINECOR*. Obtenido de Universidad Nacional Abierta y a Distancia UNAD: http://repository.unad.edu.co/bitstream/10596/2742/1/12973210.pdf

Departamento Administrativo de la Función Pública (DAFP). (s.f.). *Guía para la Administración del Riesgo*. Obtenido de Portal web dafp.gov.co: http://portal.dafp.gov.co/portal/pls/portal/formularios.retrive_publicaciones?no=1592

Estrada B., J. C., Pineda B., D. H., & Varon M., C. E. (2012). *Diseño de una metodologia para la implementación del sistema de gestión de seguridad de la información - SGSI, en el sector de laboratorios de analisis microbiologicos,*

basado en ISO 27001. Obtenido de UNIVERSIDAD EAN: http://repository.ean.edu.co/bitstream/handle/10882/2692/MurilloCarol2012.pdf?sequence=1

Garaviño, E. E. (18 de Septiembre de 2015). *Manual para aplicar normas ICONTEC 1486 y Tesis Universidad Autónoma de Occidente-Cali*. Obtenido de Biblioteca Universidad Autonoma de Occidente: http://uao.libguides.com/content.php?pid=440277&sid=3604641

Instituto Colombiano de Normas Tecnicas y Certificación (ICONTEC). (2005). *Requisitos. NTC-ISO 9001.* Bogotá D.C.

Instituto Colombiano de Normas Tecnicas y Certificación (ICONTEC). (2008). *Norma Técnica de Calidad en la Gestión Publica. NTC GP 1000:2009.* Bogotá D.C.

Ministerio de Tecnologías de la Información y las Comunicaciones (MinTic). (s.f.). *Estrategía de Gobierno en Línea para el orden territorial 2012-2017*. Obtenido de Manual para la implementación de la Estrategia de Gobierno en línea en las entidades del orden nacional de la República de Colobmia: http://programa.gobiernoenlinea.gov.co/apc-aa-files/eb0df10529195223c011ca6762bfe39e/manual-3.1.pdf

Ministerio de Tecnologías de la Información y las Comunicaciones. (17 de Junio de 2014). *Arquitectura TI Colombia*. Obtenido de Marco de Referencia, Modelos y servicios compartidos, Interoperbilidad, Experiencial Internacional: http://www.mintic.gov.co/gestionti/615/w3-propertyvalue-6203.html

Ministerio de Tecnologías de la Información y las Comunicaciones. (2015). *Gobierno TI Normatividad*. Obtenido de http://www.mintic.gov.co/marcodereferencia/624/articles-7643_normatividad.pdf

Ministerio de Tecnologías de la Información y las Comunicaciones. (Noviembre de 2015). *Guía de controles de seguridad y privacidad de la información*. Obtenido de http://www.mintic.gov.co/gestionti/615/articles-5482_Controles.pdf

Ministerio de Tecnologías de la Información y las Comunicaciones. (Noviembre de 2015). *Guía de gestión de incidentes de seguridad de la información*. Obtenido de http://www.mintic.gov.co/gestionti/615/articles-5482_Gestion_Incidentes.pdf

Ministerio de Tecnologías de la Información y las Comunicaciones. (Noviembre de 2015). *Guía de indicadores de la gestión para la seguridad de la información*. Obtenido de http://www.mintic.gov.co/gestionti/615/articles-5482_Indicadores.pdf

Ministerio de Tecnologías de la Información y las Comunicaciones. (Noviembre de 2015). *Guía de Transición de IPV4 a IPV6 para Colombia*. Obtenido de http://www.mintic.gov.co/gestionti/615/articles-5482_transicion_IPV4.pdf

Ministerio de Tecnologías de la Información y las Comunicaciones. (Noviembre de 2015). *Guía encuesta de Diagnóstico Modelo de Seguridad de la Información para las Entidades del Estado.* Obtenido de http://www.mintic.gov.co/gestionti/615/articles-5482_diagnostico.pdf

Ministerio de Tecnologías de la información y las Comunicaciones. (Noviembre de 2015). *Guía para el Aseguramiento del protocolo IPV6*. Obtenido de http://www.mintic.gov.co/gestionti/615/articles-5482_Protocolo_IPV6.pdf

Ministerio de Tecnologías de la Información y las Comunicaciones. (Noviembre de 2015). *Guía para la gestión de riesgos*. Obtenido de http://www.mintic.gov.co/gestionti/615/articles-5482_Protocolo_IPV6.pdf

Ministerio de Tecnologías de la Información y las Comunicaciones. (04 de Noviembre de 2015). *Modelo de Seguridad y Privacidad de la Información*. Obtenido de http://www.mintic.gov.co/gestionti/615/articles-5482_Modelo_Seguridad.pdf

Ministerio de Tencologías de la Información y las Comunicaciones. (Noviembre de 2015). *Formato e implementación de políticas de seguridad y privacidad de la información*. Obtenido de http://www.mintic.gov.co/gestionti/615/articles-5482_Implementacion_politicas.pdf

Ocampo G., D. (2015). *Modelo de Seguridad de la Información para las Entidad Publicas del Estado Colombiano*. Obtenido de Universidad Piloto de Colombia: http://polux.unipiloto.edu.co:8080/00002024.pdf

Presidencia de la República. (Diciembre de 2014). *Manual de la política de seguridad para las Tecnologías de la Información y las Comunicaciones - TICS*. Obtenido de http://wp.presidencia.gov.co/sitios/dapre/sigepre/manuales/M-TI-01%20Manual%20general%20Sistema%20de%20Seguridad%20de%20la%20Informacion.pdf

Romero U., K. A. (2015). *Gestion de la seguridad y el riesgo de TI*. Obtenido de Universidad Piloto de Colombia: http://polux.unipiloto.edu.co:8080/00002222.pdf

Salcedo B., R. J. (19 de Diciembre de 2014). *Plan de implementación del SGSI basado en la norma ISO 27001:2013*. Obtenido de http://openaccess.uoc.edu/webapps/o2/bitstream/10609/41002/4/rsalcedobTFC1214memoria.pdf

ANEXOS

Anexo A. Resumen Analítico Educativo (RAE)

Título de la Investigación
MODELO PARA LA IMPLEMENTACIÓN DEL SISTEMA GENERAL DE SEGURIDAD INFORMATICA Y PROTOCOLOS DE SEGURIDAD INFORMÁTICA EN LA OFICINA TIC DE LA ALCALDÍA MUNICIPAL DE FUSAGASUGÁ, BASADOS EN LA GESTIÓN DEL RIESGO INFORMÁTICO
Autor
Ana Milena Pulido Barreto – Jenith Marsella Mantilla Rodríguez
Publicación Lugar y Año de Publicación, Edición
Lugar: Fusagasugá, Colombia Año: 2016
Unidad Patrocinante
Universidad Nacional Abierta y a Distancia - UNAD
Descripción de la investigación:
Monografía de Grado
Palabras Clave o descriptores
SGSI, MSPI, MOSPI, Protocolos, Gobierno en Línea, Metodología PHVA.
Problema que aborda la investigación:
Falta de un modelo para la implementación de un Sistema de Gestión de Seguridad de la Información y protocolos de seguridad informática en la Alcaldía Municipal de Fusagasugá, con el que se pueda gestionar y controlar los Riesgos Informáticos identificados y a los que se encuentra expuesta la entidad.
Objetivos de la Investigación:
Objetivo General Entregar un Modelo para la implementación del Sistema de Gestión de Seguridad de la información y Protocolos de Seguridad Informática para la Oficina TIC de La Alcaldía Municipal de Fusagasugá, basados en la identificación previa de los riesgos informáticos por parte de la entidad. Objetivos específicos: • Analizar los diferentes riesgos informáticos que actualmente se tienen identificados en la Oficina TIC de la Alcaldía de Fusagasugá. • Establecer un modelo de Sistema Gestión de Seguridad de la información, con base en los riesgos informáticos identificados. • Desarrollar un documento con los pasos para la implementación del modelo de Sistema de Gestión de Seguridad de la información, de acuerdo a los riesgos encontrados en la Oficina TIC de la Alcaldía de Fusagasugá

Duración investigación:

Desarrollo el proyecto de monografía en mención, tomo aproximadamente seis (6) meses.

Hipótesis Planteada por la investigación:

Contenidos:

En la actualidad la normativa emitida por MinTIC en cuanto a Gobierno en Línea, exige que todas las entidades del sector público estén obligadas a implementar el Sistema de Gestión de Seguridad de la Información (SGSI) al interior de ellas. Para esto se plantea la ejecución a través de la metodología de ciclo PHVA (Planear, Hacer, Verificar y Actuar), metodología que también es usada por el Sistema Integrado Meci y Calidad de la Alcaldía de Fusagasugá (SIMCAF).

Inicialmente se realiza el análisis de los Riesgos Informáticos que se encuentran identificados al interior de la Alcaldía Municipal de Fusagasugá, los cuales fueron aprobados y se encuentran vigentes para el proceso de apoyo GESTION TIC que lidera la Oficina TIC, este proceso hace parte del Sistema Integrado Meci y Calidad de la Alcaldía de Fusagasugá (SIMCAF). Adicional a ello, se utilizar herramientas de medición como entrevistas y encuestas al personal de diferentes áreas de la Alcaldía, con resultados que permitieron concluir que es necesario implementar protocolos de seguridad informática y un modelo de Sistema de Gestión de Seguridad de la Información (SGSI), que le permitan fortalecer los procesos, actividades laborales y servicios que realiza la Oficina TIC de la Alcaldía de Fusagasugá, y dentro de la gestión del riesgo emprender acciones de control y valoración, con el fin contribuir a que el riesgo se pueda evitar, reducir, transferir, compartir o asumir, conforme al política de administración del riesgo de la entidad.

El desarrollo de la metodología del proyecto PHVA, se da así:

PLANEAR

- Análisis de Información.
- Capacidades y recursos para el Proyecto.
- Entrevistas con el personal de la Oficina TIC de la Alcaldía de Fusagasugá.
- Encuestas (4) a los funcionarios sobre SGSI, política y protocolos de seguridad (48 de 265 funcionarios, 18%)
- Análisis de resultados de las encuestas aplicadas

HACER

- Análisis del Sistema Integrado de Gestión MECI-Calidad de la Alcaldía de Fusagasugá.
- Análisis del Proceso de Gestión TIC y el Sistema Gestión de Seguridad

de la Información (SGSI).
- Análisis de la Administración del Riesgo Informático que han sido identificados por el proceso Gestión TIC de la Alcaldía de Fusagasugá.
- Selección de protocolos de seguridad requeridos por la Oficina TIC, de acuerdo a los riesgos informáticos.
- Modelo de Sistema Gestión de Seguridad de la Información (SGSI), en cumplimiento de la normatividad vigente para entidades públicas.

VERIFICAR
- Validación de los protocolos de seguridad informática con el modelo Sistema Gestión de Seguridad de la Información (SGSI).
- Verificación de los protocolos de seguridad Informática estén alineados con los riesgos informáticos y el Sistema Gestión de Seguridad de la Información (SGSI).
- Ajustes requeridos en los protocolos de seguridad y en el modelo de Sistema Gestión de Seguridad de la Información (SGSI).
- Verificación del documento del proyecto con los productos entregables, de acuerdo a los objetivos planteados.

ACTUAR
- Mejora continua para Sistema de Integrado de Gestión Mecí-Calidad de la Alcaldía de Fusagasugá (SIMCAF).
- Resultados del proyecto (productos entregables) y el cumplimiento de la normatividad vigente en modelos de seguridad de la información.
- Protocolos de seguridad (29) y un Modelo que les permitirá analizar y viabilizar la implementación el Sistema de Gestión de Seguridad de la Información (SGSI), como parte de la gestión de los riesgos informáticos identificados por la entidad.

Tipo de Investigación
El proyecto es una monografía, un documento escrito y relativamente extenso, donde se presentan organizadamente los temas objeto de estudio abordados en el desarrollo del proyecto de acuerdo a la metodología PHVA; también se presentan herramientas de medición y el análisis del resultado obtenido al aplicar encuestas y entrevistas.
Población y muestra
Ciudad: Alcaldía Municipal de Fusagasugá País: Colombia Población: Funcionarios de la Alcaldía
Técnicas de Investigación
Obtención, revisión y análisis de Documentos, Entrevistas y Encuestas.
Instrumentos de investigación
Consultas en la web, libros, artículos, metadatos, entrevistas, encuestas, análisis documental.

Metodología y estrategias seguidas por la investigación:

Método Ciclo PHVA: se basa en un ciclo de 4 pasos: Planificar, Hacer, Verificar y Actuar. Es comúnmente utilizada en la implementación de sistemas de gestión de la calidad buscando una mayor probabilidad de éxito.

Argumentos expuestos por el autor:

- La entidad debe proveer directrices o actos administrativos que permitan reglamentar el manejo de la Información que se encuentra al interior de la Alcaldía Municipal de Fusagasugá.
- La Alcaldía debe realizar campañas de sensibilización y estrategias de comunicación interna sobre Seguridad, tratamiento y niveles de confidencialidad de la Información para los servidores públicos de la Alcaldía, ayudara a mitigar y prevenir posibles fugas o robo de información a los que actualmente se encuentra expuesta la entidad.
- Diseñar dentro del Sistema de Gestión de Seguridad de la Información el Plan de continuidad del negocio, señalada por Modelo de Seguridad y Privacidad de la información MPSI como Guía para la preparación de las TIC para la continuidad del negocio de MinTIC.
- Establecer una Declaración de Aplicabilidad (SoA), con el propósito de estimar las acciones necesarias que de acuerdo al riesgo identificado y analizado que permitan mitigar, transferir, compartir y aceptar el riesgo; en este documento se deben registrar los controles de seguridad que son aplicables (necesarios), los cuales deben ser verificados para comprobar si se encuentran operando o no.

Conclusiones de la investigación:

- La implementación del Sistema de Gestión de Seguridad de la Información en la Alcaldía Municipal de Fusagasugá, ayudará a la entidad a cumplir la normativa emitida por el Ministerio de las TIC para Gobierno en Línea 3.0 y demás normatividad vigente, haciendo uso del modelo de seguridad y privacidad de la información establecido para las entidades públicas por parte del gobierno nacional.
- Los protocolos de seguridad informática contribuyen a la gestión del riesgo informático de la entidad, ya que representan acciones de control y valoración, en el que el riesgo se pueda evitar, reducir, transferir, compartir o asumir, conforme al política de administración del riesgo de la entidad.
- El resultado de las encuestas deduce que la Alcaldía de Fusagasugá debe incluir dentro de los planes de capacitación los temas de los temas de Seguridad, privacidad y confidencialidad de la información, e ingeniería social.
- Incluir dentro de los planes de capacitación los temas de los temas de Seguridad, privacidad y confidencialidad de la información, e ingeniería social, y emplear estrategias transversales de comunicación para la difusión y apropiación de la seguridad y privacidad de la información en la

entidad.

Bibliografía:

Agedum Sistema de Información. (2015). Diseño e implementación de un S.G.S.I. ISO 27001. Obtenido de http://www.agedum.com/Dise%C3%B1oeimplementaci%C3%B3ndeunSGSIISO27001/tabid/91/Default.aspx

Alcaldía de Fusagasugá. (Septiembre de 2015). Fusagasugá Digital - Oficina TIC. Obtenido de www.fusagasugadigital.gov.co

Alberto G., A. (2014). Implantación de la ISO 27001:2005 Sistema de Gestión de Seguridad de la Información. Obtenido de http://www.iso27000.es/download/Implantacion_del_ISO_27001_2005.pdf

Alcaldía de Fusagasugá. (2014). Caracterización proceso de apoyo Gestion TIC (CA-GT-001). Fusagasugá: Sistema Integrado Meci-Calidad de la Alcaldía de Fusagasugá (SIMCAF).

Alcaldía de Fusagasugá. (Septiembre de 2014). Gestión TIC . proceso de apoyo - Sistema Integrado Meci-Calidad de la Alcaldía de Fusagasugá. Recuperado el Mayo de 2015, de Drive, oficina TIC

Alcaldía de Fusagasugá. (6 de Junio de 2014). Manual de Calidad. Obtenido de http://www.fusagasuga-cundinamarca.gov.co/publicaciones.php?id=42617

Alcaldía de Fusagasugá. (Septiembre de 2015). Portal Web Municipio de Fusagasugá. Obtenido de www.fusagasuga-cundinamarca.gov.co

Alpala P., L. O. (11 de Septiembre de 2014). Propuesta de actualización, apropiación y aplicación de políticas de seguridad informática en una empresa corporativa, PROPOLSINECOR. Obtenido de Universidad Nacional Abierta y a Distancia UNAD: http://repository.unad.edu.co/bitstream/10596/2742/1/12973210.pdf

Departamento Administrativo de la Función Pública (DAFP). (s.f.). Guía para la Administración del Riesgo. Obtenido de Portal web dafp.gov.co: http://portal.dafp.gov.co/portal/pls/portal/formularios.retrive_publicaciones?no=1592

Estrada B., J. C., Pineda B., D. H., & Varon M., C. E. (2012). Diseño de una metodologia para la implementación del sistema de gestión de seguridad de la información - SGSI, en el sector de laboratorios de analisis microbiologicos, basado en ISO 27001. Obtenido de UNIVERSIDAD EAN: http://repository.ean.edu.co/bitstream/handle/10882/2692/MurilloCarol2012.pdf?sequence=1

Garaviño, E. E. (18 de Septiembre de 2015). Manual para aplicar normas ICONTEC 1486 y Tesis Universidad Autónoma de Occidente-Cali. Obtenido de Biblioteca Universidad Autonoma de Occidente: http://uao.libguides.com/content.php?pid=440277&sid=3604641

Instituto Colombiano de Normas Tecnicas y Certificación (ICONTEC). (2005). Requisitos. NTC-ISO 9001. Bogotá D.C.

Instituto Colombiano de Normas Tecnicas y Certificación (ICONTEC). (2008). Norma Técnica de Calidad en la Gestión Publica. NTC GP 1000:2009. Bogotá D.C.

Ministerio de Tecnologías de la Información y las Comunicaciones (MinTic). (s.f.). Estrategía de Gobierno en Línea para el orden territorial 2012-2017. Obtenido de Manual para la implementación de la Estrategia de Gobierno en línea en las entidades del orden nacional de la República de Colobmia: http://programa.gobiernoenlinea.gov.co/apc-aa-files/eb0df10529195223c011ca6762bfe39e/manual-3.1.pdf

Ministerio de Tecnologías de la Información y las Comunicaciones. (17 de Junio de 2014). Arquitectura TI Colombia. Obtenido de Marco de Referencia, Modelos y servicios compartidos, Interoperbilidad, Experiencial Internacional: http://www.mintic.gov.co/gestionti/615/w3-propertyvalue-6203.html

Ministerio de Tecnologías de la Información y las Comunicaciones. (2015). Gobierno TI Normatividad. Obtenido de http://www.mintic.gov.co/marcodereferencia/624/articles-7643_normatividad.pdf

Ministerio de Tecnologías de la Información y las Comunicaciones. (Noviembre de 2015). Guía de controles de seguridad y privacidad de la información. Obtenido de http://www.mintic.gov.co/gestionti/615/articles-5482_Controles.pdf

Ministerio de Tecnologías de la Información y las Comunicaciones. (Noviembre de 2015). Guía de gestión de incidentes de seguridad de la información. Obtenido de http://www.mintic.gov.co/gestionti/615/articles-5482_Gestion_Incidentes.pdf

Ministerio de Tecnologías de la Información y las Comunicaciones. (Noviembre de 2015). Guía de indicadores de la gestión para la seguridad de la información. Obtenido de http://www.mintic.gov.co/gestionti/615/articles-5482_Indicadores.pdf

Ministerio de Tecnologías de la Información y las Comunicaciones. (Noviembre de 2015). Guía de Transición de IPV4 a IPV6 para Colombia. Obtenido de http://www.mintic.gov.co/gestionti/615/articles-5482_transicion_IPV4.pdf

Ministerio de Tecnologías de la Información y las Comunicaciones. (Noviembre de 2015). Guía encuesta de

Diagnóstico Modelo de Seguridad de la Información para las Entidades del Estado. Obtenido de http://www.mintic.gov.co/gestionti/615/articles-5482_diagnostico.pdf

Ministerio de Tecnologías de la información y las Comunicaciones. (Noviembre de 2015). Guía para el Aseguramiento del protocolo IPV6. Obtenido de http://www.mintic.gov.co/gestionti/615/articles-5482_Protocolo_IPV6.pdf

Ministerio de Tecnologías de la Información y las Comunicaciones. (Noviembre de 2015). Guía para la gestión de riesgos. Obtenido de http://www.mintic.gov.co/gestionti/615/articles-5482_Protocolo_IPV6.pdf

Ministerio de Tecnologías de la Información y las Comunicaciones. (04 de Noviembre de 2015). Modelo de Seguridad y Privacidad de la Información. Obtenido de http://www.mintic.gov.co/gestionti/615/articles-5482_Modelo_Seguridad.pdf

Ministerio de Tencologías de la Información y las Comunicaciones. (Noviembre de 2015). Formato e implementación de políticas de seguridad y privacidad de la información. Obtenido de http://www.mintic.gov.co/gestionti/615/articles-5482_Implementacion_politicas.pdf

Ocampo G., D. (2015). Modelo de Seguridad de la Información para las Entidad Publicas del Estado Colombiano. Obtenido de Universidad Piloto de Colombia: http://polux.unipiloto.edu.co:8080/00002024.pdf

Presidencia de la República. (Diciembre de 2014). Manual de la política de seguridad para las Tecnologías de la Información y las Comunicaciones - TICS. Obtenido de http://wp.presidencia.gov.co/sitios/dapre/sigepre/manuales/M-TI-01%20Manual%20general%20Sistema%20de%20Seguridad%20de%20la%20Informacion.pdf

Romero U., K. A. (2015). Gestion de la seguridad y el riesgo de TI. Obtenido de Universidad Piloto de Colombia: http://polux.unipiloto.edu.co:8080/00002222.pdf

Salcedo B., R. J. (19 de Diciembre de 2014). Plan de implementación del SGSI basado en la norma ISO 27001:2013. Obtenido de http://openaccess.uoc.edu/webapps/o2/bitstream/10609/41002/4/rsalcedobTFC1214memoria.pdf

Preparado por:

ANA MILENA PULIDO BARRETO - JENITH MARSELLA MANTILLA RODRIGUEZ

Teléfono - Email

Teléfono: 3132842400 - 314 3368720
E-mail: **anamilepb@gmail.com** - **marsemanti@gmail.com**

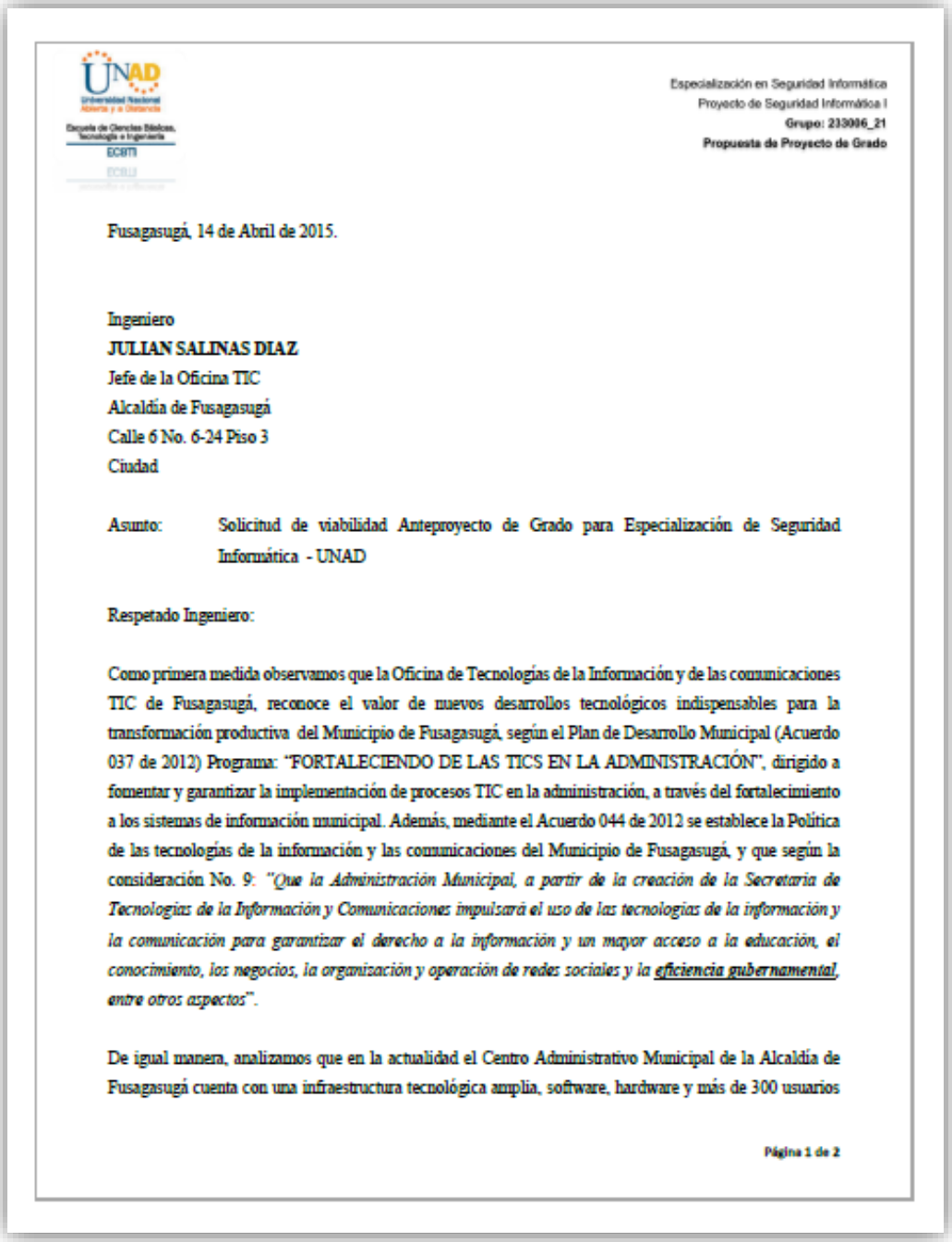
Analista del RAE:

ANA MILENA PULIDO BARRETO - JENITH MARSELLA MANTILLA RODRIGUEZ

Fecha de diligenciamiento

Fusagasugá, Abril 14 de 2016

Anexo B. Solicitud de autorización del proyecto a la Alcaldía de Fusagasugá



Fusagasugá, 14 de Abril de 2015.

Ingeniero
JULIAN SALINAS DIAZ
Jefe de la Oficina TIC
Alcaldía de Fusagasugá
Calle 6 No. 6-24 Piso 3
Ciudad

Asunto: Solicitud de viabilidad Anteproyecto de Grado para Especialización de Seguridad Informática - UNAD

Respetado Ingeniero:

Como primera medida observamos que la Oficina de Tecnologías de la Información y de las comunicaciones TIC de Fusagasugá, reconoce el valor de nuevos desarrollos tecnológicos indispensables para la transformación productiva del Municipio de Fusagasugá, según el Plan de Desarrollo Municipal (Acuerdo 037 de 2012) Programa: "FORTALECIENDO DE LAS TICS EN LA ADMINISTRACIÓN", dirigido a fomentar y garantizar la implementación de procesos TIC en la administración, a través del fortalecimiento a los sistemas de información municipal. Además, mediante el Acuerdo 044 de 2012 se establece la Política de las tecnologías de la información y las comunicaciones del Municipio de Fusagasugá, y que según la consideración No. 9: *"Que la Administración Municipal, a partir de la creación de la Secretaria de Tecnologías de la Información y Comunicaciones impulsará el uso de las tecnologías de la información y la comunicación para garantizar el derecho a la información y un mayor acceso a la educación, el conocimiento, los negocios, la organización y operación de redes sociales y la eficiencia gubernamental, entre otros aspectos"*.

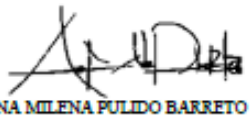
De igual manera, analizamos que en la actualidad el Centro Administrativo Municipal de la Alcaldía de Fusagasugá cuenta con una infraestructura tecnológica amplia, software, hardware y más de 300 usuarios

aproximadamente que utilizan equipos e instalaciones tecnológicas y el servicio de Internet, por consiguiente, se considera importante que la entidad establezca acciones que garanticen la seguridad física y lógica de sus activos informáticos, y que le permita mitigar los riesgos informáticos e impactos que puedan afectar la organización desde varios punto de vista y en especial la seguridad de la información.

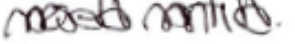
Dado lo anterior, se considera importante y prioritario contribuir al fortalecimiento de los procesos, actividades y servicios que realiza la Oficina TIC de la Alcaldía de Fusagasugá, por ello como estudiantes de la Especialización en Seguridad informática de la Universidad Nacional Abierta y A Distancia – UNAD, queremos dar a conocer el anteproyecto de grado denominado: **PROPUESTA PARA LA IMPLEMENTACIÓN DE PROTOCOLOS DE SEGURIDAD INFORMÁTICA EN LA ALCALDÍA MUNICIPAL DE FUSAGASUGÁ, BASADOS EN LA GESTIÓN DEL RIESGO INFORMÁTICO**, el cual se ha diseñado con el fin de ser aplicado en la Alcaldía de Fusagasugá; por consiguiente, amablemente solicitamos su colaboración para estudiar la viabilidad y/o autorizar el desarrollo de esta propuesta; la información básica del anteproyecto se relaciona en el documento adjunto (*Ver anexo No. 1 Anteproyecto en cinco 5 folios*).

Es importante aclarar, que si el anteproyecto es autorizado por parte de la Alcaldía de Fusagasugá, será enviado a la Tutora LORENA SUAREZ, docente de Proyecto de Seguridad Informática I de la UNAD, para que posteriormente se solicite la aprobación al Comité Curricular de la UNAD con algunos requisitos adicionales.
Agradecemos su atención y esperamos contar con su apoyo y respuesta oportuna.

Atentamente,



ANA MILENA PULIDO BARRETO
Estudiante Esp. Seguridad Informatica UNAD
Grupo: 233006_21
anamilepb@gmail.com



JENITH MARSELLA MANTILLA RODRIGUEZ
Estudiante Esp. Seguridad Informatica UNAD
Grupo: 233006_21
marsemant@gmail.com

Anexo C. Oficio de respuesta Alcaldía de Fusagasugá con autorización del Anteproyecto

ALCALDÍA DE FUSAGASUGÁ
Oficina de Tecnologías de la Información y las Comunicaciones TIC´s

Fusagasugá, 16 de Abril de 2015
1040-06.113

Ingenieras
ANA MILENA PULIDO
JENITH MARSELLA MANTILLA
Estudiantes de Especialización en Seguridad Informática
Universidad Nacional Abierta y A Distancia - UNAD
Ciudad

Asunto: Respuesta a oficio de autorización anteproyecto de grado

Respetadas Ingenieras:

La Oficina de Tecnologías de Información y Comunicación (TIC) del municipio de Fusagasugá, agradece a ustedes el reconocimiento a la gestión realizada en el plan de gobierno *"Fusagasugá | Contigo con Todo"*, y por la creación de la única Oficina (TIC) territorial del departamento de Cundinamarca con Política Publica propia en TIC (Acuerdo 044 de 2012) ***"Fusagasugá Digital, Eje de la región Inteligente"***.

Despues de haber analizado la información básica del anteproyecto de grado denominado "PROPUESTA PARA LA IMPLEMENTACIÓN DE PROTOCOLOS DE SEGURIDAD INFORMÁTICA EN LA ALCALDÍA MUNICIPAL DE FUSAGASUGÁ, BASADOS EN LA GESTIÓN DEL RIESGO INFORMÁTICO", considero que es viable que la Alcaldía cuente con protocolos que permitan garantizar la seguridad de los activos informáticos, y en especial la seguridad de la información; por consiguiente, autorizo la aplicación del proyecto en nuestra entidad bajo la coordinación y lineamientos de la Oficina, espero que tambien la universidad les conceda viabilidad del proyecto.

Agradezco la atención.

Cordialmente,

JULIAN SALINAS DIAZ
Jefe Oficina TIC

GESTIÓN DOCUMENTAL:
Original: Destinatarios
1ª Copia: Oficina de Tecnologías de la Información y las Comunicaciones – TIC
Serie: 1040-06
Nombre del Archivo Sistematizado: OficinaTIC/Oficios 2015
Elaboro: Jhonny Fabricio Tocua Jiménez, Profesional Universitario – Líder de Proyectos TIC
Reviso: Ing. Julián Salinas Diaz/ Jefe Oficina TIC

Fusagasugá | CONTIGO, CON TODO.

Calle 6 No. 6-24 - Centro Administrativo Municipal
www.fusagasuga-cundinamarca.gov.co
jefetic@fusagasuga-cundinamarca.gov.co
Teléfonos: 886 8181 – EXTENSIÓN 111 y 105 PISO 2
Codigo Postal: 252211

Anexo D. Ficha de Seguimiento Cronograma

	CRONOGRAMA	SEP				OCT				NOV				SEGUIMIENTO		
	ACTIVIDADES FASES METODOLOGIA PROYECTO DEMING CICLO PHVA	1	2	3	4	1	2	3	4	1	2	3	4	EVIDENCIA	OBSERVACIONES	Porcentaje de Cumplimiento
No.	**PLANEACIÓN**															
1	Análisis de Información													Investigación de normatividad y proyectos de grado para definir el marco de referencia: estado del Arte, marco conceptual y normativo		100%
2	Capacidades y recursos para el Proyecto													Se definen los recursos comprometidos en el proyecto		100%
3	Entrevista con el personal de la Oficina TIC de la Alcaldía de Fusagasugá.													Entrevista en sitio con el Jefe de la Oficina TIC		100%
4	Encuestas a los funcionarios sobre Sistema de Gestión de Seguridad de la Información SGSI), política, protocolos de seguridad informática en la Alcaldía de Fusagasugá.													Encuestas aplicadas a: 30 funcionarios a nivel general de la Alcaldía de Fusagasugá, 5 funcionarios de la Dirección de Gestión Humana, 3 funcionarios de la Oficina de Control Interno, 10 servidores públicos de la Oficina TIC.		100%
5	Análisis de resultados de las encuestas aplicadas.													Datos importantes del resultado de las encuestas		100%
	HACER															
6	Análisis del Sistema Integrado de Gestión MECI-Calidad de la Alcaldía de Fusagasugá.													Información proporcionada por la Alcaldía de Fusagasugá, que también se encuentra publicada en la intranet institucional de la Alcaldía de Fusagasugá el Sistema Integrado de Gestión MECI-Calidad (SIMCAF).		100%
7	Análisis del Proceso de Gestión TIC y Sistema Gestión de Seguridad de la Información (SGSI).													Información proporcionada por la Alcaldía de Fusagasugá, que también se encuentra publicada en la intranet institucional de la Alcaldía de Fusagasugá en proceso de Gestión TIC, análisis de las Fases que aplican al modelo a proponer para el SGSI.		100%
8	Análisis de la Administración del Riesgo Informático que han sido identificados por el proceso Gestión TIC													Se tienen los formatos de la administración del riesgo para el proceso de apoyo GESTION TIC.		100%

9	Selección de protocolos de seguridad requeridos por la Oficina TIC, de acuerdo a los riesgos informáticos.													Documentado en el numeral 4.3.4 del proyecto	100%
10	Modelo de Sistema Gestión de Seguridad de la Información (SGSI), en cumplimiento de la normatividad vigente para entidades públicas.													Documentado en el numeral 4.3.5 del proyecto	100%
11	Recomendaciones y conclusiones													Documentado en el numeral 4.3.6 del proyecto	100%
	VERIFICAR														
12	Validar la propuesta de protocolos de seguridad informática con el modelo Sistema Gestión de Seguridad de la Información (SGSI).													Documentado en el numeral 4.4.1 del proyecto	100%
13	Verificar que los Protocolos de seguridad Informática estén alineados con los Riesgos Informáticos, Gobierno de TI y Sistema Gestión de Seguridad de la Información (SGSI).													Documentado en el numeral 4.4.2 del proyecto	100%
14	Ajustes requeridos en los protocolos de seguridad y en el modelo de Sistema Gestión de Seguridad de la Información (SGSI).													Documentado en el numeral 4.4.3 del proyecto	100%
15	Informe Final del proyecto, productos entregables													Documentado en el numeral 4.4.4 del proyecto	100%
	ACTUAR														
16	Entregar a la Oficina TIC protocolos de seguridad y modelo de Sistema de Gestión de Seguridad de la Información (SGSI) que contribuyen a la mejora continua del proceso de Gestión TIC y la administración de sus riesgos.													Documentado en el numeral 4.5.1 del proyecto	100%