TABLA DE CONTENIDO

1. OBJETIVOS

1.1. Objetivo General

Garantizar la protección de los datos sensibles y confidenciales manejados por la entidad. Para ello, se han establecido medidas preventivas y correctivas que permiten identificar, evaluar, controlar y monitorear los riesgos asociados a la gestión de la información. Además, se han definido roles y responsabilidades claras para cada uno de los actores involucrados en el proceso, así como se ha implementado un sistema de gestión de la seguridad de la información que permita la continuidad del negocio y la recuperación ante incidentes de seguridad.

1.2. Objetivos Específicos

- Identificar y evaluar los riesgos de seguridad y privacidad de la información en los procesos de la entidad, aplicando los controles necesarios para mitigar los riesgos identificados, para garantizar la protección de la confidencialidad, integridad y disponibilidad de la información de la entidad.
- Cumplir con los lineamientos del Modelo de Seguridad y Privacidad de la información (MSPI) y el marco legal y regulatorio relacionado con la seguridad de la información en Colombia.
- Garantizar la seguridad de los productos desarrollados por la alcaldía de Fusagasugá y cumplir con los estándares de seguridad, especialmente en lo que respeta a la implementación de esquemas de seguridad y certificados SSL.
- Realizar actividades de verificación, configuración y afinamiento de las reglas del firewall y documentar los cambios o configuraciones.
- Compartir contenido digital y capacitar a los funcionarios y contratistas sobre la importancia de realizar copias de seguridad de la información.
- Compartir contenido digital y capacitar a los funcionarios y contratistas sobre las técnicas que usan los cibercriminales para engañar a los usuarios.

2. DEFINICIONES

DDoS: Denegación de servicio distribuido
Firewall: es un sistema de seguridad de red de las computadoras que restringe el tráfico de Internet entrante, saliente o dentro de una red privada. Este software o esta unidad de hardware y software dedicados funciona bloqueando o permitiendo los paquetes de datos de forma selectiva.
SSL: Un certificado SSL es un certificado digital que autentica la identidad de un sitio web y habilita una conexión cifrada
Vulnerabilidad: es la incapacidad de resistencia cuando se presenta un fenómeno amenazante.

3. ALCANCE

La alcaldía de Fusagasugá ha implementado un plan de tratamiento de riesgos de seguridad y privacidad de la información con el objetivo de proteger los datos sensibles de los ciudadanos y garantizar la integridad y confidencialidad de la información manejada por la alcaldía de Fusagasugá. El alcance de este plan abarca la identificación y evaluación de los riesgos, la implementación de medidas de seguridad, la capacitación de los empleados en temas de seguridad de la información y la supervisión constante del cumplimiento de las políticas y procedimientos establecidos. Gracias a este plan, la alcaldía de Fusagasugá ha logrado fortalecer su capacidad para prevenir y atender situaciones de riesgo en materia de seguridad y privacidad de la información, y garantizar un servicio eficiente y confiable a los ciudadanos.

4. RESPONSABLES

Las responsabilidades del Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la información recaen en todos los funcionarios de la Alcaldía de Fusagasugá (planta y contratistas), debido a que todos los servidores públicos son los encargados de crear, recolectar, procesar, analizar datos para la entidad.

Sin embargo, realizando el ajuste a lo establecido con la guía N° 4 roles y responsabilidades de los documentos del Modelo de Seguridad y Privacidad de la Información y mediante la aprobación de los miembros del Comité Institucional de Gestión y Desempeño, se conforma el equipo líder, que supervisara el plan de tratamiento de riesgos de seguridad y privacidad de la información.

Este equipo líder, estará conformado por los miembros del Comité Institucional de Gestión y Desempeño, en conjunto con el oficial de seguridad, representante de la oficina de las TIC y Transformación Digital, un representante de la Oficina de Control Interno y un representante de la Secretaría Jurídica.

5. DESARROLLO

El plan de tratamiento de riesgos de seguridad y privacidad de la información en la alcaldía de Fusagasugá es un documento crucial para garantizar la protección de los datos y documentos que maneja esta entidad pública. Con este plan se busca identificar los riesgos que pueden afectar la integridad de la información y establecer medidas preventivas para minimizarlos y, en caso de que se presenten, contar con planes de contingencia. Es fundamental para la alcaldía de Fusagasugá contar con un plan de estas características, ya que la información que maneja es sensible y puede afectar a la ciudadanía en caso de que se filtre o se pierda. Por ello se aborda el plande tratamiento con base en los dominios de la Norma ISO 27001 base fundamental del Modelo de Seguridad y Privacidad de la Información MSPI.

5.1. 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, a continuación, se muestra de forma gráfica el proceso de gestión del riesgo de la seguridad de la información.

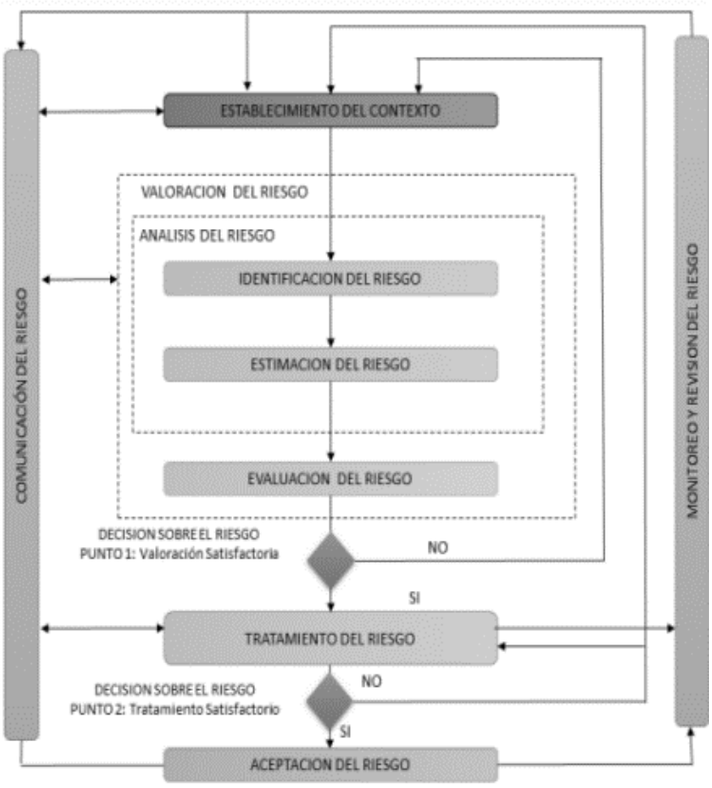

Ilustración 3: Proceso de gestión del riesgo de la seguridad de la información (Tomado de la NTC-ISO/IEC 27005)

La siguiente tabla resume las actividades de gestión del riesgo en la seguridad de la información que son pertinentes para las cuatro fases del proceso del MSPI

ETAPAS DEL MSPI	PROCESO DE GESTION DEL RIESGO EN LA SEGURIDAD DE LA INFORMACION
Planear	Establecer Contexto Valoración del Riesgo Planificación del Tratamiento del Riesgo Aceptación del Riesgo
Implementar	Implementación del Plan de Tratamiento de Riesgo
Gestionar	Monitoreo y Revisión Continua de los Riesgos
Mejora Continua	Mantener y Mejorar el Proceso de Gestión del Riesgo en la Seguridad de la Información.

5.2. Identificación del Riesgo

Se identifican tres riesgos naturales los cuales pueden afectar el proceso Gestión TIC, por lo cual también se establecen los criterios a tener en cuenta para mitigar los mismos; los riesgos identificados son:

- **Fuga de información:** Posibilidad de pérdida económica y reputacional por pérdida o fuga de información institucional debido a actos de fraude, actuaciones irregulares, comisión de hechos delictivos abuso de confianza, apropiación indebida, incumplimiento de regulaciones legales o internas de la entidad.

- **Vulneración de sistemas de información:** Posibilidad de pérdida económica y reputacional por la pérdida de información, vulneración de sistemas de información y aplicaciones informáticas fundamentales para la operación de la entidad debido a los ataques por virus informáticos
- **Indisponibilidad en la operación:** Posibilidad de pérdida económica y reputacional por la indisponibilidad en la operación de los Sistemas de Información, plataformas web, aplicaciones y comunicaciones debido a los ataques de denegación de servicios DDoS.

5.2.1 Causa raíz del riesgo

Riesgo	Impacto	Causa Inmediata	Causa Raíz
Fuga de información	Económico y Reputacional	Perdida o fuga de información institucional	Actos de fraude, actuaciones irregulares, comisión de hechos delictivos abuso de confianza, apropiación indebida, incumplimiento de regulaciones legales o internas de la entidad. Personal que no trabaja en la entidad y aún tiene acceso a los sistemas.
Vulneración de sistemas de información	Económico y Reputacional	Perdida de información, vulneración de sistemas de información y aplicaciones informáticas fundamentales para la operación de la entidad	Ataques por virus informáticos, conexión fraudulenta por medio de VPN
Indisponibilidad en la operación	Económico y Reputacional	Indisponibilidad de los Sistemas de Información, plataformas web, aplicaciones y comunicaciones de la entidad	Ataques de denegación de servicios DDoS

5.2.2 Criterios de impacto

Riesgos	Clasificación del Riesgo	Probabilidad Inherente	%	Criterios de impacto	Frecuencia con la cual se realiza la actividad
Fuga de información	Fraude Interno	Baja	40%	El riesgo afecta la imagen de la entidad internamente, de conocimiento general, nivel interno	Semestral

Vulneración desistemas de información	Fallas Tecnológicas	Baja	40%	El riesgo afecta la imagen de la entidad internamente, de conocimiento general, nivel interno.	Semestral
Indisponibilidad en la operación	Fallas Tecnológicas	Muy Baja	20%	El riesgo afecta la imagen de la entidada nivel nacional, con efecto publicitarios sostenible a nivel país	Semestral

5.2.3 Impacto Inherente

Riesgo	Impacto Inherente	%	Zona de Riesgo Inherente
Fuga de información	Menor	40%	**Moderado**
Vulneración de sistemas de información	Menor	40%	**Moderado**
Indisponibilidad en la operación	**Catastrófico**	**100%**	**Extremo**

5.3. Identificación de las Amenazas

Las amenazas causan daños a la información, estas amenazas pueden ser internas o externas, y pueden provenir de diversas fuentes, como amenazas cibernéticas, errores humanos, desastres naturales, entre otros.

TIPO	AMENAZA
Eventos naturales	Fenómenos Climáticos, polvo, corrosión
Daño físico	Pérdida del suministro de energía
Acciones no autorizadas	Uso no autorizado del equipo Corrupción de datos Procesamiento ilegal de datos Acceso forzado al sistema Copias ilegales de software y datos reservados
Pérdida de los servicios esenciales	Falla del sistema de aire acondicionado Falla en equipos de comunicaciones Fallos en discos de datos
Compromiso de la información	Hurto de documentos Hurto de equipos de computo
Fallas técnicas	Fallas en equipos Fallas en el diseño de software Faltas de mantenimiento

5.4. Identificación de las Vulnerabilidades

Las vulnerabilidades son las debilidades que se encuentran en un activo o en un control y se pueden explotar por una o más amenazas, lo que lo convierte en un riego de seguridad. Para proteger la información, se debe identificar, valorar, priorizar y corregir las debilidades que sean identificadas en los activos.

TIPO DE ACTIVO	VULNERABILIDADES	DESCRIPCIÓN
HARDWARE	Fácil acceso a las dependencias de la entidad.	No existen controles para filtrar el acceso a los visitantes y/o funcionarios de otras dependencias.
SOFTWARE	Contraseñas simples	Se deben utilizar contraseñas seguras que contengan (Debe incluir números. Utilice una combinación de letras mayúsculas y minúsculas.)
	Bloqueó de la pantalla	Todo funcionario, contratista o personal tercerizado debe bloquear la sesión en su equipo al levantarse de su puesto de trabajo, y adicionalmente debe tener habilitado el bloqueo automático de sesión por inactividad, de tal manera que la sesión se encuentre siempre cerrada cuando el puesto se encuentre sin custodia
	Copias de seguridad	Es de suma importancia realizar las copias de seguridad de forma periódica.
	Compartir usuario de red y contraseña	Es una de las vulnerabilidades mas comunes, esta se presenta en su mayoría con el personal que se encuentra en vacaciones o las nuevas contrataciones
PERSONAL	Documentos en la papelera completos.	Se deben destruir los documentos que se desechan, para no comprometer datos confidenciales.
	Desconocimiento de las políticas de seguridad	Se deben brindar capacitaciones constantes para garantizar el conocimiento de las políticas de seguridad de la entidad

6. PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD

De acuerdo con los resultados del análisis de riesgos se identifican vulnerabilidades que deben ser corregidas para los procesos de la Alcaldía de Fusagasugá, lo que conlleva a un plan de tratamiento base que debe ser aplicado y que se describe en este documento. A continuación, se aborda el plan de tratamiento con base en los dominios de la Norma ISO 27001 base fundamental del Modelo de Seguridad y Privacidad de la Información MSPI.

Las actividades implican la responsabilidad de todos los servidores públicos y los procesos frente a la participación en las capacitaciones y toma de conciencia con relación a las buenas prácticas, recomendaciones y el MSPI; generando una cultura de cambio en la entidad y la

apropiación del MSPI.

Basados en el plan de tratamiento de riesgos se proponen responsables y fechas:

6.1. Contexto de seguridad de la información

Actividad	Responsable	Periodo de ejecución
Evaluar los conocimientos de los funcionarios de la entidad mediante un formulario y determinar si estos redundan en la mejora del MSPI como insumo permanente en la identificación, valoración y tratamiento de los riesgos de seguridad de la información y aplicación de buenas prácticas para prevenir delitos informáticos y disminuir vulnerabilidades y amenazas.	Oficial de Seguridadde la Información	Semestral

6.2. Liderazgo y compromiso

Actividad	Responsable	Periodo de ejecución
Reunir al equipo de trabajo para sensibilizar a todos los funcionarios y contratistas frente al cumplimiento obligatorio de las políticas, procedimientos, formatos, manuales, guías y demás que estén definidos en el MSPI.	Líder del proceso seguridad	Cuatrimestral
Realizar una acción o actividad que permita evidenciar la mejora en la seguridad de la información o informática, como apropiación, actualización de infraestructura tecnológica, física y/o servicios de seguridad y de TI.	Líder del proceso Seguridad	Cuatrimestral
Realizar una acción anual que permitan prevenir la ocurrencia de delitos informáticos, aplicar las recomendaciones emitidas por los entes de control y vigilancia, así como, las políticas y demás lineamientos dela Alcaldía de Fusagasugá; vincular a las entidades bancarias para validar la infraestructura y servicios que permitan garantizar la seguridad en las operaciones o transacciones que comprometen recursos públicos a través de los portales o plataformas bancarias virtuales como: consultas, pagos y transferencias electrónicas. Solicitar a las entidades bancarias, capacitaciones, para poder identificar los procedimientos que realizan para la seguridad de la información monetaria de la entidad	Secretaria de Hacienda (Proceso: Hacienda Pública)	Semestral
Informar los avances y acciones ejecutadas frente al Plan de Seguridad y tratamiento de riesgos de seguridad de la información, a la Dirección de Desarrollo Organizacional.	Líder del proceso Seguridad	Semestral
Incluir dentro del plan de capacitación, sensibilización y formación a los funcionarios en temas de seguridad de la información, seguridad informática, ingeniería social y prevención de delitos informáticos, tales como (sabotaje informático, piratería informática, robo de identidad). Listados de asistencia, registro fotográfico y acta para evidenciar la realización de las mismas.	Dirección de GestiónHumana (Proceso Talento Humano)	Semestral

6.3. Planificación

Actividad	Responsable	Periodo de ejecución
Brindar al Comité Institucional de Gestión y Desempeño la información que sea necesaria para el entendimiento del MSPI en un lenguaje claro y conciso, y demás acciones que permitan la mejora del mismo.	Oficial de Seguridadde la Información	Semestral
Actualizar la matriz de riesgos informáticos con las acciones preventivas encaminadas para evitar que se presenten riesgos de fraudes y delitos electrónicos en la Alcaldía de Fusagasugá.	Oficina TIC	Anual

6.4. Operación

El MSPI trae consigo una serie de controles direccionados por políticas y procedimientos para todos los procesos definidos formalmente en la Alcaldía de Fusagasugá, y también aquellos lineamientos o sugerencias de entidades de control y vigilancia. Estos controles traerán cambios para los procesos, destacando los siguientes:

Actividad	Responsable	Periodo de ejecución
Realizar control y seguimiento frente al avance y cumplimientos de las actividades que se encuentren señaladas en el Plan de Tratamiento de Riesgos de Seguridad de la y dar a conocer los resultados en reuniones del comité institucional de Gestión y Desempeño, lo anterior, con la información brindada por cada una de las dependencias responsables.	Líder del proceso de seguridad	Semestral
Socializar a todos los funcionarios el formato de activos de información, con el fin de contextualizar y resolver las dudas necesarias para la realización del inventario completo de los activos de información de la Alcaldía de Fusagasugá, con el fin de establecer medidas de seguridad adecuadas para su protección.	Oficina de las TIC y Transformación Digital Oficina Asesora de Comunicaciones Secretaria Administrativa Secretaría Jurídica.	Semestral
Actualizar y publicar datos abiertos de la entidad en cumplimiento a la Ley 1712 de 2014 sobre Transparencia y Acceso a la Información Pública Nacional, como información pública dispuesta en formatos que permiten su uso y reutilización bajo licencia abierta y sin restricciones legales para su aprovechamiento.	Oficina de las TIC y Transformación Digital Oficina Asesora de Comunicaciones	Semestral

6.5. Organización para la seguridad de la información

6.5.1 Contacto con las autoridades

Este control es requerido para dar parte a las autoridades del orden nacional en caso de la ocurrencia de un incidente de seguridad de la información o delitos informáticos, se requiere entonces llevar a cabo una reunión con el Comité Institucional de Gestión y Desempeño para tener claridad en los casos en los que se deben reportar los incidentes de seguridad informática, de la información o delitos informáticos con autorizades establecidas del orden nacional, procedimiento que debe ser de conocimiento de toda la entidad. Las actividades propuestas para este ítem son las siguientes:

Actividad	Responsable	Periodo de ejecución
Diseñar el procedimiento y formato de reporte de incidentes de seguridad en el sistema GLPI y dar a conocer a los funcionarios su uso y aplicación, por medio de capacitaciones para el correcto uso de la aplicación, evidenciando los encuentros con listados de asistencia y levantamiento de un acta, la cual evidencia la realización de las reuniones.	Oficina de las TIC y Transformación Digital (Proceso: Gestión TIC)	Cuatrimestral
Reportar a las entidades competentes a nivel nacional los eventos o incidentes de seguridad identificados o reportados por los funcionarios, de acuerdo al caso a: Centro Cibernético Policial, Col-Sert, Comando Conjunto Cibernético, Fiscalía, Contraloría, Procuraduría, DIJIN y SIC, y a la Dirección de Desarrollo Organizacional como segunda línea de defensa de la entidad.	Oficial de seguridad de la información	Cuando ocurra el incidente

6.5.2 Contacto con grupos de interés especial

Teniendo en cuenta los requerimientos de seguridad de la información, el Oficial de seguridad, o quien haga sus veces, debe validar con que empresas, entidades, organizaciones y/o asociaciones se puede obtener apoyo para la exitosa implementación de los controles del MSPI, teniendo como guía los siguientes lineamientos:

Actividad	Responsable	Periodo de ejecución
Marco legal y regulatorio: Brindar apoyo con el marco legal y regulatorio, en cuanto a temas como protección de datos personales, derechos de autor, delitos informáticos, Ley de Transparencia y Acceso a la Información Pública, entre otros.	Secretaría Jurídica (Proceso: Gestión Jurídica) Oficial de seguridad de la información	Semestral

Nuevas amenazas: Dar a conocer las amenazas o malware detectado en la entidad y compartir las recomendaciones o sugerencias que señalan circulares, boletines y demás emitidos por otras entidades de seguridad. Realizar capacitaciones para que los funcionarios de la entidad, sepan qué hacer cuando se presente una amenaza informática.	Oficial de seguridadde la información	Cuatrimestral

6.6. Seguridad para el Talento Humano

Desde la Dirección de Gestión del Talento Humano, la Dirección de Contratación, supervisores de contrato, se debe tener en cuenta los siguientes puntos:

6.6.1 Responsabilidad de los funcionarios y contratistas

La implementación del MSPI trae consigo nuevas tareas y responsabilidades para todos los funcionarios de la alcaldía; por lo tanto, es necesario formalizar para cada perfil estas nuevas asignaciones. Esta formalización se debe realizar desde el área de Gestión del Talento Humano, la Dirección de Contratación con la orientación del Oficial de seguridad de la información, o quien haga sus veces, y el responsable del proceso correspondiente. Se debe definir los siguientes aspectos:

Actividad	Responsable	Periodo de ejecución
Actualizar el Formato Acuerdo de Confidencialidad, para la protección de la información de cada funcionario, verificando que en la vinculación laboral todos los servidores públicos suscriban: Acuerdo de confidencialidad con el propósito de informar frente a la no divulgación de información (incluido cuentas de usuario, contraseñas de los diferentes sistemas de información, aplicaciones, correos electrónicos institucionales y demás) y actualización del formato de autorización para el tratamiento de Datos Personales, teniendo en cuenta que la responsabilidad penal es individual).	Dirección de Contratación (Procesos: Gestión Jurídica) Oficial de seguridad de la información Dirección de Gestión Humana (Proceso Talento Humano)	Semestral
Firmar el formato Acuerdo de Confidencialidad, para la protección de la información por cada uno de los servidores públicos de la entidad durante su proceso de vinculación y/o inicio de contrato.	Todos los servidores Públicos	Cuando sea requerido

6.6.2 Responsabilidad de Talento humano en el MSPI

Actividad	Responsable	Periodo de ejecución
Socializar con la Dirección de Gestión del Talento Humano y la Dirección de Contratación los procedimientos relacionados con ingreso, modificación, inactivación y revisión de cuentas de usuario para uso de funcionario y contratista para las plataformas, aplicaciones y sistemas de información de la Alcaldía.	Oficina de las TIC y Transformación Digital Dirección de Gestión del Talento Humano Dirección de Contratación	Cuatrimestral
Dirección de Gestión del Talento Humano y Dirección de Contratación: Informar los traslados, retiros y las demás novedades de personal que puedan afectar el uso de licencias en los sistemas de información de la alcaldía de Fusagasugá y de esta manera mantener actualizada la información en las bases de datos de la entidad. Oficina de las TIC y Transformación Digital: realizar la consulta y ejecutar los cambios pertinentes en los sistemas de información de la alcaldía de Fusagasugá y de esta manera, garantizar la seguridad de la entidad.	Dirección de Gestión del Talento Humano, (Procesos: Talento Humano) Dirección de Contratación Oficina de las TIC y Transformación Digital	Cuatrimestral

6.7. Políticas de Seguridad de la Información

Teniendo en cuenta los riesgos identificados de seguridad de la información, la Alcaldía de Fusagasugá a continuación presenta las actividades que deben efectuarse para promover el cumplimiento de algunas políticas señaladas en el MA-GT-002 Manual de Seguridad de la Información, el cual fue aprobado por el Comité Técnico de Calidad en el mes de marzo de 2018; adicional a ello se presentan aquellos componentes que deben ser tratados dentro de este plan, así como, actividades que involucran activamente los dueños de procesos y los servidores públicos de la entidad como responsables de la seguridad de la información.

Actividad	Responsable	Periodo de ejecución
Presentación del MSPI y el Manual de Seguridad y Privacidad de la Información para poder identificar los conocimientos y la aplicación de los funcionarios y contratistas sobre sus responsabilidades y aplicación del MSPI, lo que implica el conocimiento de los conceptos de seguridad de la información, políticas, buenas prácticas, entre otros que se consideren pertinentes por medio del diligenciamiento de un formulario.	Proceso Gestión TIC	Semestral

6.7.1 Política de Control de Acceso

Objetivo de la política: La Política de Control de Acceso de la Alcaldía del municipio de

Fusagasugá provee las directrices para que la información únicamente sea accedida por los funcionarios y/o terceras partes autorizadas con base en las funciones de su rol frente a los procesos formalmente definidos por el Sistema Integrado de Gestión.

6.7.1.1 Gestión de Cuentas de Usuario

Actividad	Responsable	Periodo de ejecución
Actualizar el formato de copias de seguridad con el fin de verificar, definir y autorizar la inactivación de las cuentas de usuario de red, roles y permisos a los sistemas de información, red, correo electrónico institucional y otros que requieren los servidores públicos para el ejercicio de sus funciones u obligaciones.	Proceso Gestión TIC	Anual
Atender las solicitudes realizadas por los líderes de proceso para la creación y/o inactivación de cuentas de usuario de red, sistemas de información, plataformas web, correo electrónico institucional y otros que se autoricen según disponibilidad y pertinencia.	Proceso Gestión TIC	Cuando se requiera

6.7.1.2 Acceso a Redes y Servicios de Red

Actividad	Responsable	Periodo de ejecución
Formular la guía de control de accesos a redes cableadas y/o inalámbricas y sus servicios, validando el cumplimiento de la política de control de acceso, exclusivamente para servidores públicos activos de la entidad.	Oficina TIC (Proceso: Gestión TIC)	Semestral
Contratar el servicio de internet de respaldo con diferente operador y medio de transmisión para mitigar el riesgo de suspensión del servicio de internet sin previo aviso por el operador actual en el centro administrativo municipal.	Oficina TIC (Proceso: Gestión TIC)	Anual
Realizar las configuraciones lógicas y/o físicas para mejorar la seguridad de las redes telemáticas y garantizar el servicio.	Oficina TIC (Proceso: Gestión TIC)	Cuatrimestral

6.7.1.3 Control de Acceso Físico

Actividad	Responsable	Periodo de ejecución
Generar estrategias para el control de acceso físico a la Alcaldía de Fusagasugá, que corresponda a la seguridad física y del entorno de los equipos y demás infraestructura tecnológica de la entidad para evitar su acceso de personal no autorizado.	Dirección de Recursos Físicos (Procesos: Gestión Administrativa, Talento Humano)	Semestral

Dar a conocer a la entidad y a los proveedores de servicios de seguridad y vigilancia, cuáles son los controles establecidos para el acceso físico a la entidad.	Dirección de Recursos Físicos (Procesos: Gestión Administrativa, Talento Humano)	Semestral
Dar cumplimiento al diligenciamiento del formato para el control de acceso al centro de datos o Data Center de la entidad.	Oficina de las TIC y Transformación Digital (Proceso: GestiónTIC)	Cuando se requiera
Aplicar una directiva de seguridad en el directorio activo del servidor local para restringir el acceso de memorias USB a los equipos de cómputo de la entidad por perfiles de usuario.	Oficial de Seguridad de la Información	Anual

6.7.2 Política de uso aceptable de los activos

Objetivo de la política: La Política para el Uso Aceptable de los Activos de la Alcaldía del municipio de Fusagasugá busca que cada funcionario o contratista sepa cuál es el tratamiento que debe tener para cada uno de los activos asociados a la información que tenga a su cargo en lo referente a seguridad de la información.

El requerimiento de seguridad tiene como base el tratamiento de los riesgos identificados, por lo tanto, la entidad debe garantizar los recursos necesarios como tiempo, presupuesto, personal capacitado, verificación de la idoneidad en los servidores públicos, con el propósito de generar las acciones para controlar los regos de seguridad, de no ser así, la entidad asume el riesgo al que se expondría.

6.7.2.1 Gestión y uso aceptable de los activos

Actividad	Responsable	Periodo de ejecución
Actualizar el inventario de activos de información en el formato vigente según los lineamientos del MINTIC, teniendo claro los roles de responsable, criticidad de la información, principios de la seguridad de la información y custodio, que refleje la realidad de todos los procesos que ejecutan como parte de la misionalidad y funciones, aplicar los lineamientos de la Ley 1712 de 2014 sobre Transparencia y Acceso a la Información Pública Nacional, identificando los activos de información que contienen datos personales y otros que establece la normatividad concordante.	Oficina de las TIC y Transformación Digital Oficina Asesora de Comunicaciones Secretaria Administrativa Secretaría Jurídica	Anual
Actualizar el inventario de los activos tecnológicos, incluir las características mínimas de cada activo en cada una de las dependencias de la alcaldía de Fusagasugá.	Oficina TIC y Transformación Digital (Proceso: Gestión TIC)	Cuatrimestral

Orientar a los dueños o líderes de cada proceso para definir el uso aceptable de los activos de información que hacen parte de su responsabilidad y capacitar a los funcionarios frente al tema, indicando el marco legal y regulatorio.	Oficial de Seguridadde la Información	Anual
Creación de un Manual de usuario y/o procedimiento para indicar a los dueños de proceso como se deben salvaguardar las cuentas de usuario tipo administrador y contraseñas de las plataformas en la nube, sistemas de información, aplicaciones servidores, dominós, redes telemáticas, entre otros.	Oficina TIC y Transformación Digital (Proceso: Gestión TIC)	Anual

6.7.3 Política de Generación y Restauración de Copias de Respaldo

Objetivo de la política: La Política de Generación y Restauración de Copias de Respaldo de la Alcaldía del municipio de Fusagasugá provee las directrices para que el proceso de generación y restauración de copias de respaldo se realice aplicando los requerimientos de seguridad para los activos de información.

6.7.3.1 Responsabilidad de los Usuarios

A partir de la identificación de cualquier incidente causado por acción de un malware es responsabilidad del dueño del equipo afectado o del equipo desde donde se generó el caso realizar el reporte y atender los lineamientos brindados frente al caso. Con base en esto el responsable del proceso debe comprometer a su equipo de trabajo para que a partir de ese momento hagan efectivo la aplicación del antimalware; la Oficina TIC y Transformación Digital o quien haga sus veces procederá a desconectar el equipo de la red por el término que determine prudente para tratar el malware y evitar la proliferación del mismo.

Actividad	Responsable	Periodo de ejecución
Suscribir Acuerdo de confidencialidad (incluido cuentas de usuario, contraseñas de los diferentes sistemas de información, aplicaciones, correos electrónicos institucionales y demás) y Formato deautorización para el tratamiento de Datos Personales, aplicar los lineamientos de seguridad de la entidad y demásnormatividad aplicable, teniendo en cuenta que la responsabilidad penal es individual.	Todos los servidores públicos y contratistas	Cuando se vincule a la entidad por nombramiento o contrato
Informar a la Oficina TIC y Transformación Digital por medio de la plataforma GLPI los incidenteso eventos de malware que afectan los equipos tecnológicos, indicando desde donde se generó y cuando se presentó el incidente de seguridad.	Todos los servidores públicos y contratistas	Cuando se presente el incidente

Revisar los malware identificados, aislar el equipo de cómputo o desconectar de la red por el término que determine prudente para tratar el malware y evitar la proliferación del mismo. Instalación de un sistema de protección en todos los equipos de la entidad, activado y actualizado para la protección de la información.	Oficina TIC	Semestral

6.7.3.2. Obligatoriedad del respaldo

Es responsabilidad de cada propietario de la información realizar continuamente copia de respaldo de la información que maneja, ya que, si se presenta un incidente ocasionado por la falla en el equipo de cómputoo, la responsabilidad es del propietario de dicha información más no de la Oficina TIC y Transformación Digital.

Es responsabilidad del dueño del proceso velar por la propiedad intelectual de la información de la entidad y su custodia, así como, verificar que los funcionarios y contratistas entreguen los respaldos de la información, no la oculten o la guarden para sí mismos.

Los servidores públicos deben aplicar lo señalado en el inventario de activos de información con relación a la disponibilidad, integridad, confidencialidad y custodia de la información, según como se encuentre clasificado para su uso, así como, brindar a los ciudadanos la información requerida de acuerdo a la Ley de Transparencia y Acceso a la Información Pública o la que en su momento les sea autorizado por escrito por parte del dueño del proceso para su entrega, teniendo en cuenta la normatividad para datos personales y demás concordante.

Actividad	Responsable	Periodo de ejecución
Aplicar el procedimiento, guía y formato para garantizar la copia de seguridad de la información que genera cada uno de los servidores públicos en el ejercicio de sus obligaciones o funciones, entregarla en custodia a la Oficina TIC y Transformación Digital de acuerdo a la novedad (entrega de cargo, vacaciones, licencias, finalización de contrato, entre otros).	Todos los servidores públicos	Cuando se requiera
Realizar plan de copias de seguridad y respaldo de las bases de datos, aplicaciones, sistemas de información y demás activos que se encuentran identificados en el inventario y garantizar su custodia, según lo establecido en el procedimiento PR-GT-005.	Líderes o dueños de proceso	Anual
Recibir y custodiar las copias de seguridad de la información que entregan los funcionarios y contratistas de la entidad en unidades de almacenamiento de red o según el mecanismo que se considere conveniente.	Oficina TIC y Transformación Digital (Proceso: Gestión TIC)	Cuando se requiera

6.7.3.3 Gestión de Vulnerabilidades

Actividad	Responsable	Periodo de ejecución
Realizar la revisión permanente de las vulnerabilidades, fallas o inconvenientes que presentan los sistemas de información, aplicaciones y plataformas que se encuentran bajo la responsabilidad del proceso, con el fin que se lleven a cabo las acciones o se tomen las medidas oportunas de acuerdo con la criticidad identificada.	Líderes o dueños deproceso y Oficial de seguridadde la información	Semestral

6.7.4 Política de Construcción de Sistemas Seguros

Actividad	Responsable	Periodo de ejecución
Realizar documento del plan de pruebas para cada sistema de información, aplicaciones o plataformas desarrollados dentro de la entidad, incluyendo pruebas funcionacionales, no funcionales y exploratorias, que corroboren el correcto funcionamiento de las plataformas antes de su puesta en producción.	Líder o dueños de proceso, Oficial de seguridad de la información	Cuando se requiera
Disponer de un entorno o servidor para pruebas funcionales, en entorno QA y otro servidor para preproducción y producción de desarrollos de la entidad, aplicando protocolos establecidos en el Procedimiento No. PR-GT-007 Procedimiento de Construcción de Software.	Líder o dueños de proceso, Oficial de seguridad de la información	Anual

6.7.4.1 Reporte y Gestión de Incidentes de Seguridad de la Información

Actividad	Responsable	Periodo de ejecución
Socializar el procedimiento y formato para el reporte de eventos o incidentes de seguridad a los entes encargados a nivel nacional y a la dirección de Desarrollo Organizacional como segunda línea de defensa en la entidad.	Oficina TIC y Transformación Digital (Proceso: Gestión TIC)	Cuatrimestral
Ejecutar acciones o controles para el tratamiento o manejo de los incidentes de seguridad de la información.	Oficial de seguridad de la información	Cuando se presente
Reportar los incidentes de seguridad oportunamente cuando se presenten atendiendo los lineamientos establecidos por la Oficina TIC y Transformación Digital	Todos los servidores públicos de la entidad	Cuando se presente

6.7.5 Política de legislación aplicable y requisitos contractuales

Objetivo de la política: Evitar el incumplimiento por parte de la Alcaldía del municipio de Fusagasugá de las obligaciones legales, reglamentarias o contractuales relacionadas con la seguridad de la información.

Actividad	Responsable	Periodo de ejecución
Revisar y actualizar el Acuerdo de confidencialidad y Formato de autorización para el tratamiento de Datos Personales, para garantizar que incluyan el marco legal vigente aplicable.	Secretaría Jurídica (Procesos: GestiónJurídica)	Anual
Socializar a todos los servidores públicos la normatividad sobre delitos informáticos vigente como parte de los lineamientos de Seguridad de la Información.	Oficina TIC y Transformación Digital (Proceso: Gestión TIC)	Cuatrimestral

6.7.6 Política de Protección de Datos Personales

Actividad	Responsable	Periodo de ejecución
Socializar la política de protección de datos personales y normatividad aplicable a los servidores públicos de la entidad con el fin de tener claridad y brindar información correcta.	Secretaría Jurídica (Procesos: GestiónJurídica) Oficial de seguridad de la información	Cuatrimestral

5. 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.**