1. OBJETIVO

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

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

La responsabilidad de este procedimiento recae sobre los miembros del Comité Institucional de Gestión y Desempeño quienes se encargan de identificar, evaluar y gestionar los riesgos de seguridad que afectan a la entidad y debe ser aplicado por los contratistas y funcionarios de la entidad.

4. DEFINICIONES

- **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. DESARROLLO

La matriz de riesgos de seguridad es una herramienta utilizada , para evaluar y gestionar los riesgos relacionados con la seguridad de la información y la seguridad en general.
En términos generales, una matriz de riesgos de seguridad podría incluir los siguientes elementos:
Contexto: Definir el tipo de activo de información

ITEM	EXPLICACIÓN
Proceso	Proceso al que pertenece el activo de información. Esté debe estar aprobado por comité de calidad
Activo de información	Nombre completo del activo de información
Tipo de Activo de Información	Define el tipo de activo de información que presenta el riesgo.

TIPO DE ACTIVO DE INFORMACIÓN	DESCRIPCIÓN	EJEMPLOS
Información y datos de la entidad	Información y datos de la entidad	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 auditoría, entre otros…
Sistemas de información y aplicaciones de Software	Software de aplicación, interfaces, software del sistema, herramientas de desarrollo y otras utilidades relacionadas	Software de aplicación, correo electrónico, sistema operativo, ControlDoc, etc.
Dispositivos de Tecnologías de información – Hardware	Elementos físicos	Servidores, equipos de cómputo, memorias, discos duro, CD´s, etc…
Soporte para el almacenamiento de información	Equipos para almacenamiento deinformación	USB, discos duros, Soporte para el almacenamiento de información CDs, etc…
Servicios	Servicios de computación	Servicios de computación y comunicaciones

Identificación del riesgo: La identificación del riesgo es el proceso de identificar, analizar y comprender las amenazas y oportunidades que pueden afectar en la entidad. Este proceso es fundamental para la gestión de riesgos y ayuda a una entidad a tomar decisiones informadas para mitigar, evitar, transferir o aceptar los riesgos.

ITEM	EXPLICACIÓN
Nro.	Representa un indicador único consecutivo del riesgo.
Riesgo:	Escribir de forma general el riesgo que puede presentar el activo de información
Descripción del Riesgo	Se refiere a las características que presenta el riesgo identificado
Responsable de determinar la materialización del riesgo	Se debe indicar un coordinador responsable del proceso
Amenazas	Analizar que amenazas podría causar la materialización del riesgo
Vulnerabilidades	Analizar las vulnerabilidades que causaría si el riesgo se llega a materializar

Análisis del Riesgo Inherente: es un componente importante de la gestión de riesgos y se refiere a la evaluación de los riesgos antes de que se tomen medidas para mitigarlos o gestionarlos. El objetivo principal del análisis del riesgo inherente es comprender la magnitud de los riesgos tal como se presentan inicialmente, sin considerar aún las medidas de control o mitigación que se puedan aplicar.

ITEM	EXPLICACIÓN
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 número de veces en determinado tiempo.

TABLA DE PROBABILIDAD			
NIVEL	**DESCRIPTOR**	**DESCRIPCIÓN (FACTIBILIDAD)**	**FRECUENCIA**
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 de 1 vez en los últimos 5 años.
3	**POSIBLE**	El evento podría ocurrir en algún momento.	Al menos de 1 vez en los últimos 2 años.
4	**PROBABLE**	El evento probablemente ocurrirá en la mayoría de las circunstancias.	Al menos de 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.

ITEM	EXPLICACIÓN
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 información, de bienes, afectación de la imagen, de la credibilidad y de la confianza, interrupción de servicios, daños ambientales, entre otros

TABLA DE IMPACTO

TIPO	NIVEL	DESCRIPTOR	DESCRIPCIÓN En caso que el riesgo se materialice el impacto u afectación sería……
CONFIDENCIALIDAD EN LA INFORMACIÓN	**1**	**INSIGNIFICANTE**	Se afecta a una persona en particular.
	2	**MENOR**	Se afecta a un grupo de trabajo interno del proceso.
	3	**MODERADO**	Se afecta a todo el proceso.
	4	**MAYOR**	La afectación se da a nivel estratégico.
	5	**CATASTRÓFICO**	La afectación se da a nivel institucional.
CREDIBILIDAD O IMAGEN	**1**	**INSIGNIFICANTE**	Se afecta al grupo de funcionarios y contratistas del proceso.
	2	**MENOR**	Se afecta a todos los funcionarios y contratistas de la entidad.
	3	**MODERADO**	Se afecta a los usuarios de la Sede Central de la entidad.
	4	**MAYOR**	Se afecta a los usuarios de las Direcciones Territoriales.
	5	**CATASTRÓFICO**	Se afecta a los usuarios de la Sede Central y de las Direcciones Territoriales.
LEGAL	**1**	**INSIGNIFICANTE**	Se producen multas para la entidad.
	2	**MENOR**	Se producen demandas para la entidad.
	3	**MODERADO**	Se producen investigaciones disciplinarias.
	4	**MAYOR**	Se producen investigaciones fiscales.

	5	CATASTRÓFICO	Se producen intervenciones y o sanciones para la entidad por parte de un Ente de control u otro Ente regulador.
OPERATIVO	1	INSIGNIFICANTE	Se tendrían que realizar ajustes a una actividad concreta del proceso.
	2	MENOR	Se tendrían que realizar ajustes en los procedimientos del proceso.
	3	MODERADO	Se tendrían que realizar ajustes en la interacción de procesos.
	4	MAYOR	Se presentarían intermitencias o dificultades en la operación del proceso
	5	CATASTRÓFICO	Se presentaría paro o no operación del proceso.

ITEM	EXPLICACIÓN
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		IMPACTO				
		INSIGNIFICANTE	MENOR	MODERADO	MAYOR	CATASTRÓFICO
PROBABILIDAD	VALOR	1	2	3	4	5
RARA VEZ	1					
IMPROBABLE	2					
POSIBLE	3					
PROBABLE	4					
CASI SEGURO	5					

Identificación de Controles: es un paso crucial en la gestión de riesgos. Los son medidas o acciones diseñadas para reducir o mitigar los riesgos identificados durante el análisis de riesgos internos. Estos controles pueden ser preventivos, detectivos o correctivos.

ITEM	EXPLICACIÓN
Opciones de manejo del riesgo	se debe tener en cuenta que en *la guía*, se presenta una clasificación entre dos tipos de Controles **Preventivos:** Son aquellos que actúan para eliminar las causas del riesgo para prevenir su ocurrencia o materialización **Correctivos:** Son aquellos que permiten el restablecimiento de la actividad, después de ser detectado un evento no deseable; también permiten la modificación de las acciones que propiciaron su ocurrencia
Descripción del control	Detallar la razón del control que se va a aplicar al riesgo identificado.
Responsable de ejecutar el control	Determinar la persona responsable de ejecutar el control a este riesgo.(Jefe de Oficina – Secretario - Director)

Riesgo Residual: Se refiere al nivel de riesgo que queda después de que se han implementado medidas de control y mitigación para reducir un riesgo identificado. En otras palabras, es el riesgo que la entidad aún enfrenta incluso después de haber tomado acciones para reducir el riesgo inicial, ya sea mediante la implementación de controles, la transferencia de riesgos o cualquier otro enfoque de gestión de riesgo.(se calcula igual que el **Análisis del Riesgo Inherente**)

MANEJO DEL RIESGO RESIDUAL - Plan de Tratamiento de Riesgos: Es una parte crítica de la gestión de riesgos y está relacionado con el desarrollo de un Plan de Tratamiento de Riesgos. Una vez que se ha calculado el riesgo residual (es decir, el riesgo que queda después de implementar controles), es importante tomar medidas para abordarlo de manera efectiva

ITEM	EXPLICACIÓN
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
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.
Actividad	Cual(es) es (son) las actividades asociadas al control que va a realizar el proceso para mitigar el riesgo residual
Objetivo del control	Detallar la razón del control que se va a aplicar al riesgo identificado
Responsable de ejecutar el control	Determinar la persona responsable de ejecutar el control a este riesgo. (Jefe de Oficina – Secretario - Director)
Periodo / Fecha de Ejecución	Se refiere al período de tiempo durante el cual se lleva a cabo la actividad
Indicador	Es una medida cuantitativa o cualitativa que se utiliza para evaluar y medir el desempeño, el progreso o la situación de un proceso, un proyecto, una organización o cualquier otro aspecto de interés.

6. DOCUMENTOS DE REFERENCIA

MSPI
https://gobiernodigital.mintic.gov.co/seguridadyprivacidad/704/articles162621_Modelo_de_Seguridad_y_Privacidad MSPI.pdf

Guía No 7. Guía de gestión de riesgos
https://www.mintic.gov.co/gestionti/615/articles-5482_G7_Gestion_Riesgos.pdf

CONTROL DE CAMBIOS

VERSIÓN	FECHA DE APROBACIÓN	DESCRIPCIÓN DEL CAMBIO REALIZADO
01	Noviembre 25 de 2021	Creación del Documento
02	25 de Octubre 2023	Se realizan los ajustes de acuerdo a lo establecido en la Guía de gestión de riesgos de MinTIC