Tabla de contenido

1. OBJETIVOS

1.1. Objetivo General

Desarrollar e implementar un Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información para la Alcaldía Municipal de Fusagasugá, que promueva la mejora continua en la gestión de la seguridad de la información y la protección de datos personales.

1.2. Objetivos Específicos

- Identificar y analizar los riesgos de seguridad y privacidad de la información en la Alcaldía Municipal de Fusagasugá, mediante la aplicación de una metodología de evaluación de riesgos alineada con el marco normativo vigente, incluyendo el Decreto 767 de 2022 y la Resolución 500 de 2021.
- Diseñar e implementar controles de seguridad de la información basados en los resultados del análisis de riesgos, asegurando la protección de los activos de información y el cumplimiento de la normativa aplicable, como la ISO/IEC 27001:2022, Ley 1712 de 2014 y la Ley 1581 de 2012 sobre protección de datos personales.
- Capacitar y sensibilizar al personal de la Alcaldía en prácticas de seguridad de la información y privacidad de datos, a través de programas de formación continua que promuevan una cultura organizacional de seguridad y minimicen los riesgos asociados al factor humano.
- Establecer un sistema de monitoreo y mejora continua del Plan de Tratamiento de Riesgos, mediante la definición de indicadores clave de desempeño (KPIs), auditorías internas y revisiones periódicas para evaluar la efectividad de los controles implementados y realizar ajustes oportunos.

2. DEFINICIONES

- **Acceso a la Información Pública:** Derecho fundamental consistente en la facultad que tienen todas las personas de conocer sobre la existencia y acceso a la información pública en posesión o bajo control de sujetos obligados. (Ley 1712 de 2014, art 4).
- **Activo de información:** En relación con la seguridad de la información, se refiere a cualquier información o elemento relacionado con el tratamiento de ésta (sistemas, soportes, edificios, personas, etc.) que tenga valor para la organización. (ISO/IEC 27000).
- **Activos de Información y recursos:** se refiere a elementos de hardware y de software de procesamiento, almacenamiento y comunicaciones, bases de datos y procesos, procedimientos y recursos humanos asociados con el manejo de los datos y la información misional, operativa y administrativa de cada entidad, órgano u organismo. (CONPES 3854 de 2016).
- **Archivo:** Conjunto de documentos, sea cual fuere su fecha, forma y soporte material, acumulados en un proceso natural por una persona o entidad pública o privada, en el transcurso

de su gestión, conservados respetando aquel orden para servir como testimonio e información a la persona o institución que los produce y a los ciudadanos, o como fuentes de la historia. También se puede entender como la institución que está al servicio de la gestión administrativa, la información, la investigación y la cultura. (Ley 594 de 2000, art 3).

- **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 dicho riesgo. (ISO/IEC 27000).
- **Auditoría:** Proceso sistemático, independiente y documentado para obtener evidencias de auditoría y obviamente para determinar el grado en el que se cumplen los criterios de auditoría. (ISO/IEC 27000).
- **Autorización:** Consentimiento previo, expreso e informado del Titular para llevar a cabo el Tratamiento de datos personales (Ley 1581 de 2012, art 3).
- Bases de Datos Personales: Conjunto organizado de datos personales que sea objeto de Tratamiento (Ley 1581 de 2012, art 3).
- **Ciberseguridad:** Protección de activos de información, mediante el tratamiento de las amenazas que ponen en riesgo la información que se procesa, almacena y transporta mediante los sistemas de información que se encuentran interconectados.
- **CERT:** (Computer Emergency Response Team) Equipo de Respuesta a Emergencias cibernéticas, por su sigla en inglés. Es el equipo que dispone de la capacidad centralizada para la coordinación de gestión de incidentes de seguridad digital.
- **Ciberespacio:** Red interdependiente de infraestructuras de tecnología de la información que incluye Internet, redes de telecomunicaciones, sistemas informáticos, procesadores y controladores integrados en industrias. (art. 2.2.21.1.1.3. del, Decreto 1078 de 2015).
- **Ciberdefensa:** Capacidad del Estado para prevenir y contrarrestar toda amenaza o incidente de naturaleza cibernética que afecte la sociedad, la soberanía nacional, la independencia, la integridad territorial, el orden constitucional y los intereses nacionales. Implica el empleo de las capacidades militares ante amenazas cibernéticas, ataques cibernéticos o ante actos hostiles de naturaleza cibernética.
- **CSIRT:** (Computer Security Incident & Response Team) Equipo de Respuesta a Incidentes de Seguridad Cibernética, por su sigla en inglés. Es el equipo que provee las capacidades de gestión de incidentes a una organización/sector en especial. Esta capacidad permitir minimizar y controlar el daño resultante de incidentes, proveyendo la respuesta, contención y recuperación efectiva, así como trabajar en pro de prevenir la ocurrencia de futuros incidentes.
- **CSIRT sectorial:** Son los equipos de respuesta a incidentes de cada uno de los sectores, para el adecuado desarrollo de sus actividades económicas y sociales, a partir del uso de las tecnologías de la información y las comunicaciones.
- **CSIRT sectorial crítico:** Son los equipos de respuesta a incidentes sectoriales de cada uno de los sectores identificados como críticos.

- **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.
- **Datos Abiertos:** Son todos aquellos datos primarios o sin procesar, que se encuentran en formatos estándar e interoperables que facilitan su acceso y reutilización, los cuales están bajo la custodia de las entidades públicas o privadas que cumplen con funciones públicas y que son puestos a disposición de cualquier ciudadano, de forma libre y sin restricciones, con el fin de que terceros puedan reutilizarlos y crear servicios derivados de los mismos Ley 1712 de 2014.
- **Datos Personales:** Cualquier información vinculada o que pueda asociarse a una o varias personas naturales determinadas o determinables. (Ley 1581 de 2012, art 3)
- **Datos Personales Públicos:** Es el dato que no sea semiprivado, privado o sensible. Son considerados datos públicos, entre otros, los datos relativos al estado civil de las personas, a su profesión u oficio y a su calidad de comerciante o de servidor público. Por su naturaleza, los datos públicos pueden estar contenidos, entre otros, en registros públicos, documentos públicos, gacetas y boletines oficiales y sentencias judiciales debidamente ejecutoriadas que no estén sometidas a reserva. (Decreto 1377 de 2013, art 3)
- **Datos Personales Privados:** Es el dato que por su naturaleza íntima o reservada sólo es relevante para el titular. (Ley 1581 de 2012, art 3 literal h)
- **Datos Personales Mixtos:** Para efectos de este documento es la información que contiene datos personales públicos junto con datos privados o sensibles.
- **Datos Personales Sensibles:** Se entiende por datos sensibles aquellos que afectan la intimidad del Titular o cuyo uso indebido puede generar su discriminación, tales como aquellos que revelen el origen racial o étnico, la orientación política, las convicciones religiosas o filosóficas, la pertenencia a sindicatos, organizaciones sociales, de derechos humanos o que promueva intereses de cualquier partido político o que garanticen los derechos y garantías de partidos políticos de oposición, así como los datos relativos a la salud, a la vida sexual, y los datos biométricos. (Decreto 1377 de 2013, art 3)
- **Derecho a la Intimidad:** Derecho fundamental cuyo núcleo esencial lo constituye la existencia y goce de una órbita reservada en cada persona, exenta de la intervención del poder del Estado o de las intromisiones arbitrarias de la sociedad, que le permite a dicho individuo el pleno desarrollo de su vida personal, espiritual y cultural (Jurisprudencia Corte Constitucional).
- **Encargado del Tratamiento de Datos:** Persona natural o jurídica, pública o privada, que por sí misma o en asocio con otros, realice el Tratamiento de datos personales por cuenta del responsable del Tratamiento. (Ley 1581 de 2012, art 3)
- **Evento:** Un evento es cualquier suceso observable en un sistema o red, como un usuario que se conecta a un recurso compartido de archivos, un usuario que envía un archivo electrónico o un firewall que bloquea un intento de conexión, entre otros. Igualmente, los eventos adversos,

son aquellos que tienen consecuencias negativas, como fallos en un sistema, usos no autorizados de privilegios en un sistema, acceso no autorizados y ejecución de malware.

- **Defacement:** Ataque sobre un servidor web como consecuencia del cual se cambia su apariencia.
- **DoS / DDoS (Denial of Service / Distributed Denial of Service:** Se entiende como denegación de servicio, en términos de seguridad informática, a un conjunto de técnicas que tienen por objetivo dejar un servidor inoperativo. Mediante este tipo de ataques se busca sobrecargar un servidor y de esta forma no permitir que sus legítimos usuarios puedan utilizar los servicios por prestados por él. El ataque consiste en saturar con peticiones de servicio al servidor, hasta que éste no puede atenderlas, provocando su colapso.
- **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).
- **Gobernanza de la seguridad digital para Colombia:** Corresponde al conjunto de interacciones y enfoques entre las múltiples partes interesadas para identificar, enmarcar, proponer, y coordinar respuestas proactivas y reactivas a posibles amenazas a la confidencialidad, integridad o disponibilidad de los servicios tecnológicos, sistemas de información, infraestructura tecnológica, redes e información que en conjunto constituyen el entorno digital.
- **Incidente:** Un incidente es una violación o amenaza inminente a las políticas de seguridad digital, políticas de uso aceptable y o prácticas de seguridad básicas.
- **Información Pública Clasificada:** Es la que está en poder o custodia de un sujeto obligado pertenece al ámbito propio, particular y privado o semiprivado de una persona natural o jurídica, por lo que su acceso podrá negarse o exceptuarse si se trata de las circunstancias legítimas y necesarias y los derechos particulares o privados consagrados en el artículo 18 de la Ley 1712 de 2014. (Ley 1712 de 2014, art 6)
- **Información Pública Reservada:** Es aquella información que estando en poder o custodia de un sujeto obligado en su calidad de tal, es exceptuada de acceso a la ciudadanía por daño a intereses públicos y bajo cumplimiento de la totalidad de los requisitos consagrados en el artículo 19 de la Ley 1712 de 2014. (Ley 1712 de 2014, art 6).
- **Ingeniería social:** Son técnicas basadas en engaños que se emplean para dirigir la conducta de una persona u obtener información sensible. El afectado es inducido a actuar de determinada forma (pulsar en enlaces, introducir contraseñas, visitar páginas, etc.) convencido de que está haciendo lo correcto cuando realmente está siendo engañado por el ingeniero social.
- **Inyección de ficheros remota:** Estado de vulnerabilidad que se crea por métodos de codificación poco seguros, y que tiene como resultado una validación de entradas inapropiada, que permite a los atacantes transferir código malicioso al sistema subyacente a través de una aplicación web.
- **Inyección SQL:** Tipo de ataque a sitios web basados en bases de datos. Una persona malintencionada ejecuta comandos SQL no autorizados aprovechando códigos inseguros de un

sistema conectado a Internet. Los ataques de inyección SQL se utilizan para robar información normalmente no disponible de una base de datos o para acceder a las computadoras host de una organización mediante la computadora que funciona como servidor de la base de datos.

- **Incidente de seguridad digital - Ciberincidente:** Ocurrencia de una situación que pone en peligro la confidencialidad, integridad o disponibilidad de un sistema de información o la información que el sistema procesa, almacena o transmite; o que constituye una violación a las políticas de seguridad, procedimientos de seguridad o políticas de uso aceptable.
- **Infraestructura crítica cibernética:** Sistemas y activos, físicos o virtuales, soportados por Tecnologías de la Información y las Comunicaciones, cuya afectación significativa tendría un impacto grave en el bienestar social o económico de los ciudadanos, o en el funcionamiento efectivo del gobierno o la economía.
- **Ley de Habeas Data:** Se refiere a la Ley Estatutaria 1266 de 2008.
- **Ley de Transparencia y Acceso a la Información Pública:** Se refiere a la Ley Estatutaria 1712 de 2014.
- **Mecanismos de protección de datos personales:** Lo constituyen las distintas alternativas con que cuentan las entidades destinatarias para ofrecer protección a los datos personales de los titulares tales como acceso controlado, anonimización o cifrado.
- **Modelo de Gobernanza de Seguridad digital:** Es el esquema de trabajo compuesto por un conjunto de políticas de operación, principios, normas, reglas, procedimientos de toma de decisiones y programas compartidos por las múltiples partes interesadas de la seguridad digital del país, con el fin de fortalecer las capacidades para la gestión de riesgos e incidentes de seguridad digital y para la respuesta proactiva y reactiva a posibles amenazas a la confidencialidad, integridad o disponibilidad de los servicios tecnológicos, sistemas de información, infraestructura tecnológica y las redes e información que, en conjunto, constituyen el entorno digital en el país.
- **Múltiples partes interesadas:** Corresponde al conjunto de actores que dependen del entorno digital para todas o algunas de sus actividades, económicas y sociales. Comprende a las autoridades, las organizaciones privadas, los operadores o propietarios de las infraestructuras críticas cibernéticas nacionales, los prestadores de servicios esenciales, la academia y la sociedad civil.
- **Partes interesadas (Stakeholder):** Persona u organización que puede afectar a, ser afectada por o percibirse a sí misma como afectada por una decisión o actividad.
- **Pharming:** Ataque informático que consiste en modificar o sustituir el archivo del servidor de nombres de dominio cambiando la dirección IP legítima de una entidad (comúnmente una entidad bancaria) de manera que en el momento en el que el usuario escribe el nombre de dominio de la entidad en la barra de direcciones, el navegador redirigirá automáticamente al usuario a otra dirección IP (Internet Protocol) donde se aloja una web(página) falsa que suplantará la identidad legítima de la entidad, obteniéndose de forma ilícita las claves de acceso de los clientes la entidad.

- **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 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).
- **Plan de Respuesta a Ciberincidentes:** Conjunto predeterminado y ordenado de instrucciones o procedimientos para detectar, analizar, contener, erradicar y recuperar para minimizar las consecuencias de un ciberincidente.
- **Ransomware:** Código malicioso para secuestrar datos, una forma de explotación en la cual la atacante cifra los datos de la víctima y exige un pago por la clave de descifrado, se propaga a través de archivos adjuntos de correo electrónico, programas infectados y sitios web comprometidos, secuestrando computadores y servidores (imposibilidad de usarlo) o cifrando los archivos, con la promesa de liberarlo tras el pago de una cantidad de dinero por el rescate.
- **RAT- Remote Acces Tool:** Pieza de software que permite a un "operador" controlar a distancia un sistema como si se tuviera acceso físico al mismo. Aunque tiene usos perfectamente legales, el software RAT se asocia habitualmente con ciberataques o actividades criminales o dañinas. En estos casos, el malware suele instalarse sin el conocimiento de la víctima, ocultando frecuentemente un troyano.
- **Registro Nacional de Bases de Datos:** Directorio público de las bases de datos sujetas a Tratamiento que operan en el país. (Ley 1581 de 2012, art 25)
- **Responsabilidad Demostrada:** Conducta desplegada por los responsables o Encargados del tratamiento de datos personales bajo la cual a petición de la Superintendencia de Industria y Comercio deben estar en capacidad de demostrarle a dicho organismo de control que han implementado medidas apropiadas y efectivas para cumplir lo establecido en la Ley 1581 de 2012 y sus normas reglamentarias.
- **Responsable del Tratamiento de Datos:** Persona natural o jurídica, pública o privada, que por sí misma o en asocio con otros, decida sobre la base de datos y/o el Tratamiento de los datos. (Ley 1581 de 2012, art. 3).
- **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).
- **Riesgo de seguridad digital:** Es la combinación de amenazas y/o vulnerabilidades que se pueden materializar en el curso de cualquier actividad en el entorno digital y que puede afectar el logro de los objetivos económicos o sociales al alterar la confidencialidad, integridad y disponibilidad.
- **Rootkit:** T Es una herramienta que sirve para ocultar actividades ilegítimas en un sistema. Una vez que ha sido instalado, permite al atacante actuar con el nivel de privilegios del administrador del equipo.

- **Scanner (Scanning) Escáner de vulnerabilidades:** Programa que analiza un sistema buscando vulnerabilidades. Utiliza una base de datos de defectos conocidos y determina si el sistema bajo examen es vulnerable o no.
- **Spam (correo basura):** Correo electrónico no deseado que se envía aleatoriamente en procesos por lotes. Es extremadamente eficiente y barata forma de comercializar cualquier producto. La mayoría de los usuarios que están expuestos a este correo basura que se confirma en encuestas que muestran que más del 50% de todos los e-mails son correos basura. No es una amenaza directa, pero la cantidad de e-mails generados y el tiempo que lleva a las empresas y particulares relacionarlo y eliminarlo, representa un elemento molesto para los usuarios de Internet.
- **Spear Phising:** Phishing dirigido de forma que se maximiza la probabilidad de que el sujeto objeto del ataque pique el anzuelo (suelen basarse en un trabajo previo de ingeniera social sobre la victima).
- **Spyware "spy software":** Tipo de software malicioso que al instalarse intercepta o toma control parcial de la computadora del usuario sin el consentimiento de este último.
- **Suplantación (Spoofing):** Técnica basada en la creación de tramas TCP/IP utilizando una dirección IP falseada; desde su equipo, un atacante simula la identidad de otra máquina de la red (que previamente ha obtenido por diversos métodos) para conseguir acceso a recursos de un tercer sistema que ha establecido algún tipo de confianza basada en el nombre o la dirección IP del anfitrión suplantado.
- **Seguridad de la información:** Preservación de la confidencialidad, integridad, y disponibilidad de la información en cualquier medio: impreso o digital. (ISO/IEC 27000).
- **Seguridad digital:** Preservación de la confidencialidad, integridad, y disponibilidad de la información que se encuentra en medios digitales.
- **Servicio esencial:** En el marco de la gestión de riesgos de la seguridad digital es aquel servicio necesario para el mantenimiento de las actividades sociales y económicas del país, que dependen del uso de tecnologías de la información y las comunicaciones, y un incidente en su infraestructura o servicio podría generar un daño significativo que afecte la prestación de dicho servicio y la consecuente parálisis de las actividades.
- **Titulares de la información:** Personas naturales cuyos datos personales sean objeto de Tratamiento. (Ley 1581 de 2012, art 3)
- **Tratamiento de Datos Personales:** Cualquier operación o conjunto de operaciones sobre datos personales, tales como la recolección, almacenamiento, uso, circulación o supresión. (Ley 1581 de 2012, art 3).
- **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).

- **Troyano:** Programa que aparentemente, o realmente, ejecuta una función útil, pero oculta un subprograma dañino que abusa de los privilegios concedidos para la ejecución del citado programa.
- **Virus:** Programa que está diseñado para copiarse a sí mismo con la intención de infectar otros programas o ficheros.

3. ALCANCE

El presente plan está dirigido a la Alcaldía Municipal de Fusagasugá, con el propósito de fortalecer la gestión de la seguridad de la información y la protección de datos personales. Este plan abarca la identificación y análisis de riesgos asociados a los activos de información, garantizando su tratamiento conforme a la normativa vigente, como el Decreto 767 de 2022, la Resolución 500 de 2021, la ISO/IEC 27001:2022, y la Ley 1581 de 2012 sobre protección de datos personales.

Ademas, incluye el diseño e implementación de controles de seguridad, enfocados en mitigar riesgos y proteger la información sensible de la Alcaldía. También contempla la capacitación del personal, promoviendo prácticas seguras que reduzcan vulnerabilidades relacionadas con el factor humano.

Para asegurar la efectividad del plan, se implementará un sistema de monitoreo y mejora continua, con indicadores de desempeño, auditorías o revisiones internas y revisiones periódicas, permitiendo realizar ajustes necesarios según la evolución de los riesgos y el entorno organizacional.

Este plan aplica a todos los procesos, sistemas, activos de información y colaboradores de la Alcaldía que intervienen en el manejo de los datos, asegurando un enfoque integral para la protección de la información. Por último, las responsabilidades del plan recaen en todos los funcionarios de la Alcaldía de Fusagasugá (planta y contratistas), quienes son los encargados de crear, recolectar, procesar, analizar datos para entidad.

4. DESARROLLO

La Alcaldía de Fusagasugá ha desarrollado un Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información para proteger los datos y documentos que gestiona, asegurando su confidencialidad, integridad y disponibilidad. Este plan permite identificar los riesgos que podrían afectar la información, implementar medidas preventivas para reducir su impacto y establecer planes de contingencia para responder ante posibles incidentes.

Dada la naturaleza sensible de la información que maneja, es fundamental contar con un enfoque estructurado que garantice su protección y minimice las amenazas que puedan comprometer la confianza de la ciudadanía. Para ello, el plan se basa en los dominios de la norma ISO 27001, alineándose con el Modelo de Seguridad y Privacidad de la Información (MSPI), lo que permite cumplir con estándares internacionales y regulaciones locales, como el Decreto 767 de 2022 y la Resolución 500 de 2021.

El proceso de implementación del plan involucra la participación de todas las áreas de la Alcaldía,

fomentando una cultura de seguridad a través de la capacitación constante del personal y el uso de controles tecnológicos y operativos que permitan una gestión eficiente de los riesgos.

Este plan busca prevenir incidentes y establecer una dinámica de mejora continua, evaluando constantemente la efectividad de las acciones implementadas para garantizar un entorno seguro y confiable en la gestión de la información.

.

4.1. PROCESO PARA EL TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

Para la evaluación de riesgos en seguridad de la información un insumo vital es la clasificación de activos de información ya que una buena práctica es realizar gestión de riesgos a los activos de información que se consideren con nivel de clasificación ALTA dependiendo de los criterios de clasificación; es decir que en los criterios de Confidencialidad, Integridad y Disponibilidad tengan la siguiente calificación:

CONFIDENCIALIDAD	INTEGRIDAD	DISPONIBILIDAD
INFORMACIÓN PUBLICA RESERVADA	ALTA (A)	ALTA (1)
INFORMACIÓN PUBLICA CLASIFICADA	MEDIA (M)	MEDIA (2)
INFORMACIÓN PÚBLICA	BAJA (B)	BAJA (3)
NO CLASIFICADA	NO CLASIFICADA	NO CLASIFICADA

Ilustración 1: Criterios de Clasificación

ALTA	Activos de información en los cuales la clasificación de la información en dos (2) o todas las propiedades (confidencialidad, integridad, y disponibilidad) es alta.
MEDIA	Activos de información en los cuales la clasificación de la información es alta en una (1) de sus propiedades o al menos una de ellas es de nivel medio.
BAJA	Activos de información en los cuales la clasificación de la información en todos sus niveles es baja.

Ilustración 2: Niveles de Clasificación

El proceso de gestión del riesgo consta de cinco etapas principales: identificación de riesgos, evaluación de riesgos, tratamiento de riesgos, implementación de controles y monitoreo y revisión. Al llevar a cabo este proceso de manera efectiva, la alcaldía puede identificar y minimizar los riesgos asociados a la seguridad de la información, continuación se muestra de forma gráfica el proceso de gestión del riesgo de la seguridad de la información.

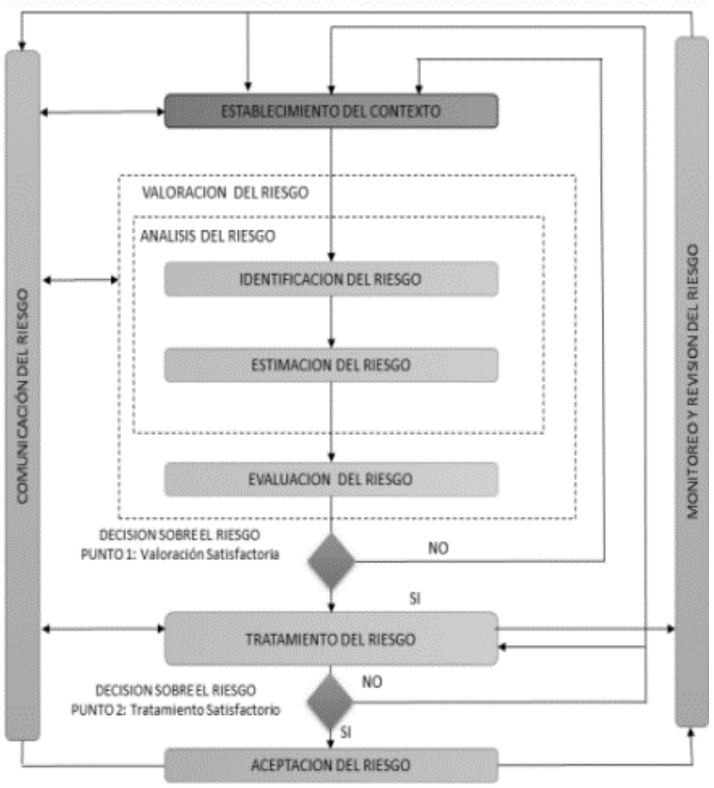

Ilustración 3: Proceso de gestión del riesgo de la seguridad de la información (Tomado de la NTC-ISO/IEC 27005)

La siguiente grafica resume las actividades de gestión del riesgo en la seguridad de la información que son pertinentes:

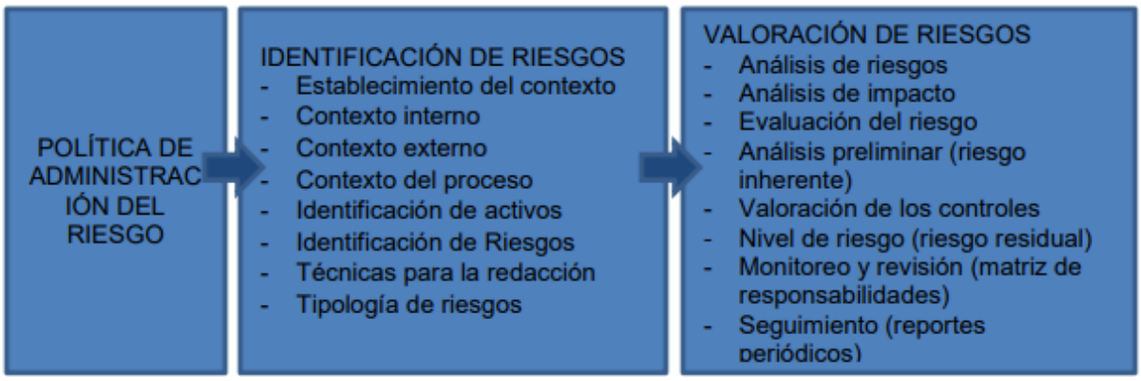

Ilustración 4: Actividades Gestión de Riesgos

La Alcaldía Municipal de Fusagasugá implementa diversas estrategias para garantizar la protección de la información que gestiona, reconociendo su importancia en la prestación de servicios a la comunidad. Por ello, sigue guías y metodologías especializadas que permiten una gestión de riesgos eficiente y alineada con las mejores prácticas internacionales y normativas nacionales.

El marco rector de esta gestión es la **Política de Administración del Riesgo PO-DE-001**, un documento que define lineamientos claros para identificar, analizar, evaluar y mitigar riesgos de seguridad y privacidad de la información.

Esta política está alineada con los estándares establecidos por el Departamento Administrativo de la Función Pública, asegurando su conformidad con el Modelo Integrado de Planeación y Gestión (MIPG) y la normativa vigente en Colombia, como el Decreto 767 de 2022 y la Resolución 500 de 2021.

4.2. METODOLOGÍA PARA LA GESTIÓN DEL RIESGO DE SEGURIDAD Y PRIVACIDAD

Para lograr una protección efectiva de los activos de información, la Alcaldía ha adoptado una metodología estructurada en etapas, que permite un enfoque integral y sistemático para la gestión de riesgos. Esta metodología abarca los siguientes dos grandes grupos de actividades la gestión de activos de información y la gestión de riesgos

4.2.1 Identificación de los Activos de Seguridad de la Información

La **primera línea de defensa** tiene la responsabilidad de identificar los activos de seguridad de la información en cada proceso de la entidad. Estos activos comprenden todos los elementos utilizados para el funcionamiento en el entorno digital, tales como:

- Aplicaciones
- Servicios web
- Redes
- Información física o digital
- Tecnologías de información (TI)
- Tecnologías de operación (TO)

Para llevar a cabo una correcta identificación de los activos de seguridad de la información, es necesario seguir los siguientes pasos:

4.2.2 Listar los activos por cada proceso:

Se deben identificar y documentar los activos que intervienen en cada uno de los procesos de la entidad.

- **Identificar el dueño de cada activo:**
  Se debe asignar la responsabilidad de cada activo a un propietario, quien será el encargado de su gestión y protección.
- **Clasificar los activos:**
  Es importante categorizar los activos en función de su tipo y uso dentro de la organización, considerando factores como la confidencialidad, integridad y disponibilidad.
- **Clasificar la información:**
  Se debe definir el nivel de sensibilidad de la información que maneja cada activo, con base en criterios de clasificación establecidos por la entidad.
- **Determinar la criticidad del activo:**
  Evaluar la importancia de cada activo en relación con su impacto en la operación y la continuidad del negocio.
- **Identificar si existe infraestructura crítica cibernética:**
  Reconocer aquellos activos que pueden ser considerados como infraestructura crítica, debido a

su relevancia estratégica o su impacto en la prestación de servicios esenciales.

Al seguir los pasos anteriores serán gestionados de manera efectiva los activos de seguridad de la información, asegurando su adecuada protección y alineación con las normativas vigentes.

4.3. IDENTIFICACIÓN Y GESTIÓN DE RIESGOS

Una vez se ha realizado el levantamiento y clasificación de los activos de información, la siguiente etapa es la identificación y gestión de los riesgos, con el objetivo de garantizar la confidencialidad, integridad y disponibilidad de la información. Este proceso permite a la entidad anticiparse a posibles amenazas, mitigar vulnerabilidades y minimizar el impacto de eventos que puedan comprometer la seguridad de los activos.

Para ello es determinante realizar algunas actividades

- **Identificación de riesgos:**
    1. Reconocimiento de activos de información críticos.
    2. Análisis de posibles amenazas y vulnerabilidades.
    3. Mapeo de actores internos y externos que puedan representar riesgos.
- **Análisis y evaluación de riesgos:**
    1. Valoración del impacto y la probabilidad de ocurrencia de los riesgos identificados.
    2. Priorización de los riesgos según su criticidad.
    3. Definición de niveles de aceptación del riesgo por parte de la organización.
- **Tratamiento de riesgos:**
    1. Diseño e implementación de controles de seguridad para reducir, transferir, aceptar o evitar los riesgos.
    2. Establecimiento de medidas preventivas y correctivas.
    3. Planes de contingencia para garantizar la continuidad del negocio ante incidentes.
- **Monitoreo y seguimiento:**
    1. Evaluación periódica del desempeño de los controles implementados.
    2. Auditorías internas para verificar el cumplimiento de las políticas de seguridad.
    3. Revisión y ajuste del plan de tratamiento de riesgos según la evolución del entorno tecnológico y organizacional.

La Alcaldía promueve una cultura organizacional de seguridad, involucrando a todas las áreas en la identificación y mitigación de riesgos, con el apoyo de programas de capacitación y sensibilización dirigidos a los funcionarios.

Además, se establecen mecanismos de monitoreo continuo para medir el impacto de las estrategias implementadas y realizar ajustes necesarios, garantizando un enfoque de mejora continua, clave para

mantener la seguridad de la información en un entorno cambiante.

5. SEGUIMIENTO Y MEDICIÓN

La oficina de Control interno realiza revisión del cumplimiento del monitoreo de los riesgos y controles y conceptúa acerca de las evidencias entregadas, así como de las fechas de cumplimiento de monitoreo de los controles. La eficacia de la Gestión de riesgos puede medirse con un indicador “Riesgos de Seguridad digital y seguridad de la información mitigados” que está orientado principalmente a disminuir el número de riesgos identificados con nivel alto y extremo, a través de la implementación de controles asociados al cumplimiento de la Norma ISO 27001:2012.

6. CRONOGRAMA

Fase	Actividad	Fecha inicio	Fecha fin	Responsables	Recursos
Fase 1: Gestión de Activos	Determinación de gestores activos de información y de riesgos en los procesos	1/02/2025	28/02/2025	• Líderes de cada proceso • Oficial • seguridad de la Información	Humanos
Fase 1: Gestión de Activos	Capacitación gestión de activos de información	3/03/2025	14/03/2025	Gestores de activos y riesgos Oficial de Seguridad de la Información	Humanos / Tecnológicos (ofimática)
Fase 1: Gestión de Activos	Identificación de activos de información	17/03/2025	30/04/2025	Gestores de activos y riesgos Oficial de Seguridad de la Información	Humanos / Tecnológicos (ofimática)
Fase 1: Gestión de Activos	Clasificación y valoración de activos	2/05/2025	30/05/2025	Gestores de activos y riesgos Oficial de Seguridad de la Información	Humanos / Tecnológicos (ofimática)
Fase 2: Identificación y análisis de riesgos	Recopilación de información sobre riesgos	1/05/2025	31/05/2025	Gestores de activos y riesgos Oficial de Seguridad de la Información	Humanos / Tecnológicos (ofimática)

Fase	Actividad	Fecha inicio	Fecha fin	Responsables	Recursos
Fase 2: Identificación y análisis de riesgos	Evaluación de amenazas y vulnerabilidades	1/05/2025	31/05/2025	Oficial de Seguridad de la Información	Humanos / Tecnológicos (ofimática)
Fase 2: Identificación y análisis de riesgos	Clasificación y priorización de riesgos	1/05/2025	30/05/2025	Oficial de Seguridad de la Información	Humanos / Tecnológicos (ofimática)
Fase 3: Diseño de controles	Definición de controles de seguridad y privacidad	1/06/2025	30/06/2025	Oficial de Seguridad de la Información Lideres de procesos	Humanos / Tecnológicos (ofimática)
Fase 3: Diseño de controles	Someter a aprobación la matriz de riesgo de seguridad y privacidad de la información al Comité Institucional de Gestión y Desempeño	1/06/2025	30/06/2025	Oficial de Seguridad de la Información Lideres de procesos	Humanos / Tecnológicos (ofimática)
Fase 4: Implementación de controles	Capacitación y sensibilización del personal	3/06/2025	30/06/2025	Oficial de Seguridad de la Información	Humanos / Tecnológicos (ofimática)
Fase 4: Implementación de controles	Implementación de los controles	10/06/2025	31/12/2025	Oficial de Seguridad de la Información	Humanos / Tecnológicos (ofimática)
Fase 4: Implementación de controles	Despliegue de controles tecnológicos y operativos	3/06/2025	31/12/2025	Oficial de Seguridad de la Información	Humanos / Tecnológicos (Acorde a los resultados de la evaluación)
Fase 5: Monitoreo y mejora continua	Monitoreo de los riesgos.	3/06/2025	31/12/2025	Oficial de Seguridad de la Información	Humanos / Tecnológicos (ofimática)

Fase	Actividad	Fecha inicio	Fecha fin	Responsables	Recursos
Fase 5: Monitoreo y mejora continua	Evaluación del cumplimiento y efectividad de los controles.	3/06/2025	31/12/2025	Oficia de control interno	Humanos / Tecnológicos (ofimática)

CONTROL DE CAMBIOS VERSIÓN	FECHA DE APROBACIÓN	DESCRIPCIÓN DEL CAMBIO REALIZADO
01	01/2019	CREACIÓN DEL DOCUMENTO
02	01/2020	Actualización del Plan por cambio a vigencia 2020
03	01/2021	Actualización del Plan por cambio a vigencia 2021
04	01/2022	Actualización del Plan por cambio a vigencia 2022
05	30/01/2023	Actualización del Plan por cambio a vigencia 2023
06	19/09/2023	Se actualiza el plan dando cumplimiento a la normatividad vigente, y basado en los resultados del instrumento de evaluación del MSPI.
07	30/01/2024	Se actualiza el plan teniendo en cuenta los resultados de evaluación de los riesgos y al cumplimiento de las actividades definidas para mitigar los riesgos identificados. Actualización del plan para la vigencia 2024.
08	29/01/25	Fue reestructurado el documento en objetivo general, específicos, se actualiza las definiciones y el apartado de desarrollo fue modificado ajustándolo al plan de seguridad proyectado para la anualidad. Adicional fue estructurado el plan desde la fase de levantamiento de activos de información hasta la culminación de la gestión de riesgos.