CONTRIBUIR EN EL DESARROLLO E IMPLEMENTACIÓN DEL PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN EN LA ALCALDIA DE FUSAGASUGÁ.

Juan Sebastián Gutiérrez Campos

Universidad de Cundinamarca
Ingeniería electrónica
Facultad de ingeniería
Fusagasugá, Colombia
2023

CONTRIBUIR EN EL DESARROLLO E IMPLEMENTACIÓN DEL PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN EN LA ALCALDIA MUNICIPAL DE FUSAGASUGÁ

Trabajo de grado presentado como requisito parcial para optar por el título de ingeniero electrónico

Juan Sebastián Gutiérrez Campos

Director:
Ing. Alexander Gordillo Gaitán, MSc.

Asesores:
Ing. Daniel Camilo Ramírez Martínez

Universidad de Cundinamarca
Ingeniería electrónica
Facultad de ingeniería
Fusagasugá, Colombia
2023

Resumen

Con el propósito de cumplir con los objetivos planteados durante el proceso de pasantía desarrollado en la oficina Tic de la alcaldía de Fusagasugá , donde se aplican diferentes series de actividades que ofrecen una exigencia de ética profesional al momento de presentar problemáticas que van direccionados a la ciberseguridad y conforme al ámbito de aplicación respecto a la estrategia de clasificación de activos de información en entidades públicas se propone unas directrices emitidas por el Min tic con la finalidad de implementar una gestión de seguridad informática.

Formando equipo de trabajo con la oficina TIC de la alcaldía Municipal de Fusagasugá, se ejecutó diferentes actividades orientadas al desarrollo e implementación del plan de tratamiento de riesgos de Seguridad y Privacidad de la información, apoyando la implementación y capacitación del Modelo de la Seguridad y Privacidad de la Información (MSPI), la cual está estipulada en la resolución 500 de 2021 expedida en el Ministerio De Tecnología de la Información y las Comunicaciones (MinTIC), con el objeto de realizar un seguimiento y clasificación de los activos de información de cada una de las dependencias de la entidad pública relacionada.

Fomentando los pilares fundamentales de la seguridad cibernética fundamentados en la ley 1712 de 2014 (Disponibilidad, confidencialidad e integridad) por la cual se realizó por medio de campañas y herramientas que identificaran las vulnerabilidades y posibles amenazas identificadas que fortalecieran los sistemas de gestión frente delitos informáticos en el desarrollo de identificación de posibles amenazas dentro de la alcaldía de Fusagasugá, especialmente a los funcionarios de la oficina TIC.

Uno de los procesos más relevante para el cumplimiento del modelo de Seguridad y Privacidad de la información fue las capacitaciones integradas a cada una de las dependencias de la alcaldía de Fusagasugá, esto con el fin de dar cumplimiento a las actividades propuestas por la oficina Tic, para dar evolución en el proceso de identificar los posibles activos de información.

Contenido

Índice de Figuras

Índice de tablas

Capítulo 1. Contexto

El Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC), estableció la gestión sistemática de los riesgos de seguridad digital para promover un entorno digital confiable, que maximice los beneficios económicos y sociales de todos los actores públicos y privados que se basa en unos principios fundamentales como la protección de los derechos humanos y los valores fundamentales de las personas. La adopción de un enfoque basado en el riesgo para permitir que las personas operen de forma libre y segura en el entorno digital, garantizando la responsabilidad compartida entre todos los actores involucrados (Ministerio de Tecnologías de la información y las comunicaciones Política de Seguridad Digital, 2021)

El continuo desarrollo del gobierno electrónico en Colombia, según la Oficina TIC y de acuerdo con la política de gobernanza digital donde se ha dejado en claro la importancia de las TIC en la gestión de las entidades públicas y la mejora de los servicios que brinda el estado a los ciudadanos, pero ahora hay una nueva realidad donde la política de gobernanza digital no solo mejora los procesos y servicios existentes, sino que también posibilita la implementación del proceso de transformación digital, que cambia la relación tradicional del país con el ciudadano. (Oficina Tic política de gobierno digital, 2021)

Durante el desarrollo de la pasantía y como punto de partida para el desempeño de las actividades, se realizaron diferentes procesos de capacitaciones a las dependencias de la Alcaldía de Fusagasugá, obteniendo como resultado la clasificación de los activos de información fomentando los 3 pilares de la información (Disponibilidad, integridad y confidencialidad), para el mejoramiento de las posibles vulnerabilidades presentadas en la alcaldía de Fusagasugá.

Capítulo 2. Actividades

Se plantearon y se realizaron diferentes actividades individuales en el proceso de apoyo, aplicación y uso. Contribuyendo en el desarrollo e implementación del plan de tratamiento de riesgos de seguridad y privacidad de la información en la alcaldía de Fusagasugá.

1. Apoyo en la implementación del Modelo de la Seguridad y Privacidad de la Información (MSPI) estipulado por el Min TIC a cada una de las dependencias de la Alcaldía de Fusagasugá.
2. Aplicar el modelo MSPI para el seguimiento y clasificación de riesgos de los activos de cada una de las dependencias de la Alcaldía de Fusagasugá.
3. Fomentar el principio de Disponibilidad de la información a través de campañas, capacitaciones técnicas, frente a los delitos informáticos dentro de la Alcaldía de Fusagasugá.
4. Hacer uso de herramientas de ciberseguridad para identificar vulnerabilidades y reducir las amenazas en las redes y dispositivos tecnológicos para mejorar la seguridad a los funcionarios de dependencia TIC de la Alcaldía de Fusagasugá.

Capítulo 3. Marco de referencia

Un marco de referencia es un apartado que interviene en todo proyecto de investigación donde se detallan pequeños conceptos característicos y claves para tener un contexto en que se introduce la investigación. (Etecé, 2023).

A continuación, se analiza algunos casos de estudio que simplifican los lineamientos del documento.

3.1. Antecedentes.

Los antecedentes son diferentes puntos de investigaciones previos hechos por otros autores o instituciones sobre el tema de estudio, y que guardan alguna vinculación con el problema planteado, y ayudan a comprender el fenómeno de investigación mediante teorías o conclusiones elaboradas por especialista en el tema. En esta etapa identificaremos los diferentes antecedentes sobre la ciberseguridad que brindan distintos puntos de vista sobre el planteamiento de las problemáticas que hallamos sobre la seguridad digital.

Como primer antecedente evidenciamos la tesis doctoral de Ángel Marcelo Rea, madurez en la identificación y evaluación de riesgos en ciberseguridad. Esto indica que la ciberseguridad es un concepto ampliamente utilizado en los sistemas de información para proteger los activos que abordan las amenazas que comprometen la información procesada, almacenada y transmitida por los sistemas de información. (Rea Guamán, 2020)

Según la compañía internacional dedicada a la seguridad informática Kaspersky, que define la ciberseguridad como un arte de defender las computadoras, servidores, dispositivos móviles, redes y datos de todo ataque que se pueda considerar de forma que comprometa la información o datos dentro de una entidad. (Kaspersky, 2020)

Analizamos casos de estudio donde se evidencia los costos por los delitos cibernéticos, este estudio llamado “The Cost of Cybercrime” y combina la investigación a través de 16 industrias, las cuales se entrevistaron a diferentes líderes de 355 empresas para determinar el impacto económico, lo cual se tomó que Estados Unidos encabeza una lista con un costo anual por medio del delito cibernético que aumentó en un 29% en 2018 para llegar a US $ 27,4 millones, en relación al 2017 que obtuvo delitos informáticos que consumen $ 11,7 millones por empresa, en el Reino Unido las

organizaciones experimentaron un aumento del 31% que equivale a US $11,5 millones, seguida de Japón que aumentó en un 30% en 2018 para alcanzar los US $ 13,6 millones, por ello es importante siempre evidenciar la importancia que conlleva la ciberseguridad, (Accenture and Ponemon institute, 2019).

A Nivel nacional podemos tomar como referencia el artículo de la Revista Criminalidad, donde se puede identificar datos relevantes de las perdidas monetarias de ataques cibernéticos a nivel empresarial, al igual podemos determinar que la mayoría de las empresas colombianas no cuentan con sistema de seguridad digital para el tratamiento de sus activos de información, esto las hace vulnerables a cualquier ataque cibernético (Ospina Diaz et al, 2020).

Colombia fue uno de los primeros países de América Latina en ser golpeado por ciberataques en 2022, empresas tales como EPM, EPS Sanitas, INVIMA, Viva Air, Claro Colombia, Carvajal, la Universidad Javeriana y la fiscalía general del país, fueron las entidades escogidas por los ciberdelincuentes. Uno de los modus operandi más utilizados en los ciberataques es la introducción de ransomware en las organizaciones, especialmente en aquellas que no cuentan con una política de ciberseguridad donde estas técnicas pueden ser utilizadas como spam malicioso que contiene archivos maliciosos o redirigido a páginas web que afectan a los sistemas. Sophos realizó una investigación de ransomware en 2022 y descubrió que 2,04 millones de dólares fueron pagados en recuperación de datos. (Molano Diego, 2023)

Identificamos otra fuente de investigación, tesis realizada por Peña Barranco Geovanna Patricia, titulada marco de gobierno y gestión de ciberseguridad para ciudades inteligentes en el contexto colombiano, se analiza el futuro que tiene que ver con el crecimiento poblacional en ciudades y el manejo de las tecnologías que va de la mano con la ciber seguridad.

En esta esta tesis se analiza una propuesta de transformación de ciudades tradicionales en ciudades inteligentes, teniendo en cuenta el crecimiento poblacional en zonas urbanas y la cual se tiene, se analizan procesos de tecnología como lo es el internet de las cosas (IoT), que permiten integrar datos captados por dispositivos y poder analizarlos, y es allí donde este avance tecnológico es susceptible a las amenazas de ciber ataque obteniendo como beneficio un frente a los diversos sistemas de ataque, mejorando la operatividad y la toma de decisiones en busca de ser más eficientes en la prestación de estos servicios (Peña Barranco-Geovanna Patricia, 2021).

Podemos determinar diferentes líneas de investigación a profundidad de la ciberseguridad, tales como la importancia de las posibles amenazas, los tipos de programas maliciosos y de ciber atacante, activos de una organización, riegos, vulnerabilidades y amenazas de ciber seguridad, que da una visión diferente del manejo de nuestros activos de información teniendo en cuenta diferentes procesos para la identificación de las posibles fracturas identificadas en la organización.

3.2. Fundamentos teóricos.

En este punto se identificaron conceptos teóricos que tuvieron como base para el desarrollo óptimo de la pasantía realizada en la alcaldía de Fusagasugá.

3.2.1. Ciberseguridad

La ciberseguridad se determina en proteger los sistemas críticos y la información confidencial de todo aquello que se podría tomar como un ataque digital. Combatir las amenazas a los sistemas y aplicaciones en red también conocidas como seguridad de la tecnología de la información (TI), independientemente de si las amenazas se originan dentro o fuera de la organización a la que están destinadas. (IBM, 2020).

3.2.2 Modelo de Seguridad y Privacidad de la Información.

Según MINTIC el Modelo de Seguridad y Privacidad de la Información - MSPI, Orienta y posibilita la adecuada gestión e implementación del ciclo de vida de la seguridad de la información (planificación, implementación, evaluación y mejora continua), haciendo referencia a estándares internacionales y brindando orientación pública sobre la implementación y adopción de las mejores prácticas que proporcione a la institución. (Ministerio de Tecnología de la información y las comunicaciones, 2022)

Esto se basa en el marco de referencia de la arquitectura de TI, el modelo integrado de planificación y control (MIPG) y la Guía para la gestión de riesgos y diseño en los sectores públicos. Este modelo es uno de los pioneros integrales de la política de seguridad y protección de datos y gobierno digital, se desarrollará a través del documento maestro del Modelo de Seguridad y Privacidad de la Información y su documento guía donde debe ser desarrollado por un líder o responsable de seguridad de la información con el apoyo de toda la estructura organizacional. De acuerdo con el

Modelo de Seguridad y Privacidad de la Información (MSPI), se evidencia en la Figura 1 y Figura 2 un análisis más a profundidad.

Ciclo de operación del MSPI

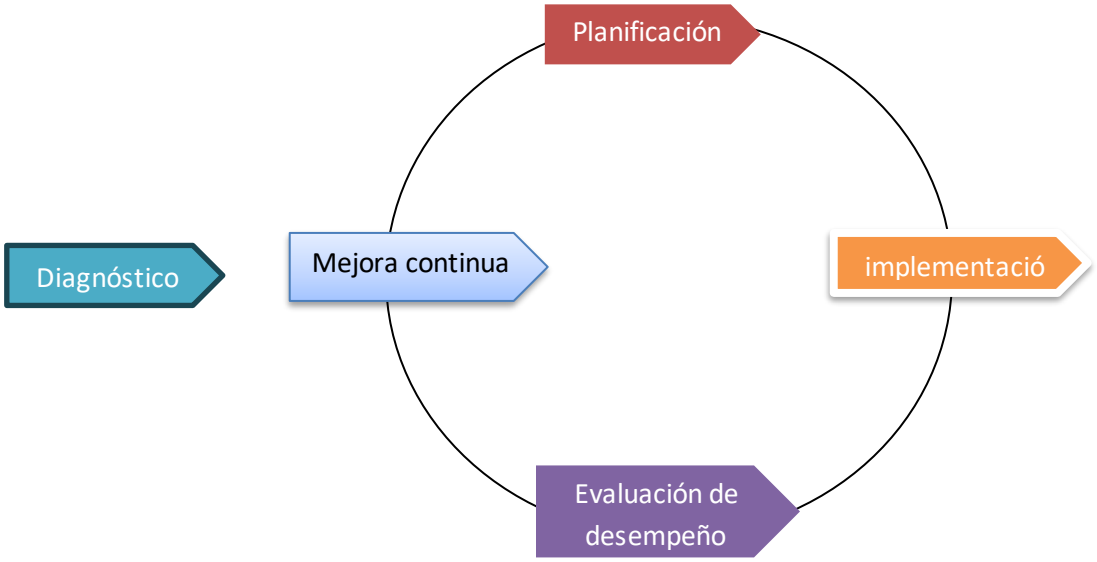

Figura 1. Ciclo de operación.
Fuente: Min tic, 2021.

Concorde a esto podemos identificar 5 procesos que inicia en el diagnostico identificando el estado de los activos de información de la entidad, consiguiente se analiza una planificación los cuales se alinean con un análisis y tratamiento de los riegos, una tercera fase de implementación de los planes de tratamientos de riegos, las actividades de monitoreo y revisión para una evaluación de desempeño y por ultimo un continuo mejoramiento que determinan acciones correctivas durante el proceso.

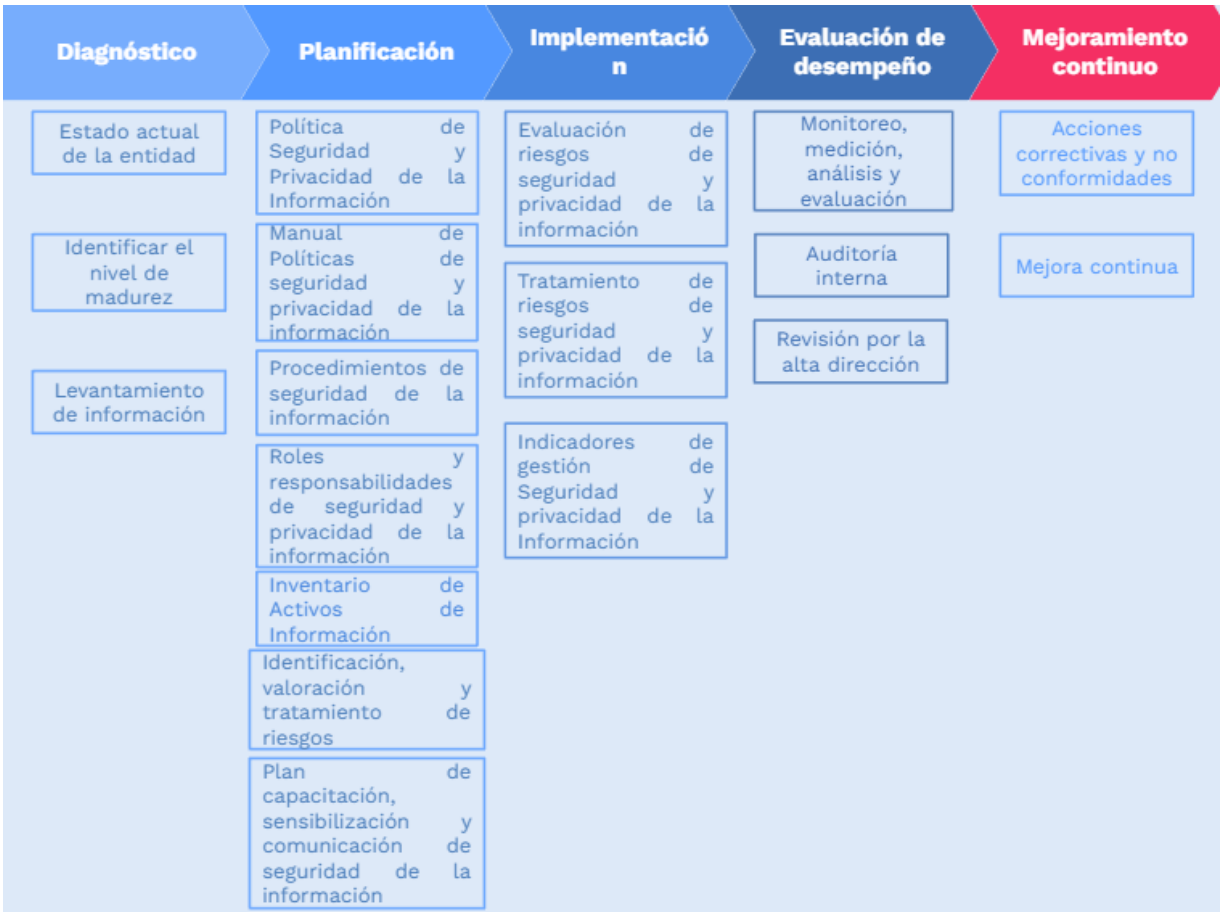

Figura 2. Ciclo de operación características.
Fuente: Min tic, 2021.

Conforme a la Figura 2 podemos realizar un análisis más profundo de cada uno de los procesos determinando las características principales para el óptimo desarrollo del modelo de seguridad y privacidad de la información (MSPI).

3.2.3. Activos de información

Según MINTIC (Ministerio de Tecnología de la información y las comunicaciones, 2021) Los activos de información es cada dato por clasificar activos de la empresa de acuerdo con la política general de seguridad y privacidad de la información. Esta política define los activos que posee la compañía, cómo se utilizan, funciones y responsabilidades establecidas en la Figura 3 y Figura 4 explican mayores rasgos en la gestión e identificación de los activos de información.

Figura 3. Gestión de activos.
Fuente: Min tic, 2021

Conforme con el Ministerio de Tecnologías de la Información y las comunicaciones (Min tic), podemos deducir que los activos de información son todo tipo de datos física y digital que se encuentran en este caso en las entidades públicas y determinarlas por diferentes características según su uso, donde se generan algún tipo de activo que requiera ser clasificado de acuerdo con la ley 1712 que resalta tres maneras de clasificarlas según los pilares de las seguridad que son la confidencialidad, integridad y disponibilidad.

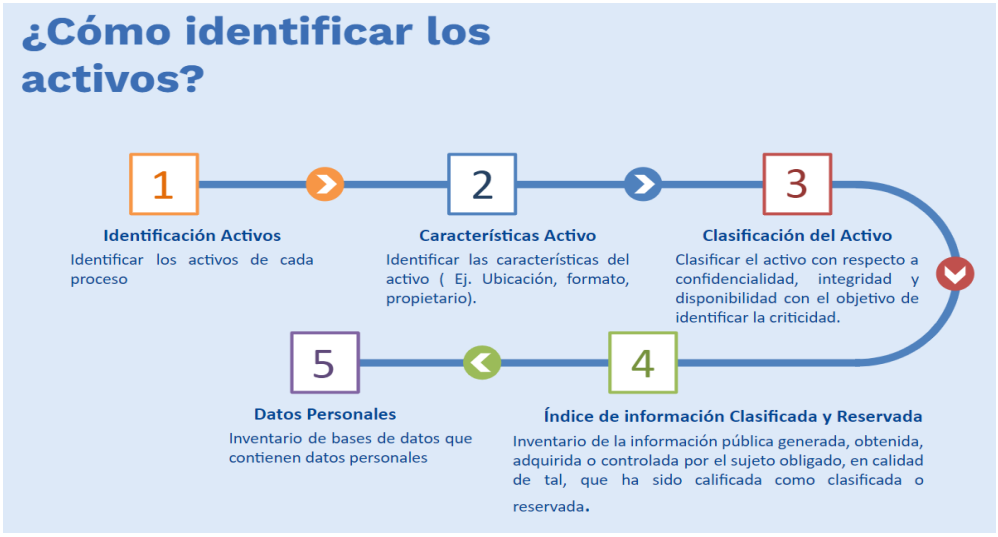

Figura 4. Identificación de activos.
Fuente: Min tic, 2021.

3.2.4. Norma ISO 27001

La Organización Internacional para la Estandarización (ISO) publicó ISO 27001, un estándar global que describe cómo administrar la seguridad de la información en una empresa. El nombre completo de esta norma, que se actualizó por última vez en 2013, ahora es ISO/IEC 27001:2013. Basado en el estándar británico BS 7799-2, la primera revisión se publicó en 2005. (Advisera, 2022)

3.2.5. Pilares de la seguridad de la información

Confidencialidad

Este pilar está relacionado con la protección de datos, por lo que incluye actividades encaminadas a garantizar que la información reservada y confidencial esté protegida y no sea robada mediante ciberataques, espionaje u otros delitos informáticos (DocuSign, 2021).

Integridad

La integridad es un pilar de la seguridad de la información que se identifica en mantener la precisión y consistencia de los datos u sistemas comerciales a lo largo de la vida de un proceso o negocio. En otras palabras, la integridad garantiza la exactitud de la información, lo que significa que la información no se puede cambiar sin permiso previo. Sin embargo, si hay un cambio innecesario, inesperado o no planificado, la información puede cambiar de forma irreversible. (DocuSign, 2021).

Disponibilidad

"El tercer pilar de la seguridad de la información tiene que ver con el tiempo y el acceso a los datos y sistemas comerciales, poder verlos en el momento adecuado". (DocuSign, 2021).

3.2.6. Amenazas cibernéticas

Malware

Malware se identifica a variantes de programas maliciosos tales como gusanos informáticos, virus y programas espías, que pueden dar un acceso no autorizado y puedan causar dalos al sistema operativo. Los ataques de estos programas están determinados para evadir métodos de detección como herramientas de antivirus que escanean archivos maliciosos. (IBM, 2022)."

Ransomware

El ransomware es un tipo de programa maligno que bloquea archivos, datos o sistemas, elimina o destruye datos, o amenaza con divulgarlos de forma privada o confidencial al público a menos que se pague un rescate a los ciberdelincuentes que lanzaron el ataque. (IBM, 2022). “

3.3. Marco legal

La siguiente tabla proporciona las bases normativas por las que se rige la dependencia de la Oficina TIC, que construye y decreta los lineamientos de la ciber seguridad:

AÑO	NORMATIVIDAD	DESCRIPCIÓN
2012	Ley 1581	Por el cual se dictan disposiciones generales para la protección de datos personales
2012	Decreto 0884	Por medio del cual se reglamenta la Ley 1221 de 2008 y se dictan otras disposiciones
2013	Decreto 1377	Por el cual se reglamenta parcialmente la Ley 1581 de 2012.
2014	Ley 1712	Por medio de la cual se crea la Ley de transparencia y del derecho de acceso a la información Pública Nacional y se dictan otras disposiciones.
2015	Decreto 1078	Por medio del cual se expide el Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones.
2016	Decreto 0415	Por el cual se adiciona el Decreto Único Reglamentario del sector de la Función Pública, Decreto número 1083 de 2015, en lo relacionado con la definición de los lineamientos para el fortalecimiento institucional en materia de Tecnologías de la Información y las Comunicaciones
2017	Decreto 0728	Por el cual se adiciona el Capítulo 2 al Título 9 de la Parte 2 del Libro 2 del Decreto Único Reglamentario del sector TIC, Decreto 1078 de 2015, para fortalecer el modelo de Gobierno Digital en las entidades del orden nacional del Estado colombiano, a través de la implementación de zonas de acceso público a Internet inalámbrico.
2017	Decreto 1413	Por el cual se adiciona el Título 17 a la Parte 2 del Libro 2 del Decreto Único Reglamentario del sector de Tecnologías de la Información y las Comunicaciones,

		Decreto número 1078 de 2015, para reglamentarse parcialmente el Capítulo IV del Título III de la Ley 1437 de 2011 y el artículo 45 de la Ley 1753 de 2015, estableciendo lineamientos generales en el uso y operación de los servicios ciudadanos digitales.
2017	Resolución 3436	Por la cual se reglamentan los requisitos técnicos, operativos y de seguridad que deberán cumplir las zonas de acceso a Internet inalámbrico de que trata el Capítulo 2, Título 9, Parte 2, Libro 2 del Decreto 1078 de 2015.
2018	Ley 1928	Por medio de la cual se aprueba el «convenio sobre la ciberdelincuencia», adoptado el 23 de noviembre de 2001, en Budapest.
2018	Decreto 1008	Por el cual se establecen los lineamientos generales de la política de Gobierno Digital y se subroga el capítulo 1 del título 9 de la parte 2 del libro 2 del Decreto 1078 de 2015, Decreto Único Reglamentario del sector de Tecnologías de la Información y las Comunicaciones.
2021	Resolución 500	Por la cual se establecen los lineamientos y estándares para la estrategia de seguridad digital y se adopta el modelo de seguridad y privacidad como habilitador de la política de Gobierno Digital.
2021	Decreto 45	Por el cual se derogan el Decreto 704 de 2018 y el artículo 1.1.2.3. del Decreto número 1078 de 2015, Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones.
2000	Ley 594	La presente ley tiene por objeto establecer las reglas y principios generales que regulan la función archivística del Estado.
2015	Decreto 103	Este decreto tiene por objeto reglamentar la Ley 1712 de 2014, en lo relativo a la gestión de la información pública.
2012	Ley 1581	Ley que complementa la regulación vigente para la protección del derecho fundamental que tienen todas las personas naturales a autorizar la información personal que es almacenada en bases de datos o archivos, así como su posterior actualización y rectificación.

Tabla 1. Normativa.
Fuente: Propia.

Capítulo 4. Plan de trabajo

En este capítulo se identificarán los procesos y procedimientos que se utilizaron para el desarrollo de cada una de las actividades en la Alcaldía de Fusagasugá.

4.1 Apoyo en la implementación del Modelo de la Seguridad y Privacidad de la Información (MSPI) estipulado por el Min TIC a cada una de las dependencias de la Alcaldía de Fusagasugá.

- Como primera actividad a realizar fue el reconocimiento del Modelo y Seguridad y Privacidad de la información de los documentos y conceptos relacionados al municipio de Fusagasugá, tales como la gestión de las TIC, la infraestructura (Data center), proyectos, decretos y su modelo de seguridad además de obtener un buen control de privacidad de la información.

- A partir de tener una base de conocimientos sobre la gestión que se iba a realizar a cada una de las dependencias de la alcaldía de Fusagasugá sobre temas de activos de información y el correcto diligenciamiento de la MATRIZ DE INVENTARIO Y CLASIFICACIÓN DE ACTIVOS DE INFORMACIÓN, se procede a la respectiva organización de reuniones para impartir el modelo de seguridad solicitado por el MINTIC.

- Relacionado a esto se realiza una circular informativa que fue enviada mediante el software (ControlDoc) que es un sistema de gestión documental y sirve para para la gestión de los procesos generales de los sistemas certificables, la cual por medio de esta circular se proporciona el respectivo link de consulta para el propósito de la organización en donde cada dependencia proporcionaba la información necesaria como nombres, el correo electrónico, la dependencia a la que pertenece y una fecha con horario específico para la construcción de agendamiento de cada una de las entidades de la alcaldía de Fusagasugá.

4.2 Aplicar el modelo MSPI para el seguimiento y clasificación de riesgos de los activos de cada una de las dependencias de la Alcaldía de Fusagasugá.

De acuerdo a lo planteado y dando seguimiento al cronograma del horario establecido por cada una de las dependencias de la Alcaldía de Fusagasugá se procede con las respectivas capacitaciones con todas las dependencias de la entidad, dando la introducción de los puntos a conocer del Modelo de seguridad y Privacidad de la Información, sus activos de información y el correcto diligenciamiento de la matriz de activos de información respetando la normatividad dicha por esta, lo cual se aplicó y se dio a conocer los ítems a llenar propuestos por el Min Tic tales como macroproceso, proceso, confidencialidad e disponibilidad, entre otros. A continuación, en la Tabla 2 se identifica la secretaría y su respectiva fecha.

DEPENDENCIA	FECHA
Capacitación con secretaria de planeación.	7 de septiembre de 2021
Capacitación con secretaria de agricultura, ambiente y tierras.	8 de septiembre de 2021
Capacitación con secretaria de educación.	8 de septiembre de 2021
Capacitación con secretaria de familia e integración social.	9 de septiembre de 2021
Capacitación con secretaria jurídica.	10 de septiembre de 2021
Capacitación con secretaria de salud.	14 de septiembre de 2021
Capacitación con oficina de proyectos.	15 de septiembre de 2021
Capacitación con oficina de control interno disciplinario.	16 de septiembre de 2021
Capacitación con oficina de turismo.	20 de septiembre de 2021
Capacitación con secretaria de agricultura, ambiente y tierras (presencial)	21 de septiembre de 2021
Capacitación con secretaría de hacienda.	23 de septiembre de 2021
Capacitación con oficina de control interno.	27 de septiembre de 2021

Capacitación con secretaria de gobierno, seguridad y convivencia.	27 de septiembre de 2021
Capacitación con oficina de desarrollo institucional.	29 de septiembre de 2021

Tabla 2. Capacitaciones.
Fuente propia.

Conforme a esto se da por concluido este proceso de reconocimiento del correcto diligenciamiento se da un plazo de 8 días para la respectiva entrega de la matriz, con la posibilidad de realizar una nueva reunión para dar seguimiento y las posibles dudas que se generan durante el proceso de diligenciamiento de la matriz de activos de información. A continuación, en la Figura 5 y Figura 6 se evidencia algunas de estas capacitaciones dadas:

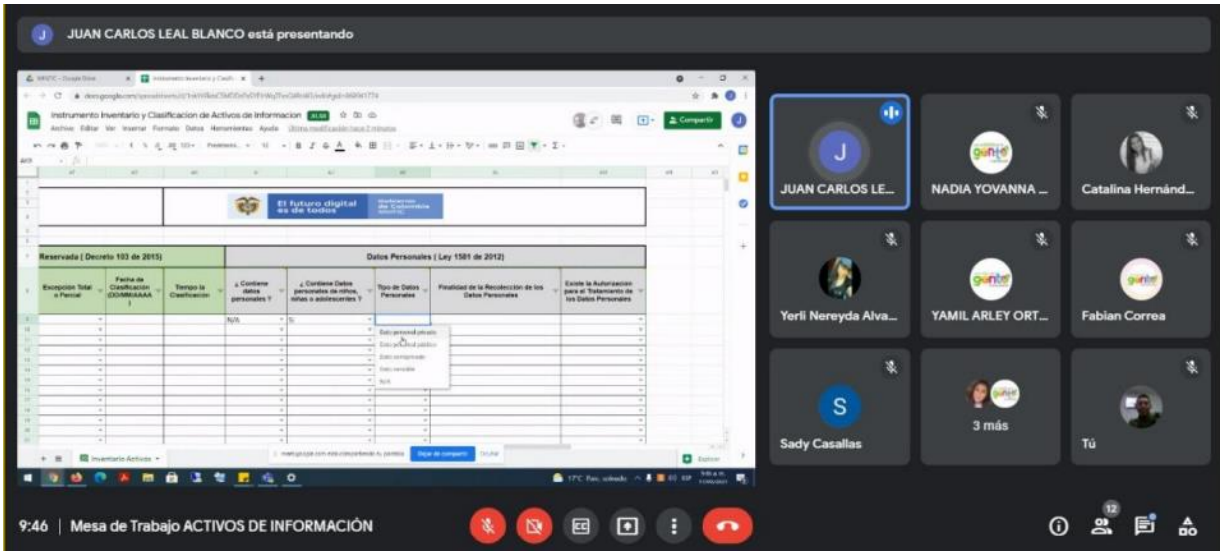

Figura 5. Secretaria de planeación.
Fuente: Propia.

Figura 6. Reunión con secretaria de agricultura, ambiente y tierras. Fuente: Propia.

Conforme con lo establecido se brindó el apoyo y la guía pertinente en la implementación de las políticas de seguridad en cuanto a la conceptualización de todos los criterios determinados en la matriz de inventario y clasificación de activos de información , realizada por el Min Tic, lo cual esta guiada por 4 puntos específicos que son la identificación del activo de información, determinada por (Ley 594 de 2000 – Ley 1712 de 2014 – Decreto 103 de 2015 – Decreto 1080 de 2015 – ISO 27001), clasificación del activo de información (ISO 27001), índice de información clasificada y reservada (Decreto 103 de 2015) y datos personales (Ley 1581 de 2012), estos 4 puntos direccionan el diligenciamiento de la matriz, lo cual fueron los temas a tratar en dichas reuniones planteadas por el oficial de seguridad. Para observar al detalle los temas mencionados en la capacitación referirse a Apéndice 2. Seguridad y privacidad de la información.

4.3. Fomentar el principio de Disponibilidad de la información a través de campañas, capacitaciones técnicas, frente a los delitos informáticos dentro de la Alcaldía de Fusagasugá.

En esta actividad se realizaron apoyos de sensibilización a la oficina TIC de la alcaldía de Fusagasugá aplicando los procesos de disponibilidad de la información, para así obtener que las dependencias de la alcaldía de Fusagasugá conozcan e identifiquen

los riesgos a los que están expuestos en el entorno digital y aprendan como protegerse, prevenir y reaccionar ante delitos y ataques cibernéticos tales como:

- Robo de credenciales.
- Fugas de información.
- Virus.
- Rasomware.
- Phishing.

- Como segunda medida se realizó un soporte y mantenimiento a cada uno de los ordenadores de las dependencias de la alcaldía de Fusagasugá, en este mantenimiento se realizaba la verificación de impurezas de una forma interna y externa, limpieza cuidadosa de los componentes electrónicos, verificación de funcionamiento y validación de todos los componentes para el óptimo manejo del equipo, en la Figura 7 podemos observar las evidencias pertinentes acorde a lo solicitado.

Figura 7. Mantenimientos ordenadores de las dependencias.
Fuente: Propia.

- En consecuencia a lo planteado se realizó sensibilización sobre los activos de información, la cual como punto principal es informar a funcionarios específicos de cómo manejar, manipular y emplear cada uno de los activos que se manejan diariamente en la alcaldía de Fusagasugá, en la Figura 8 podemos observar las evidencias pertinentes acorde a lo solicitado.

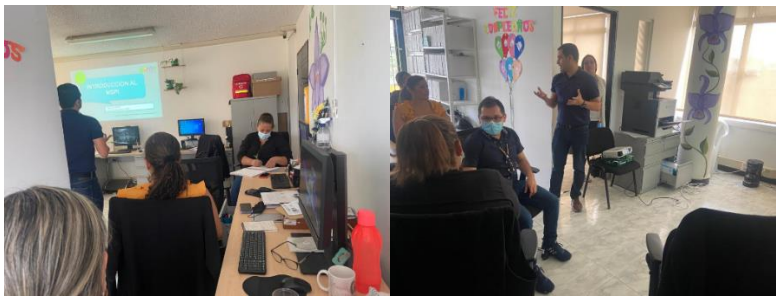

Figura 8. Sensibilización a funcionarios de las dependencias.
Fuente: Propia

- Explicación de software FOCA en el festival latinoamericano de software libre, en donde la principal actividad era exponer que es, su funcionamiento y para qué sirve este software como fin de dar sensibilización de los metadatos que contienen cada uno de los archivos que manejamos día a día, analizando que FOCA se especializa en la extracción de aquella información adicional incrustada en los ficheros de cada documento, en la Figura 9 se evidencia la socialización que se realizó en el evento organizado por la Alcaldía de Fusagasugá.

Figura 9. Explicación herramienta FOCA.
Fuente: Propia

4.4 Hacer uso de herramientas de ciberseguridad para identificar vulnerabilidades y reducir las amenazas en las redes y dispositivos tecnológicos para mejorar la seguridad a los funcionarios de dependencia TIC de la Alcaldía de Fusagasugá.

Concorde con la actividad planteada se realizaron diferentes tareas específicas, la cual ayuda en el fortalecimiento de la ciberseguridad en las dependencias de la alcaldía de Fusagasugá, como primera medida se realizó:

- Apoyo en la realización del nuevo canal de internet y un análisis de vulnerabilidades a sistemas de la alcaldía de Fusagasugá, lo cual en la Figura 10 se evidencia el apoyo pertinente guiado por el oficial de seguridad a cargo.

Figura 10. Apoyo a identificación de vulnerabilidades.
Fuente: Propia

A través de la herramienta NMAP que es un software de código abierto que se utiliza para escanear redes y sus puertos para obtener información importante sobre las redes para controlar y administrar la seguridad. Normalmente se utiliza para auditorías de seguridad y supervisión de redes.

- Conocimiento de ZABBIX, una herramienta de software libre utilizada para el monitoreo de código abierto de redes y aplicaciones. Supervisa miles de métricas recopiladas de servidores, máquinas virtuales, dispositivos de red y aplicaciones web en tiempo real. En este caso, para monitorear y registrar el estado de varios servicios desde el servidor de la Alcaldía de Fusagasugá. A continuación, en la Figura 11 se evidencia la sesión realizada para mayor profundidad de la herramienta:

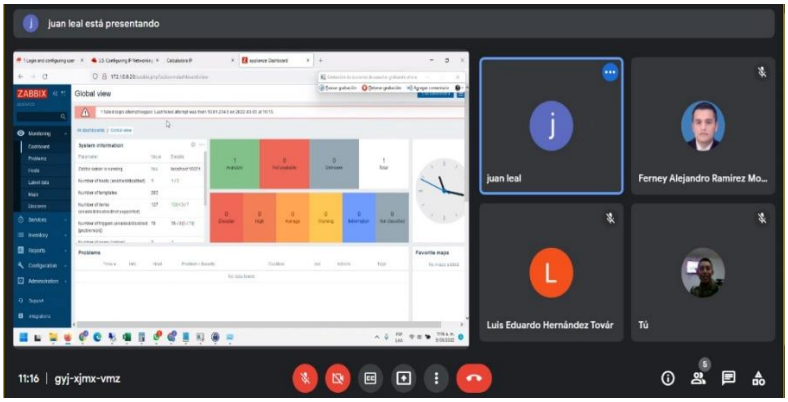

Figura 11. Profundización de la herramienta ZABBIX.
Fuente: Propia.

De acuerdo con la solicitud planteada del oficial de seguridad se pudo identificar una posible vulnerabilidad, ya que se identificaban gran cantidad y variedad de usuarios con la totalidad de permisos, lo cual no es conveniente para la seguridad de los ordenadores y activos de la oficina Tic.

- Instalación de antivirus licenciado ENDPOINT SECURITY, a los equipos de dominio de la alcaldía de Fusagasugá, en la Figura 12 se identifican las evidencias de dicho proceso realizado.

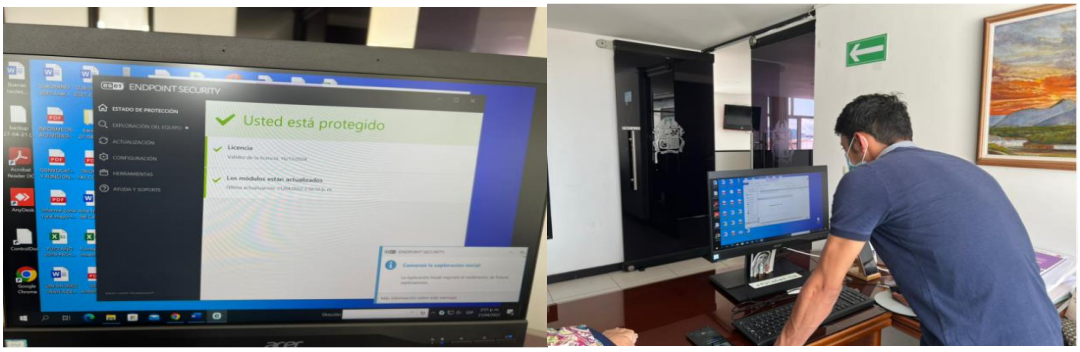

Figura 12. Instalación Antivirus.
Fuente: Propia.

Ajustado con la solicitud presentada por el oficial de seguridad se realizó el proceso de instalación de antivirus a los equipos de dominio de la alcaldía de Fusagasugá, ya que no se contaba con un antivirus licenciado que generara una protección adecuada a los problemas de seguridad a los que se encuentran expuestos los principales ordenadores de la alcaldía de Fusagasugá, así se genera una mitigación en cuanto los posibles ataques de software maliciosos específicamente en la web.

Capítulo 5. Análisis de resultados

Para lograr los objetivos originales de las pasantías realizadas en la Alcaldía de Fusagasugá, en este capítulo se evalúan los resultados del plan de trabajo establecido. Por lo tanto, se nombra cada actividad y el resultado obtenido de ella.

5.1. Aplicar el modelo MSPI para el seguimiento y clasificación de riesgos de los activos de cada una de las dependencias de la Alcaldía de Fusagasugá.

En la Figura 13 identificamos los porcentajes sobre el valor total de los objetivos planteados sobre el proceso de la actividad realizada verificando actividades principales sobre el Modelo de Seguridad y Privacidad de la Información. Para observar al detalle de las subtareas referirse al apéndice 3.

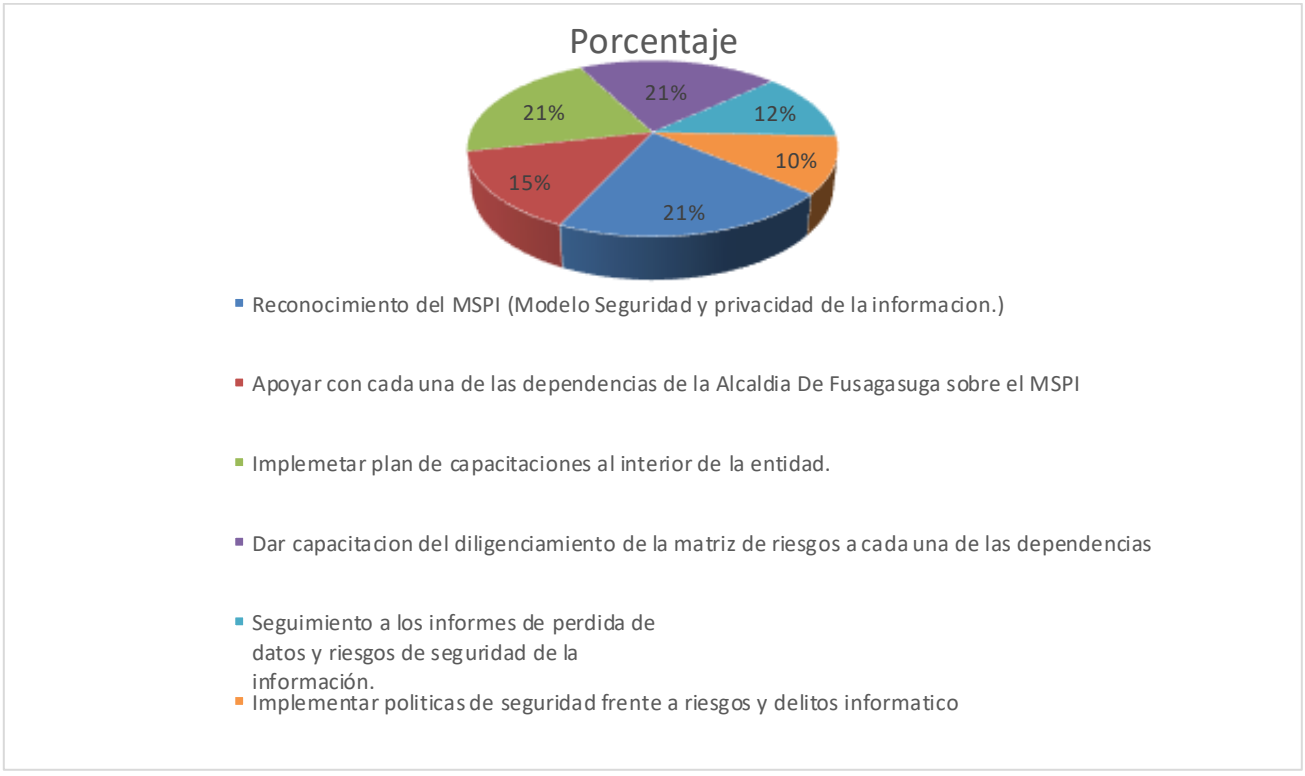

Figura 13. Porcentaje actividades completadas.
Fuente propia.

- Con la información suministrada por el oficial de seguridad de la oficina TIC de la alcaldía de Fusagasugá, se organizó cada una de las reuniones propuestas,

para dar una capacitación requerida sobre los activos de información impuesta por el MINTIC, obteniendo en la Figura 14 los siguientes resultados.

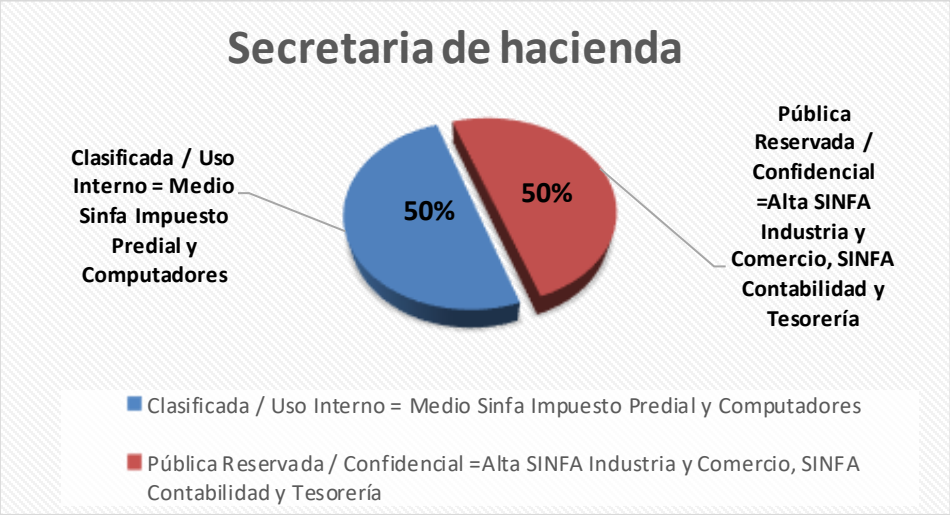

Figura 14. Clasificación VS confidencialidad.
Fuente propia.

- Como primer resultado obtuvo 4 activos de información brindados por la secretaria de Hacienda, la cual se concluyó una clasificación de acuerdo con el nombre y su respectiva confidencialidad analizando que encontramos 2 activos de información clasificada de manera media lo cual son documentos que están en un constante cambio, y tienen la visualización solamente de las personas a cargo de estos documentos, por otro lado encontramos activos de clasificación alta lo cual nos indica que están a cargo del líder de la entidad y no puede ser visualizada por diferentes entes.

- En el segundo ítem enviado por la secretaría de Gobierno mediante la Tabla 3 se analiza que se encuentran 20 diferentes tipos de documentos de información la cual cada uno de ellos se encuentra en el tipo de clasificación Clasificada / Uso Interno = Medio, obteniendo así un 100% que los activos nombrados por la secretaria no están directamente asociados de manera pública y solo es gestionada por algunos funcionarios autorizados para el tratamiento de esta información.

SECRETARIA DE GOBIERNO	
NOMBRE	**CONFIDENCIALIDAD**
COMISIONES	Clasificada / Uso Interno = Medio
Comportamientos contrarios a la actividad económica	
Comportamientos contrarios a la expulsión de domicilio ajeno	
Comportamientos contrarios a la Integridad Urbanística	
Comportamientos contrarios a la posesión y mera tenencia, servidumbre y ocupación de hecho de bienes inmuebles	
Comportamientos contrarios a la salud pública	
Comportamientos contrarios a la tranquilidad y relación respetuosa de las personas	
Comportamientos contrarios al cuidado e integridad del espacio público	
Comportamientos contrarios al medio ambiente - flora, fauna y agua	
Comportamientos contrarios que afectan a los animales	
Comportamientos contrarios que afectan la seguridad en bienes de servicios públicos	
Comportamientos contrarios que ponen en riesgo la vida y seguridad	
DECOMISOS	
Informes de actividades	
Inventarios de transferencias Documentales	
Libros de registros de infracciones y contravenciones	
Peticiones	
Quejas	
Reclamos y sugerencias	

Tabla 3. Activos de secretaría de gobierno.
Fuente: Propia.

De acuerdo con la Figura 15 podemos deducir que en la secretaria de Familia e Integración Social se analizan 54 archivos de información la cual en 31 son documentos que no son accesibles a todo público y son custodiados por el oficial a cargo de la dependencia, contrario a esto los activos de uso interno medio equivalentes a 22 activos proporcionan el 40.74%, y solo cuentan con un activo la cual puede ser visible al público en general.

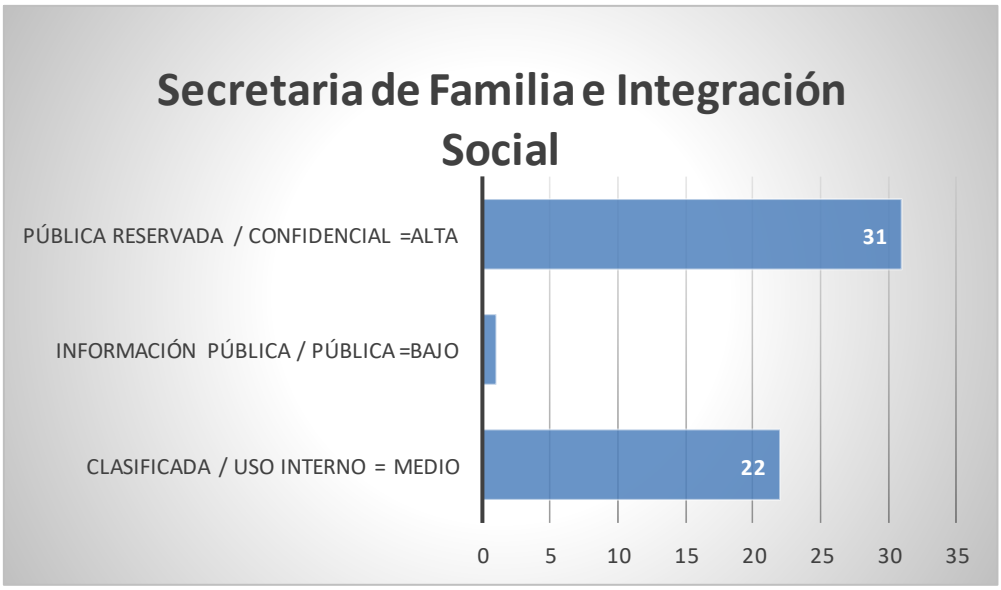

Figura 15. Activos VS confidencialidad secretaria de Familia.
Fuente: Propia

Acorde con la Figura 16 la secretaria de Dirección de Planificación de Desarrollo y Finanzas Publicas, analizamos que, en sus 24 activos de información, 22 son netamente publica que son equivalentes al 80%, lo cual significa que esta información puede ser revisada por cualquier ente que desee conocer sobre los archivos que están bajo esta clasificación.

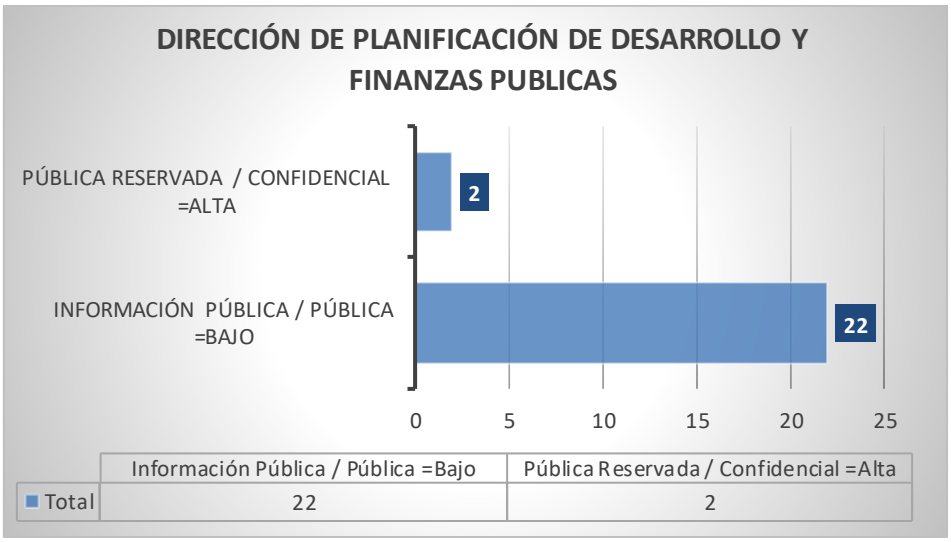

Figura 16. Activos VS confidencialidad secretaria de dirección.
Fuente: Propia.

Conforme con la Figura 17 la secretaria de secretaria Oficina de Proyectos, identificamos 44 activos de información, lo cual equivale a 70.4% son netamente publica, y con un índice de cero activos de información en clasificación Alta.

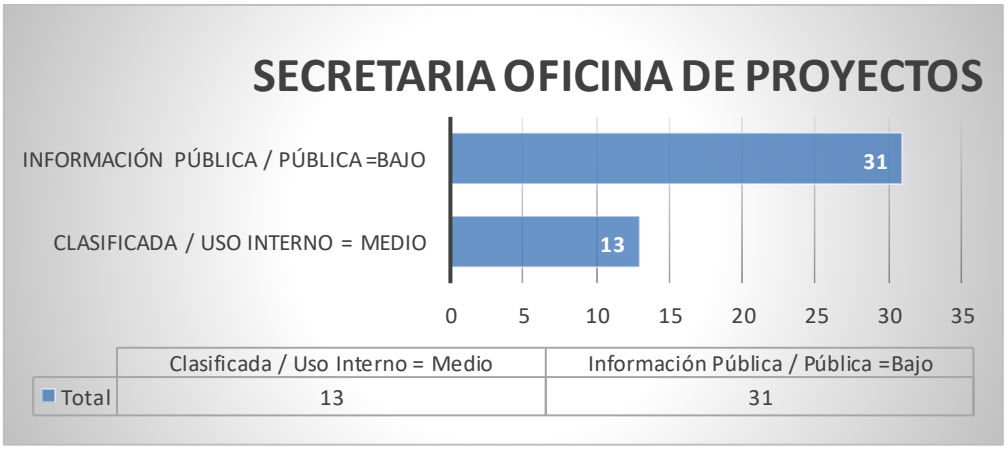

Figura 17. Activos VS confidencialidad secretaria de proyectos.
Fuente: Propia.

Correspondiente a la actividad planteada y sus subtareas podemos determinar que el alcance final en porcentaje concorde a cada uno de los ítems identificados al plan de trabajo en cuanto a los sistemas encargados de reconocimiento, apoyo, implementación y capacitación se cumplió en un 48, 97 % dando así un alto flujo de implementación del modelo de Seguridad y Privacidad de la información en cuestión de clasificación de activos de información y todos los ítems de prioridad que conforma la norma.

5.2. Fomentar el principio de Disponibilidad de la información a través de campañas, capacitaciones técnicas, frente a los delitos informáticos dentro de la Alcaldía de Fusagasugá.

En la Figura 18 identificamos los porcentajes sobre el valor total de los objetivos planteados sobre el proceso de la actividad realizada, objetualizando un alto porcentaje en el mantenimiento preventivo principalmente a los equipos de las dependencias de la alcaldía de Fusagasugá que a su vez se establecía procedimientos de mejora en activación de la disponibilidad del mantenimiento realizado. Para observar al detalle de las subtareas referirse a al apéndice 3.

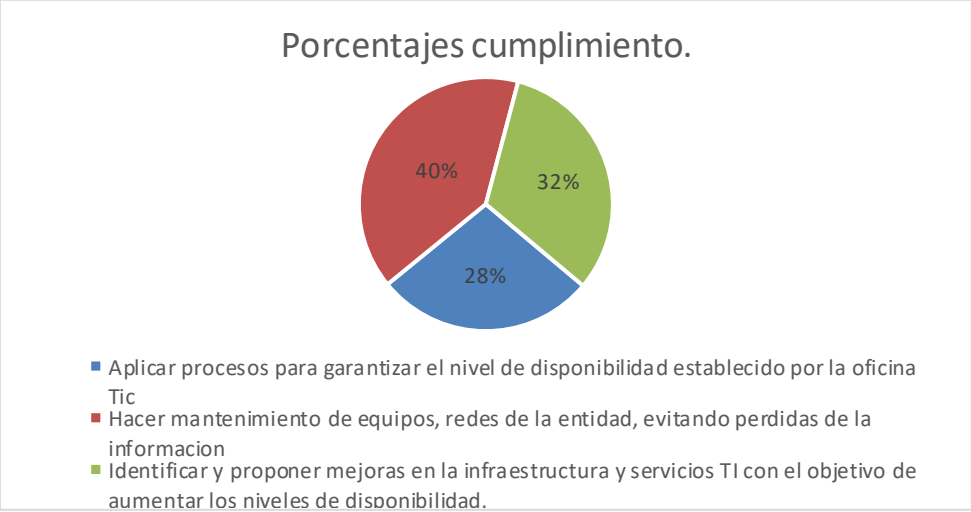

Figura 18. Porcentajes de cumplimiento.
Fuente propia.

Como primera medida para fomentar el principio de delitos informáticos se realizó un mantenimiento preventivo general a cada una de las dependencias de la Alcaldía de Fusagasugá, obteniendo resultados generales de totales de equipos de las dependencias de la alcaldía de Fusagasugá, en la Tabla 4 se analiza el total de porcentaje de equipos que fueron puestos a esta actividad.

NO. DE EQUIPOS	**620**
FORMATO Código: FO-GT-005	**620**
FIRMAS FORMATO Código: FO-GT-003	**620**
EQUIPOS EN INVENTARIO	**620**
TOTAL, MANTENIMIENTOS REALIZADOS	**549**
PORCENTAJE= **FIRMAS FORMATO Código: FO-GT-003 X 100** **NO. DE EQUIPOS**	**88,55**

Tabla 4. Ordenadores Dependencias Alcaldía.
Fuente Oficina TIC Alcaldía de Fusagasugá.

Dando como resultado un porcentaje de ejecución del plan de mantenimiento preventivo en un 88,55% de su totalidad. En donde se realizaban acciones a cada uno de los ordenadores tales como:

- Mantenimiento de hardware: Donde se especificaba el retiro de polvo, validación de pasta térmica del procesador, memoria RAM, fuente de poder, funcionamiento de ventiladores y encendido.

- Mantenimiento de Software: Se valida desde la BIOS que el dispositivo de arranque sea el disco duro, arranque del Sistema Operativo, se valida por medio del comando netplwiz, la existencia de un usuario administrador del equipo, licenciamiento del Sistema Operativo, etc.

Según lo planteado unas las principales actividades que conducía a fomentar el principio de disponibilidad era el mantenimiento preventivo de equipos, redes y plantas físicas de la entidad, lo cual permitía garantizar procesos de protección de datos en los equipos de las dependencias de la alcaldía de Fusagasugá, evaluando comando de mantenimiento lógico a través de CMD tales como %temp% o prefectch e instalación del programa ccleaner, que permitía una evaluación del estado del equipo y su mejoramiento, obteniendo así 25,51 % de los objetivos totales.

5.3. Hacer uso de herramientas de ciberseguridad para identificar vulnerabilidades y reducir las amenazas en las redes y dispositivos tecnológicos para mejorar la seguridad a los funcionarios de dependencia TIC de la Alcaldía de Fusagasugá.

En la Figura 19 determinamos los porcentajes sobre el valor total de los objetivos planteados sobre el proceso de la actividad realizada, dando prioridad a herramientas o software que permitían identificar vulnerabilidades planteadas por el oficial de

seguridad, una de esas herramientas identificadas es la plataforma ZABBIX que complementa en la instrucción dada.

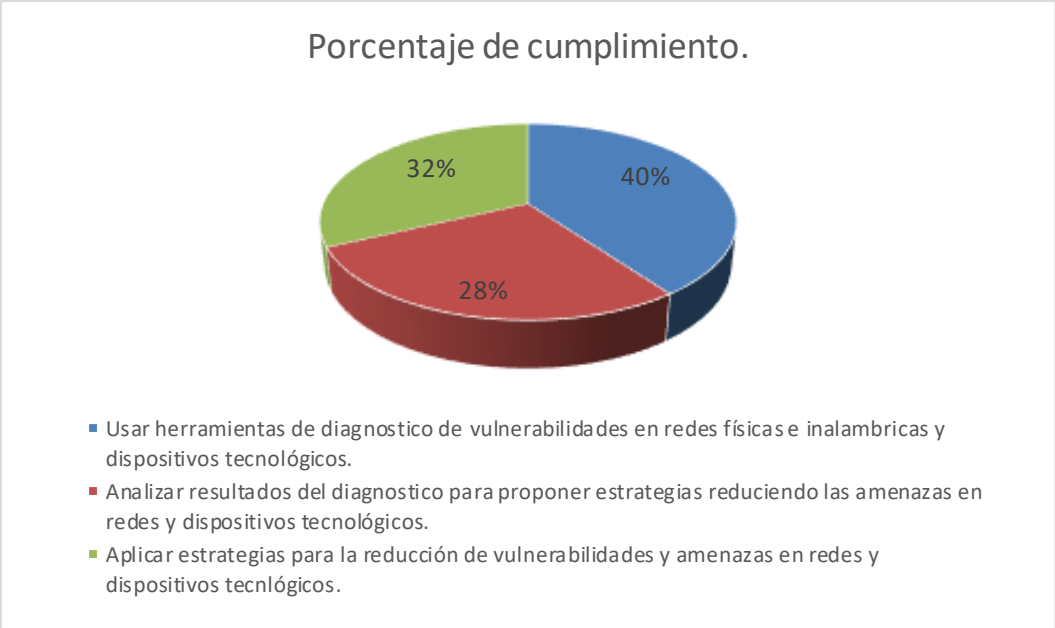

Figura 19. Cumplimiento uso de herramientas.
Fuente propia.

5.3.1. Apoyo en la realización del nuevo canal de internet y un análisis de vulnerabilidades a sistemas de la alcaldía de Fusagasugá.

Como resultado del uso de herramientas de ciberseguridad para poder identificar algunas vulnerabilidades en la oficina TIC de la alcaldía de Fusagasugá guiados por el líder encargado de desarrollar esta actividad se obtiene que a través del comando Ping -t que es un ping sostenido, la cual por medio de este comando podemos obtener información del servidor o de la red que deseemos analizar y ver sus vulnerabilidades, conectándonos al servidor. Tomando el comando -A que permite verificar que puertos tenemos abiertos, su versión, sus aplicativos, en este caso se analizó que el puerto 80, 135,139,145 que no deberían estar abiertos ya que son del directorio activo del servidor 07, tienen un acceso que en normalidad no debería estar en esta condición, estos comandos realizados por medio de la herramienta NMAP establece esta vulnerabilidad donde se puede generar perdida de datos sensibles que afectan el funcionamiento de la oficina TIC. Generando comunicación con el ingeniero a cargo de estos puertos para su respectiva corrección.

5.3.2. A través de la Herramienta de software libre ZABBIX, que sirve la monitorización de código abierto para redes y aplicaciones. Ofrece monitorización en tiempo real de miles de métricas recogidas de servidores, equipos virtuales, dispositivos de red y aplicaciones web. En este caso para monitorizar y registrar el estado de varios servicios de los servidores de la alcaldía de Fusagasugá, se pudo obtener un listado donde se identifica el rol del personal inscrito en la Oficina TIC, corrigiendo así el rol de permisos.

Por medio de la herramienta ZABBIX y ejecutando el siguiente comando Get-ADGroupMember -Identity "Admins. del dominio" Export-Csv -Path C:\scriptresoult\usuariosadmindomain.csv, se pudo obtener el listado de usuarios administradores de dominio a eliminar solicitado por el oficial de seguridad.

5.3.3. Instalación de antivirus licenciado ENDPOINT SECURITY, a los equipos de dominio de la alcaldía de Fusagasugá.

De acuerdo con lo solicitado por el oficial de seguridad se obtuvieron 241 licencias de antivirus ENDPOINT SECURITY, este antivirus implementa análisis, detección, evaluación y actuar sobre las vulnerabilidades en la red mediante el sistema de inspección, de acuerdo con eso se realizó la mayor parte de instalación de este antivirus para su uso, en la Tabla 5 vemos el porcentaje exacto de los equipos beneficiados.

NO. DE EQUIPOS	**241**
EQUIPOS EN INVENTARIO	**300**
TOTAL INSTALACION REALIZADA	**198**
PORCENTAJE= $\frac{\text{Equipos en inventario X 100}}{\text{NO. DE EQUIPOS}}$	**82.5 %**

Tabla 5. Porcentaje de antivirus instalados.
Fuente: Oficina TIC Alcaldía de Fusagasugá.

Consecuente al uso de herramientas que permitían un identificar vulnerabilidades y reducir amenazas en las redes y dispositivos de las dependencias de la Alcaldía de Fusagasugá se hallan herramientas altamente eficaces que encaminaban una mejora continua del plan de trabajo, obteniendo así el 25,51 % de cumplimiento en los objetivos totales.

Acorde a los objetivos planteados durante el proceso de la pasantía de la Alcaldía de Fusagasugá y siguiendo cada una de las actividades determinadas en el cronograma podemos determinar que se realizó un 81.6 % de la actividades propuestas durante el desarrollo de la pasantía en la alcaldía de Fusagasugá y dando seguimiento al modelos de seguridad y privacidad de la información (MSPI) impuesto por el Ministerio de las tecnologías de la información y las comunicaciones (MINTIC), donde su objetivo principal y conforme al decreto 1078 de 2015, es promover el uso e implementación de mejores prácticas de la información en las entidades públicas del estado colombiano, siguiendo los lineamientos de clasificación tales como la confidencialidad, integridad y disponibilidad de la información.

Todo esto haciendo referencia al marco de la transformación digital para el estado que su único objetivo es buscar el mejoramiento de relación entre el estado y ciudadano a toda la información pública dando una interacción más sencilla y efectiva con las entidades del estado.

Conclusiones

- La aplicación del Modelo de seguridad y privacidad de la información (MSPI) como estrategia integral permitió la identificación de activos de cada una de las dependencias de la Alcaldía de Fusagasugá, logrando una comprensión más profunda de los activos críticos, las amenazas potenciales y las vulnerabilidades existentes, lo que a su vez permitió una toma de decisiones más informada y proactiva en términos de seguridad y protección.

- El fomento de una cultura organizativa del principio de Disponibilidad de la información a través de campañas y capacitaciones técnicas en relación con los delitos informáticos dentro de la Alcaldía de Fusagasugá permitió fortalecer la seguridad cibernética y garantizar la integridad y accesibilidad de los activos de información.

- La implementación de herramientas de ciberseguridad para identificar vulnerabilidades y reducir amenazas en las redes y dispositivos tecnológicos en la dependencia de TIC de la Alcaldía de Fusagasugá permitió fortalecer la seguridad de la información y garantizar un entorno tecnológico más seguro para los funcionarios.

Referencias

Advisera. (2022). *advisera.com*. Obtenido de https://advisera.com/27001academy/es/que-es-iso-27001/

Berbeo, G. A. (2017). *Informe Final de Pasantia Galeria neebex*. Obtenido de chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://repository.udistrital.edu.co/bitstream/handle/11349/7039/BerbeoGarciaAriadna2017.pdf?sequence=1&isAllowed=y

Diaz, O. M., & Sanabria, R. P. (2020). Desafíos nacionales frente a la ciberseguridad en el escenario global: un análisis para Colombia. Obtenido de chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/http://www.scielo.org.co/pdf/crim/v62n2/1794-3108-crim-62-02-199.pdf

DocuSign, C. (24 de Agosto de 2021). *DocuSign*. Obtenido de https://www.docusign.mx/blog/seguridad-de-la-informacion

Etecé, E. (18 de Febrero de 2023). *Concepto*. Obtenido de https://concepto.de/marco-de-referencia/

IBM. (2020). *¿Qué es la ciberseguridad?* . Obtenido de https://www.ibm.com/mx-es/topics/cybersecurity

Ministerio de Asuntos Economicos y Transformacion Digital. (2021). Obtenido de chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://www.incibe.es/sites/default/files/contenidos/guias/doc/guia_glosario_ciberseguridad_2021.pdf

MINTIC . (Julio de 2020). Seguridad y Privacidad de la información. . Colombia.

MINTIC . (19 de Oct de 2021). MATRIZ DE INVENTARIO Y CLASIFICACIÓN DE ACTIVOS DE INFORMACIÓN.

MINTIC. (15 de Mar de 2016). *MINTIC.* Obtenido de chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://www.mintic.gov.co/gestionti/615/articles-5482_G5_Gestion_Clasificacion.pdf

Peña, B. P. (2021). *MARCO DE GOBIERNO Y GESTIÓN DE CIBERSEGURIDAD PARA CIUDADES INTELIGENTES EN EL CONTEXTO COLOMBIANO.* Barranquilla, Colombia. .

Rea, G. Á. (2020). *Madurez en la Identificación y Evaluación de Riegos de Ciberseguridad.* Madrid, España.

Apéndice 1: Glosario.

Activo de información:
Es cualquier información o sistema relacionado con el tratamiento de la misma que tenga valor para la organización, pueden ser procesos de negocio, datos, aplicaciones, equipos informáticos, personal, soportes de información, redes, equipamiento auxiliar o instalaciones.

Alta disponibilidad:
Característica de un sistema o servicio que permite reducir al mínimo el tiempo de indisponibilidad en caso de fallo o incidente.

Amenaza:
Circunstancia desfavorable que puede ocurrir y que cuando sucede tiene consecuencias negativas sobre los activos provocando su indisponibilidad.

Antivirus:
Software de protección para evitar que ejecutemos algún tipo de software malicioso en nuestro equipo que infecte al equipo.

Ciberataque:
Intento deliberado de un ciberdelincuente de obtener acceso a un sistema informático sin autorización sirviéndose de diferentes técnicas y vulnerabilidades para la realización de actividades con fines maliciosos, como el robo de información, extorsión del propietario o simplemente daños al sistema.

Confidencialidad:
Confidencialidad es la propiedad de la información, por la que se garantiza que está accesible únicamente a personal autorizado a acceder a dicha información.

Criticidad:
Atributo que mide el riesgo que provoca un comportamiento erróneo o negligente respecto a las condiciones normales de funcionamiento al que está sometido un proceso, sistema o equipo. A mayor nivel de criticidad, mayor gravedad de los hechos ocurridos.

Dirección IP:
Las direcciones IP (del acrónimo inglés IP para Internet Protocol) son un número único e irrepetible con el cual se identifica a todo sistema conectado a una red.

Escaneo de puertos:
Técnica intrusiva en la que los atacantes buscan de manera activa los puertos y servicios que pudieran estar a la escucha, en busca de recopilar información de la víctima con la finalidad de evaluar vulnerabilidades que explotar en la fase de ataque.

Fuga de datos:
La fuga de datos o fuga de información es la pérdida de la confidencialidad de la información privada de una persona o empresa.

Incidente de seguridad:
Cualquier suceso que afecte a la confidencialidad, integridad o disponibilidad de los activos de información de la empresa.

Metadatos:
Los metadatos son el conjunto de datos relacionados con un documento y que recogen información fundamentalmente descriptiva del mismo, así como información de administración y gestión. Los metadatos es una información que enriquece el documento al que está asociado.

Ping:
Utilidad de diagnóstico que mide el estado, velocidad y calidad de una red de comunicaciones mediante el envío de paquetes de solicitud y de respuesta a uno o varios dispositivos.

Vulnerabilidad:
Debilidad o fallo de un sistema que puede ser aprovechado con fines maliciosos (normalmente mediante un programa que se denomina exploit). Cuando se descubre el desarrollador del software o hardware lo solucionará publicando una actualización de seguridad del producto. Sinónimo: Agujero de seguridad

Apéndice 2: Seguridad y Privacidad de la Información.

Apéndice 3: Cronograma de actividades

		Semanas																														
Objetivos	Actividades	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32
1. Apoyo en la implementación del Modelo de la Seguridad y Privacidad de la Información (MSPI) estipulado por el Mintic a cada una de las dependencias de la Alcaldía de Fusagasugá.	Reconocimiento del MSPI (Modelo Seguridad y privacidad de la informacion.)	x	x	x	x	x	x																										
	Apoyar con cada una de las dependencias de la Alcaldia De Fusagasuga sobre el MSPI.			x	x	x	x	x	x	x	x	x																					
	Implemetar plan de capacitaciones al interior de la entidad.				x	x	x																										
	Informes de actividad				x					x					x					x					x				x				x
2. Aplicar el modelo MSPI para el seguimiento y clasificación de riesgos de los activos de cada una de las dependencias de la Alcaldía de Fusagasugá.	Dar capacitacion del diligenciamiento de la matriz de riesgos a cada una de las							x	x		x	x																				
	Seguimiento a los informes de perdida de datos y riesgos de seguridad de la información.							x	x	x	x						x	x	x	x						x	x	x	x				
	Implementar politicas de seguridad frente a riesgos y delitos informatico									x									x	x	x	x											
	Informes de actividad				x					x					x					x					x				x				x
3. Fomentar el principio de Disponibilidad de la información a través de campañas, capacitaciones tecnicas, frente a los delitos informáticos dentro de la Alcaldía de Fusagasugá.	Aplicar procesos para garantizar el nivel de disponibilidad establecido por la oficina de						x	x	x		x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x				
	Hacer mantenimiento de equipos, redes de la entidad, evitando perdidas de la informacion.									x	x	x	x						x	x	x	x					x	x	x	x			
	Identificar y proponer mejoras en la infraestructura y servicios TI con el objetivo de aumentar los niveles de disponibilidad.									x											x	x	x	x	x								
	Informes de actividad				x					x					x					x					x				x				x
4. Hacer uso de herramientas de ciberseguridad para identificar vulnerabilidades y reducir las amenazas en las redes y dispositivos tecnológicos para mejorar la seguridad a los funcionarios de dependencia TIC de la Alcaldía de Fusagasugá.	Usar herramientas de diagnostico de vulnerabilidades en redes fisicas e inalambricas y dispositivos tecnológicos												x	x	x	x																	
	Analizar resultados del diagnostico para proponer estrategias reduciendo las amenazas en redes y dispositivos tecnológicos.																		x	x	x	x											
	Aplicar estrategias para la reducción de vulnerabilidades y amenazas en redes y dispositivos tecnlógicos.																														x	x	x
	Realizacion de documento pasantia.		x	x	x	x	x	x	x		x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x