Contenido

1. OBJETIVOS

- Promover el uso de mejores prácticas en seguridad de la información, como base de aplicación de la Política de Seguridad Digital.
- Adoptar la Resolución 500 de 2021, con referencia a 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.
- Dar a conocer el procedimiento para la diligenciar el formato MAPA DE RIESGOS SEGURIDAD DE LA INFORMACIÓN, con el fin de realizar una buena identificación y

clasificación de los riesgos existentes en la Alcaldía de Fusagasugá según su criticidad basados en la confidencialidad, integridad y disponibilidad para posteriormente definir el tratamiento adecuado de los mismos estableciendo procedimientos de seguridad que permitan la apropiación de la política de Gobierno Digital.

2. ALCANCE

Este procedimiento aplica para todos los procesos definidos en el Sistema de Gestión de Calidad de la entidad, que deben diligenciar el mapa de riesgos de seguridad de la información, de acuerdo a los lineamientos establecidos por el MINTIC, que son adoptados, definidos y aprobados por el Comité Técnico de Calidad, para que en el plan de tratamiento de riesgos y se establezcan los controles necesarios que permitan una mejora continua al Modelo de Seguridad y Privacidad de la Información de la Alcaldía del municipio de Fusagasugá.

3. RESPONSABLE DEL PROCEDIMIENTO

Jefe de la Oficina de Tecnologías de la Información y las Comunicaciones y debe ser aplicado por los contratistas y funcionarios de la entidad.

4. GLOSARIO

- **Acceso a la Información Pública:** Derecho fundamental consistente en la facultad que tienen todas las personas de conocer sobre la existencia y acceder a la información pública en posesión o bajo control de sujetos obligados. (Ley 1712 de 2014, art 4).
- **Activo:** En relación con la seguridad de la información, se refiere a cualquier información o elemento relacionado con el tratamiento de esta (sistemas, soportes, edificios, personas…) 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 20116).

- **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.(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).

- **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.

- **Confidencialidad**: Propiedad de la información que la hace no disponible o sea divulgada a individuos, entidades o procesos no autorizados.

- **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.

- **Disponibilidad**: Propiedad de ser accesible y utilizable a demanda por una entidad.

- **Gobierno Digital:** De forma general, consiste en el uso de las tecnologías digitales como parte integral de las estrategias de modernización de los gobiernos para crear valor público.

- **Impacto**: las consecuencias que puede ocasionar a la organización la materialización del riesgo.

- **Integridad**: Propiedad de exactitud y completitud.

- **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.

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

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

- **Riesgo Inherente**: Nivel de riesgo propio de la actividad. El resultado de combinar la probabilidad con el impacto, nos permite determinar el nivel del riesgo inherente, dentro de unas escalas de severidad.

- **Riesgo Residual**: El resultado de aplicar la efectividad de los controles al riesgo inherente.

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

- **Seguridad de la información**: Preservación de la confidencialidad, integridad, y disponibilidad de la información en cualquier medio: impreso o digital. (ISO/IEC 27000).

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

5. DOCUMENTOS DE REFERENCIA

- **RESOLUCIÓN NÚMERO 00500 DE MARZO 10 DE 2021**

https://gobiernodigital.mintic.gov.co/692/articles-162625_recurso_2.pdf

"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"

- **MSPI**

https://gobiernodigital.mintic.gov.co/seguridadyprivacidad/704/articles162621_Modelo_de_Seguridad_y_Privacidad__MSPI.pdf

Modelo de Seguridad y Privacidad de la Información

6. DESARROLLO

ACTIVIDAD	DESCRIPCIÓN	RESPONSABLE
1. Descripciones de la matriz	Revisar de manera detallada las descripciones de cada campo.	Lider del proceso
2. Contexto: Definir el tipo de activo de información	Proceso Nombre del proceso que posee el riesgo que se va a identificar.	Líder del proceso

	Tipo de activo de información: Define el tipo de activo de información que presenta el riesgo. • Información y datos de la entidad: Información almacenada física o electrónicamente Ejemplo: Bases y archivos de datos, contratos, documentación del sistema, investigaciones, acuerdos de confidencialidad, manuales de usuario, procedimientos operativos o de soporte, planes para la continuidad del negocio, acuerdos sobre retiro y pruebas de auditoria, entre otros… • Sistemas de información y aplicaciones de Software: Software de aplicación, interfaces, software del sistema, herramientas de desarrollo y otras utilidades relacionadas. • Dispositivos de Tecnologías de información – Hardware: Elementos físicos Ejemplo: Servidores, equipos de cómputo, memorias, discos duro, CD´s, etc… • Soporte para el almacenamiento de información: Equipos para almacenamiento de información Ejemplo: USB, discos duros, CDs, etc…	Líder del proceso – Jefe oficina TIC

	• Servicios: Servicios de computación y comunicaciones Ejemplo: Internet, páginas de consulta, directorios compartidos e intranet.	
	Activo de información: Nombre completo del activo de información.	Líder del proceso – Jefe oficina TIC
Identificación del riesgo	Nro. Representa un indicador único consecutivo del riesgo.	Líder del proceso – Jefe oficina TIC
	Riesgo Escribir de forma general el riesgo que puede presentar el activo de información	Líder del proceso – Jefe oficina TIC
	Descripción del riesgo Describa el riesgo, está descripción se refiere a las características que presenta el riesgo identificado.	Líder del proceso – Jefe oficina TIC
	Responsable de determinar la materialización del riesgo Se debe indicar un coordinador responsable del proceso	Líder del proceso
	Amenazas Analizar que amenazas podría causar la materialización del riesgo.	Líder del proceso – Jefe oficina TIC

	Vulnerabilidades Analizar las vulnerabilidades que causaría si el riesgo se llega a materializar.	Líder del proceso – Jefe oficina TIC

Análisis de riesgo inherente	Probabilidad. Es la medida para estimar la ocurrencia en que el riesgo inherente identificado se materialice, este se determina con criterios de Frecuencia, si se ha materializado cierto numero de veces en determinado tiempo. 1. **RARO:** El evento puede ocurrir solo en circunstancias excepcionales. No se ha presentado en los últimos 5 años. 2. **IMPROBABLE:** El evento puede ocurrir en algún momento. Al menos 1 vez en los últimos 5 años. 3. **POSIBLE:** El evento podría ocurrir en algún momento. Al menos 1 vez en los últimos 2 años. 4. **PROBABLE:** El evento probablemente ocurrirá en la mayoría de las circunstancias. Al menos 1 vez en el último año. 5. **CASI SEGURO:** Se espera que el evento ocurra en la mayoría de las circunstancias. Más de 1 vez al año.	Líder del proceso – Jefe oficina TIC

	Impacto Son las consecuencias potenciales que genera el hecho de que el riesgo inherente se materialice, este impacto se da generalmente sobre las personas, bienes materiales e inmateriales, daños físicos, sanciones, investigaciones, pérdidas económicas, de	Líder del proceso – Jefe oficina TIC
	información, de bienes, afectación de la imagen, de la credibilidad y de la confianza, interrupción de servicios, daños ambientales, entre otros. Se evalúa en 5 categorías: 1. **INSIGNIFICANTE:** Si el hecho llegara a presentarse, tendría consecuencias o efectos mínimos sobre la entidad. 2. **MENOR:** Si el hecho llegara a presentarse, tendría bajo impacto o efecto sobre la entidad. 3. **MODERADO:** Si el hecho llegara a presentarse, tendría medianas consecuencias o efectos sobre la entidad. 4. **MAYOR:** Si el hecho llegara a presentarse, tendría altas consecuencias o efectos sobre la entidad. 5. **CATASTRÓFICO:** Si el hecho llegara a presentarse, tendría desastrosas consecuencias o efectos sobre la entidad.	

	Zona de riesgo Representa la zona en la que se encuentra el riesgo, a la que se enfrenta inicialmente un proceso o la entidad, en ausencia de controles. **ZONA DE RIESGO BAJA, MODERADA, ALTA O EXTREMA**	Líder del proceso – Jefe oficina TIC
Identificación de controles	Opciones de manejo del riesgo Representa las posibilidades que se tienen para administrar el riesgo, por medio de controles.	Líder del proceso – Jefe oficina TIC
	Descripción del control	Líder del

	Cuáles son los controles que realiza la entidad para mitigar el riesgo inherente.	proceso – Jefe oficina TIC
	Responsable de ejecutar el control.	Líder del proceso – Jefe oficina TIC
Riesgo residual	Probabilidad Representa la probabilidad residual, de materialización del riesgo, una vez evaluados los controles establecidos para mitigar la probabilidad de que se efectué el riesgo inherente. 1. **RARO:** El evento puede ocurrir solo en circunstancias excepcionales. No se ha presentado en los últimos 5 años. 2. **IMPROBABLE:** El evento puede ocurrir en algún momento. Al menos 1 vez en los últimos 5 años. 3. **POSIBLE:** El evento podría ocurrir en algún momento. Al menos 1 vez en los últimos 2 años. 4. **PROBABLE:** El evento probablemente ocurrirá en la mayoría de las circunstancias. Al menos 1 vez en el último año. 5. **CASI SEGURO:** Se espera que el evento ocurra en la mayoría de las circunstancias. Más de 1 vez al año.	Líder del proceso – Jefe oficina TIC

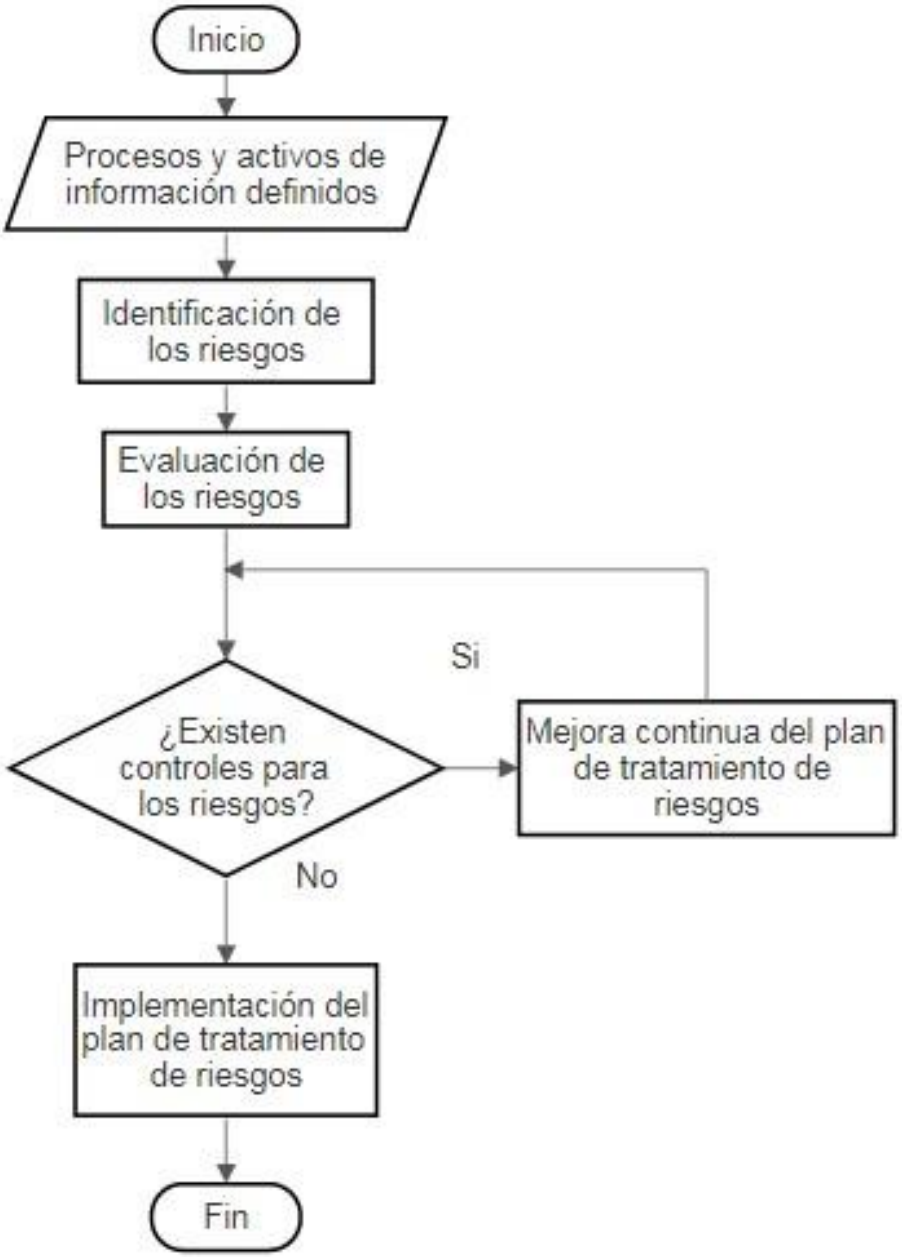
	Impacto	Líder del proceso – Jefe oficina TIC
	Representa el impacto de materialización del riesgo, una vez evaluados los controles establecidos para mitigar la probabilidad de que se efectué el riesgo inherente. Se evalúa en 5 categorías: 1. **INSIGNIFICANTE:** Si el hecho llegara a presentarse, tendría consecuencias o efectos mínimos sobre la entidad. 2. **MENOR:** Si el hecho llegara a presentarse, tendría bajo impacto o efecto sobre la entidad. 3. **MODERADO:** Si el hecho llegara a presentarse, tendría medianas consecuencias o efectos sobre la entidad. 4. **MAYOR:** Si el hecho llegara a presentarse, tendría altas consecuencias o efectos sobre la entidad. 5. **CATASTRÓFICO:** Si el hecho llegara a presentarse, tendría desastrosas consecuencias o efectos sobre la entidad.	
	Zona de Riesgo Residual. Representa la nueva zona de riesgo. **ZONA DE RIESGO BAJA, MODERADA, ALTA O EXTREMA**	Líder del proceso – Jefe oficina TIC

Manejo residual – Plan de Tratamiento de Riesgos	Opciones de manejo del riesgo Esta nueva opción de manejo del riesgo. Representa las posibilidades que se tienen para administrar el riesgo residual, a través de acciones de manejo del riesgo	Líder del proceso – Jefe oficina TIC

	Controles Una vez se han identificado los riesgos, la entidad pública debe definir el tratamiento para cada uno de los riesgos analizados y evaluados, conforme a los criterios y al apetito de riesgo definidos previamente en la Política de Administración de Riesgos Institucional.	Líder del proceso – Jefe oficina TIC
	Actividad Cual(es) es (son) las actividades asociadas al control que va a realizar el proceso para mitigar el riesgo residual	Líder del proceso – Jefe oficina TIC
	Objetivo del control Detallar la razón del control que se va a aplicar al riesgo identificado.	Líder del proceso – Jefe oficina TIC
	Responsable de ejecutar el control Determinar la persona responsable de ejecutar el control a este riesgo.	Líder del proceso – Jefe oficina TIC

	Periodo / Fecha de ejecución	Líder del proceso – Jefe oficina TIC
	Indicador	Líder del proceso – Jefe oficina TIC

6. FLUJOGRAMA



CONTROL DE CAMBIOS

VERSIÓN	FECHA DE APROBACIÓN	DESCRIPCIÓN DEL CAMBIO REALIZADO
01	Noviembre 25 de 2021	Creación del Documento