



ALCALDÍA DE TULUÁ

PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN.

DICIEMBRE 2022



Tabla de Contenido

INTRODUCCIÓN.....	3
1. OBJETIVOS.....	4
1.1 OBJETIVO GENERAL	4
1.2 OBJETIVOS ESPECIFICOS	4
2. MARCO NORMATIVO	5
3. MARCO TEORICO	6
3.1 SEGURIDAD INFORMÁTICA	6
3.2 NORMA ISO 27001.....	6
3.3 NORMA ISO 27005.....	6
3.4 MODELO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN - MINTIC	7
4.1 PLANEAR	10
4.2 HACER	10
4.3 VERIFICAR.....	10
4.4 ACTUAR	10
5. CRONOGRAMA.....	12



INTRODUCCIÓN

La norma ISO 27005:2011 es un estándar internacional diseñado para la gestión del riesgo en la seguridad de la información dentro de un sistema de gestión de seguridad de la información. Contiene diferentes procedimientos y directrices, que permiten establecer los riesgos que enfrenta una organización y poder mitigarlos de la mejor manera. Se realiza la identificación, el análisis, la evaluación de los riesgos, las políticas y controles que permiten reaccionar ante una posible materialización del riesgo mediante el plan de tratamiento de riesgos.

El no contar con una buena gestión de la seguridad de la información, para la Alcaldía Municipal de Tuluá puede traer consecuencias graves, como pérdida fuga o robo de información, alteración de documentos, negación de servicios etc.

Es muy importante que la alcaldía de Tuluá tenga un plan de tratamiento de riesgos para minimizar pérdidas y maximizar oportunidades. Por este motivo, se ha visto la necesidad de desarrollar un análisis de gestión de riesgo de seguridad de la información aplicado en La Alcaldía Municipal de Tuluá.

El aporte que arroja este plan permite identificar el nivel de riesgo en que se encuentran los activos mediante el nivel de madurez de la seguridad existente y sobre todo incentivar al personal a seguir las respectivas normas y procesos referentes a la seguridad de la información y recursos, todos los servidores público, están en cumplimiento de sus funciones expuestos a riesgos que puedan hacer fracasar una gestión; por tal razón es necesario tomar medidas para identificar las causas y consecuencias de la materialización de dichos riesgos.



1. OBJETIVOS

1.1 OBJETIVO GENERAL

Mitigar los riesgos asociados a la seguridad y privacidad de la información en los procesos de la Alcaldía Municipal de Tuluá Valle, mediante la aplicación de la norma ISO 27005.

1.2 OBJETIVOS ESPECIFICOS

- ❖ Definir la metodología, fases y actividades para la implementación del plan.
- ❖ Identificar los riesgos actuales y sus posibles causas.
- ❖ Establecer controles y políticas de seguridad de la información que garantice la confidencialidad integridad y disponibilidad de la información.

2. MARCO NORMATIVO

Marco Normativo para las TIC		
AÑO	NORMA	TEMA
2014	Ley 1712	"Por medio de la cual se crea la Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional y se dictan otras disposiciones"
2015	Decreto 1078	"Por medio del cual se expide el Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones".
2014	Decreto 2573	"Por el cual se establecen los lineamientos generales de la Estrategia de Gobierno en línea, se reglamenta parcialmente la Ley 1341 de 2009 y se dictan otras disposiciones".
2016	Decreto 415	"Por el cual se adiciona el Decreto Reglamentario del Sector de la Función Pública, Decreto número 1083 de 2015, en lo relacionado con la definición de los lineamientos para el fortalecimiento institucional en materia de Tecnologías de la Información y las comunicaciones".
2009	Ley 1341	"Por la cual se definen Principios y conceptos sobre la sociedad de la información y la organización de las Tecnologías de la Información y las comunicaciones –TIC-, se crea la Agencia Nacional del Espectro y se dictan otras disposiciones".
1994	Ley 152	"Por la cual se establece la Ley Orgánica del Plan de Desarrollo".
1998	Ley 489	"Por la cual se dictan normas sobre la organización y funcionamiento de las entidades del orden nacional, se expiden las disposiciones, principios y reglas generales para el ejercicio de las atribuciones previstas en los numerales 15 y 16 del artículo 189 de la Constitución Política y se dictan otras disposiciones".
2003	Ley 872	(Derogado Ley rama Ejecutiva del poder público y en otras entidades prestadoras de servicios) "Por la cual se crea el sistema de gestión de la calidad en la Rama Ejecutiva del Poder Público y en otras entidades prestadoras de servicios".
2015	Ley 1753	"Por el cual se expide el Plan Nacional de Desarrollo 2014-2018"

3. MARCO TEORICO

3.1 SEGURIDAD INFORMÁTICA

La seguridad Informática y la seguridad de la información son métodos y técnicas físicas y documentales empleadas para mantener siempre la confidencialidad, integridad y disponibilidad de la información.



Fuente: Pilares de la seguridad informática.

3.2 NORMA ISO 27001

La norma ISO 27001 es un estándar internacional que describe cómo implementar el Sistema de gestión de seguridad de la información de una empresa. Investiga como salvaguardar la información mediante una serie de estándares, lineamientos y procesos que facilitan la identificación de los riesgos.

3.3 NORMA ISO 27005

La norma ISO 27005 es un soporte a la norma (ISO 27001) la cual proporciona directrices para la gestión de riesgos de seguridad de la información, es aplicable a todos los tipos de organización y no proporciona ni recomienda una metodología específica.



Las secciones contenidas en la norma ISO 27005 son:

- ❖ Prefacio
- ❖ Introducción
- ❖ Referencias normativas
- ❖ Términos y definiciones
- ❖ Estructura
- ❖ Fondo
- ❖ Descripción general del proceso de ISRM
- ❖ Establecimiento de contexto
- ❖ Evaluación de riesgos de seguridad de la información (ISRA)
- ❖ Tratamiento de riesgos de seguridad de la información
- ❖ Seguridad de la información Aceptación del riesgo
- ❖ Seguridad de la información Comunicación de riesgos
- ❖ Seguridad de la información Monitoreo y revisión de riesgos
- ❖ Anexo A: Definición del alcance del proceso
- ❖ Anexo B: Valoración de activos y evaluación de impacto
- ❖ Anexo C: ejemplos de amenazas típicas
- ❖ Anexo D: Vulnerabilidades y métodos de evaluación de vulnerabilidad
- ❖ Anexo E: enfoques ISRA"

3.4 MODELO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN - MINTIC:

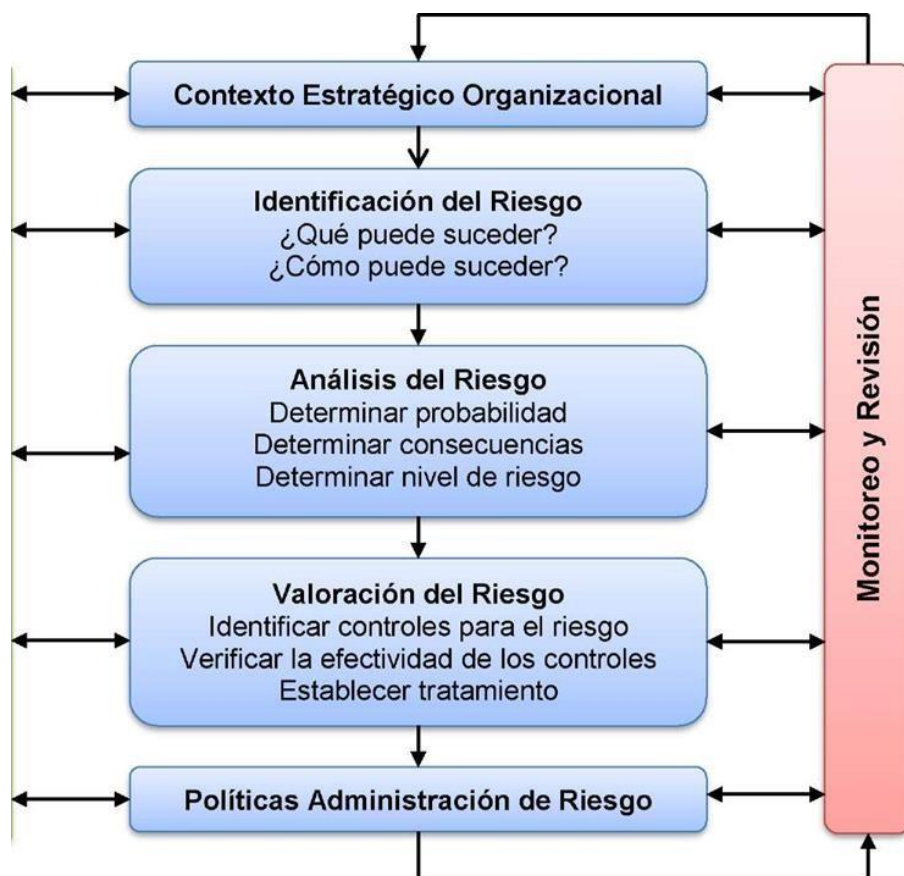
Recopilación de las mejores prácticas, nacionales e internacionales, para suministrar requisitos para el diagnóstico, planificación, implementación, gestión y mejoramiento continuo, del Modelo de Seguridad y Privacidad de la Información - MSPI de la Estrategia de Gobierno en Línea - GEL.

3.5 GUÍA DE GESTIÓN DE RIESGOS - MINTIC:

Permite la alineación de los objetivos estratégicos de la Entidad, al desarrollo del MSPI para lograr una integración con lo establecido a través de la guía de Riesgos del DAFP, así como con lo determinado en otros modelos de Gestión por ejemplo el MECI.

En la siguiente figura se muestra el procedimiento de la guía 7 que propone el departamento administrativo de la función pública (DAFP) junto con el ministerio de la

tecnología de información y comunicación (MinTIC) para la gestión de riesgos informáticos.



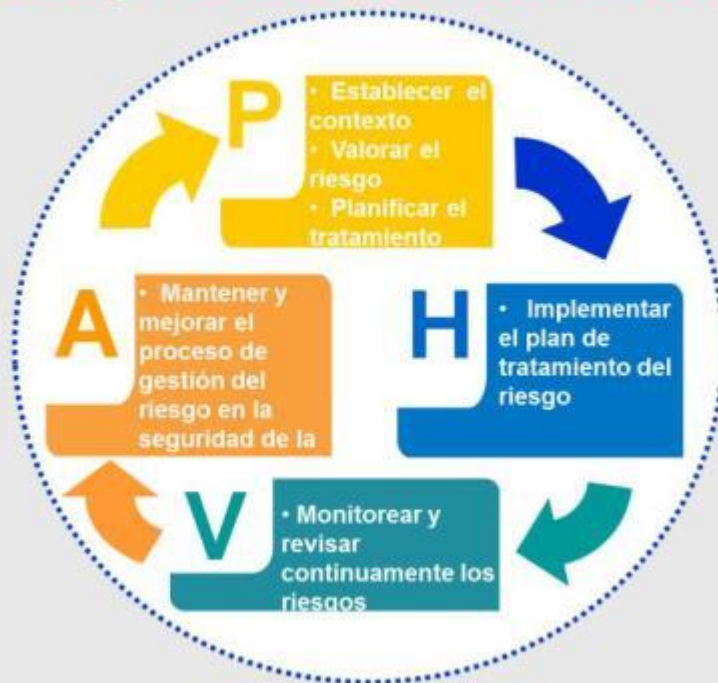
Fuente: Guía para la administración del riesgo – DAFP

3.6 MODELO PHVA PARA EL SGSI (PLANEAR, HACER, VERIFICAR, ACTUAR):

Un SGSI establece una serie de procesos y lineamientos que se deben seguir mediante la estandarización de la norma ISO 27001 para asegurar los activos de información como Bases de datos, oficios, actas etc. de una organización. El objetivo es mantener siempre la confidencialidad, integridad y disponibilidad de la información.

El ciclo PHVA logra enmarcar la gestión del riesgo dentro de la seguridad de la información, que se establece en el Modelo de Seguridad y Privacidad de la Información - MSPI, así:

El SGSI y la Gestión del Riesgo



Fuente Tomada de NTC-ISO/IEC 27005 Gestión de Riesgos

4. FASES DE IMPLEMENTACIÓN

La alta dirección debe adquirir el compromiso de facilitar el cumplimiento de los objetivos sobre la gestión del riesgo de seguridad y privacidad de la información, a través del establecimiento de políticas, roles y responsabilidades, y la designación de recursos necesarios para que el proceso se desarrolle en la institución de forma efectiva.

4.1 PLANEAR

Abarca los Pasos 1, 2 y 3 de la Guía para la Administración de los Riesgo de Gestión, Corrupción y Seguridad Digital y el Diseño de Controles en Entidades Públicas, emitida por la Función Pública.

4.2 HACER

Con los insumos de la ejecución de la fase anterior, se ejecuta la ruta crítica definida, es decir, se implementan los planes de tratamiento de riesgos definidos. Aquí la Línea Estratégica debe cumplir con el compromiso de brindar los recursos necesarios para iniciar el tratamiento de los riesgos.

El responsable de seguridad digital deberá supervisar y acompañar el proceso de implementación de los planes de tratamiento, verificando que los responsables de los planes.

4.3 VERIFICAR

Monitoreo y revisión a través de las tres líneas de defensa definidas en el MIPG en la Dimensión 7 Control Interno, de los planes de tratamiento para determinar su efectividad.

4.4 ACTUAR

Mejoramiento continuo de la gestión del riesgo de seguridad digital, se debe garantizar la mejora continua de la gestión de riesgos de seguridad digital, por lo tanto, debe establecer que cuando existan hallazgos, falencias o incidentes de seguridad digital se debe mitigar el impacto de su existencia y tomar acciones para

controlarlos y prevenirlos. Adicionalmente, se debe establecer y hacer frente a las consecuencias propias de la no conformidad que llegó a materializarse.

6. DEFINIR ALCANCE

• IDENTIFICACIÓN DE LOS ACTIVOS DE INFORMACION

En esta fase se establece los objetivos, justificación del procedimiento que se va a realizar, los funcionarios implicados y el contexto de seguridad informática con el que cuenta la Alcaldía Municipal.

El principal activo de una organización es la información en sí, la cual puede estar en forma física como documentos impresos o escritos a mano, en medios electrónicos almacenados en Discos Duros Externos, Memorias USB o en forma digital, en los equipos de cómputo o en la Nube. Toda esta información requiere ser analizada para su protección. (Un activo es todo aquello que genera valor para una empresa u organización.)

Para ello el equipo de soporte nivel 1 llevaron a cabo el inventario de activos de información el cual es elemento clave para proceder a implementar el documento.

Tabla 2: Evaluación de Integridad

Nivel	Descripción Criterio de Confidencialidad	Denominación
0	Información que puede ser conocida y utilizada sin autorización por cualquier persona, sea empleado de la Alcaldía o no	Público
1	Información que puede ser conocida y utilizada por todos los empleados de la Alcaldía y algunas entidades externas debidamente autorizadas, y cuya divulgación o uso no autorizados podría ocasionar riesgos o pérdidas leves para la Alcaldía, el Sector Público Nacional o terceros.	Reservada – Uso Interno

2	Información que sólo puede ser conocida y utilizada por un grupo de empleados, que la necesiten para realizar su trabajo, y cuya divulgación o uso no autorizados podría ocasionar pérdidas significativas a la Alcaldía o a terceros.	Reservada - Confidencial
3	Información que sólo puede ser conocida y utilizada por un grupo muy reducido de empleados, generalmente de la alta dirección de la Alcaldía, y cuya divulgación o uso no autorizados podría ocasionar pérdidas graves al mismo o a terceros.	Reservada Secreta

Tabla 2: Evaluación de Integridad

Nivel	Descripción Criterio de Integridad
0	Información cuya modificación no autorizada puede repararse fácilmente, o no afecta la operatoria de la Alcaldía.
1	Información cuya modificación no autorizada puede repararse, aunque podría ocasionar pérdidas leves para la Alcaldía o terceros
2	Información cuya modificación no autorizada es de difícil reparación y podría ocasionar pérdidas significativas para la Alcaldía o terceros.
3	Información cuya modificación no autorizada no podría repararse, ocasionando pérdidas graves a la Alcaldía o a terceros.

Tabla 3: Evaluación de Disponibilidad.

Nivel	Descripción Criterio de Disponibilidad
0	Información cuya inaccesibilidad no afecta la operatoria de la Alcaldía.
1	Información cuya inaccesibilidad permanente durante una semana podría ocasionar pérdidas significativas para la Alcaldía o terceros.
2	Información cuya inaccesibilidad permanente durante un día podría ocasionar pérdidas significativas a la Alcaldía o a terceros.
3	Información cuya inaccesibilidad permanente durante una hora podría ocasionar pérdidas significativas a la Alcaldía o a terceros.

• IDENTIFICACIÓN DEL RIESGO

El objetivo de la identificación de riesgos es conocer los incidentes o eventos que pueden causar pérdidas o alteración en el funcionamiento de la Alcaldía municipal de Tuluá y pueden afectar la confidencialidad, integridad y disponibilidad de la información.

La identificación de los riesgos se realiza con observación directa, ingeniería social y con el análisis a los equipos de seguridad perimetral. Por confidencialidad de la Alcaldía municipal de Tuluá se presenta la identificación de riesgos general.

Tabla 4: Identificación de Riesgos Informáticos.

RIESGOS INFORMÁTICOS	CAUSAS	EFEECTO
Perdida Robo o Fuga de Información	<ul style="list-style-type: none"> -Fallas en el proceso de copia de respaldo o de restauración de la información, o pérdida de la misma. -Fallas en los análisis y socialización de las vulnerabilidades de la infraestructura de IT -No contar con acuerdos de confidencialidad con los empleados y terceros -Falta de autorización para la extracción de información generadas por requerimientos. -Ingreso a la red y acceso a los activos de TI por parte de máquinas ajenas a la entidad -Habilitación de puertos USB en modo lectura y escritura para medios de almacenamiento -Ataques cibernéticos internos o externos - Empleados no capacitados en los temas de riesgos informáticos. -Desconocimiento del riesgo. -Prestar los equipos informáticos a personal no autorizado. -No cerrar sesión cuando se desplaza del puesto 	<ul style="list-style-type: none"> -Afectación parcial o total de la continuidad de las operaciones de los servicios del Incumplimiento normativo - Vulneración de los sistemas de seguridad operando actualmente -Mala imagen, multas, sanciones y pérdidas económicas -Generación de consultas, funcionalidades o reportes con información sensible de los clientes -Pérdida o fuga de información

RIESGOS INFORMÁTICOS	CAUSAS	EFFECTO
	<ul style="list-style-type: none"> -Acceso no autorizado a las dependencias. -Conectar dispositivos externos a los equipos. -Falta de implementación de la política escritorio limpio 	
Correos electrónicos de extraña procedencia	<ul style="list-style-type: none"> -Empleados no capacitados en los temas de riesgos informáticos. - Desconocimiento del riesgo. - No generar una Cultura de Seguridad de la Información - Falta de Filtros en el Servidor de Correo - Programas de DLP (Data Lost Prevention) - Falta de instalación de EndPoint (programa seguridad punto final) en las estaciones de trabajo. 	<ul style="list-style-type: none"> -Cifrado de la información. - Captura de las pulsaciones del teclado. - Monitoreo de las actividades realizadas en el equipo. - Ataque remoto mediante un troyano o gusano. - Robo de contraseñas. - Equipo usado como Zombie para BotNet (usado para atacar otros DDoS) - Robo de documentos y/o archivos. - Sistema con mal funcionamiento.
Daño en los equipos tecnológicos	<ul style="list-style-type: none"> -Manejo inadecuado de los equipos - Falta de mantenimiento o mala conexión de los mismos en las instalaciones eléctricas - Falta de equipos de potenciación - Fallas por defectos de fabrica - Derrame de líquido - Falta de ambiente adecuado para los equipos - Falta Educación a los usuarios en el manejo de los equipos de computo 	<ul style="list-style-type: none"> -Perdida de información - Perdidas de los quipos informáticos - Indisponibilidad del Servicio - Traumatismos en los procesos
Dumpsterdiving (buceo en la basura)	<ul style="list-style-type: none"> -Desconocimiento del riesgo. -Falta de capacitación y conciencia. 	<ul style="list-style-type: none"> -Creación de perfil de ataque - Captura de información privilegiada
RIESGOS INFORMÁTICOS	CAUSAS	EFFECTO
Perdida de conectividad	<ul style="list-style-type: none"> -Daño externo del ISP (Internet service provider) -Ataque DDoS o DOS (denegación de servicios distribuidos o Denegación de servicios) 	

Ataques Informáticos	-Estimulo o Reto personal -Rebelión -Ánimo de lucro -Espionaje	-Daño en los equipos tecnológicos -incidente en la confidencialidad, integridad y disponibilidad de la información -Denegación de servicios -Secuestro de la información - Divulgación ilegal de la información -Suplantación de identidad -Destrucción de la información -Soborno de la información
-----------------------------	---	---

• IDENTIFICACIÓN DE LAS AMENAZAS

Tabla 5: Identificación de Amenazas

AMENAZA	TIPO
Polvo, Corrosión	Evento Naturales
Inundación	Evento Naturales
Incendios	Evento Naturales
Fenómenos Sísmicos	Evento Naturales
Fenómenos Térmicos	Evento Naturales y Daños físicos
Perdida en el suministro de energía	Daño Físico
Espionaje remoto	Acciones no autorizadas
Ingeniería Social	Acciones no autorizadas
Intrusión	Acciones no autorizadas
Accesos forzado al sistema	Acciones no autorizadas
Manipulación del Hardware	Acciones no autorizadas
Manipulación con Software	Acciones no autorizadas
Fallas del equipo	Fallas técnicas
Saturación del sistema de información	Fallas técnicas

• IDENTIFICACIÓN DE LAS VULNERABILIDADES

Las vulnerabilidades son las Fallas o debilidades en un sistema, que puede ser explotada por quien la conozca. Cuando la amenaza encuentra la vulnerabilidad es cuando se crea el riesgo. Por eso es necesario conocer la lista de amenazas y el inventario de activos de información.

Tabla 6: Identificación de Vulnerabilidades

VULNERABILIDADES	DESCRIPCIÓN
Fácil acceso a las dependencias o Secretarías.	No existe un control para el acceso de las personas no autorizadas a las secretarías.
Falta de dispositivos de seguridad biométrica para acceso a las secretarías de alto riesgo.	El dispositivo de seguridad biométrica reduce el riesgo de robo de información o equipos electrónicos por fácil acceso.
Falta de Aplicación de la Política de escritorio Limpio.	La política de escritorio limpio, es implementada para que los funcionarios no dejen expuestos: documentos, equipos electrónicos u objetos de valor, sobre los escritorios, que pueden ser robados fácilmente
Falta de máquina trituradora de papel	La máquina trituradora de papel, evita que las personas arrojen documentos importantes con información personal a la basura, que puedan ser usados para crear perfiles de ataque.
Falta de Capacitación de los funcionarios en temas de seguridad Informática.	El eslabón más débil en términos de seguridad informática en una organización son los funcionarios, dado que no tienen conocimiento sobre las amenazas y riesgos que enfrentan y como poder mitigarlos.
Falta de equipos electrónicos para copias de respaldo.	El no contar con un HDD externo, impide a los funcionarios realizar copias de respaldo o Back ups
Falta de equipos institucionales.	El no contar con suficientes equipos institucionales, lleva a los funcionarios a traer equipo personal que pueden afectar el funcionamiento de la red o infectarla. Adicionalmente promueve el compartir cuentas de usuarios y claves que pueden afectar al prestador
Equipo clon.	Los equipos clon, no cuentan con software legal que pueden infectar la red o traer problemas legales



- **IDENTIFICACIÓN DE CONTROLES EXISTENTES**

La identificación de los controles existentes permite realizar la evaluación de riesgos. Los controles garantizan que al momento de la materialización de un riesgo se reduzcan o mitiguen los riesgos informáticos y la organización funcionen correctamente. Pero se debe tener en cuenta que nunca se va a estar 100% seguros.

Dada la importancia de los controles, con que cuenta la Alcaldía Municipal de Tuluá no es adecuado exponerlos en el proyecto, por lo que se pueden crear perfiles de ataque.

- **EVALUACIÓN DE RIESGO**

La evaluación de riesgo se realiza con enfrentamiento entre la probabilidad de ocurrencia y el impacto que genera el riesgo en los activos de información, dado por la matriz de calificación, evaluación y respuestas a los riesgos.

- **ANÁLISIS DEL RIESGO**

El análisis del riesgo busca establecer la probabilidad de ocurrencia del mismo y sus consecuencias, calificándolos y evaluándolos con el fin de obtener información para establecer el nivel de riesgo.

Se han establecido dos aspectos a tener en cuenta en el análisis de los riesgos identificados, probabilidad e impacto. Por la primera se entiende la posibilidad de ocurrencia del riesgo; esta puede ser medida con criterios de Frecuencia, si se ha materializado, o de Factibilidad teniendo en cuenta la presencia de factores internos y externos que pueden propiciar el riesgo, aunque éste no se haya materializado. Por Impacto se entiende las consecuencias que puede ocasionar a la Entidad la materialización del riesgo. La etapa de análisis de los riesgos se divide en:

✓ **Calificación del riesgo:**

Se logra a través de la estimación de la probabilidad de su ocurrencia y el impacto que puede causar la materialización del riesgo. La primera representa el número de veces que el riesgo se ha presentado en un determinado tiempo o puede presentarse, y la segunda se refiere a la magnitud de sus efectos.

Para la determinación de la calificación del riesgo, con base en la probabilidad y el impacto se debe tener en cuenta las siguientes tablas:

Escala para calificar la probabilidad del riesgo		
Nivel	Concepto	Frecuencia
Raro	El evento puede ocurrir solo en circunstancias excepcionales.	No se ha presentado en los últimos 5 años.
Improbable	El evento puede ocurrir en algún momento.	Al menos de 1 vez en los últimos 5 años.
Moderado	El evento podría ocurrir en algún momento.	Al menos de 1 vez en los últimos 2 años.
Probable	El evento probablemente ocurrirá en la mayoría de las circunstancias.	Al menos de 1 vez en el último año.
Casi certeza	Se espera que el evento ocurra en la mayoría de las circunstancias.	Más de 1 vez al año.

Escala para calificar el impacto del riesgo							
Tipos de efecto o impacto		a) Estratégico	b) Operativo	c) Financieros	d) Cumplimiento	e) Tecnología	f) Imagen
INSIGNIFICANTE	Si el hecho llegara a presentarse, tendría consecuencias o efectos mínimos o bajos	Afecta el cumplimiento de algunas actividades	Genera ajustes a una actividad concreta	La pérdida financiera no afecta la operación normal de la institución	Genera un requerimiento	Afecta a una persona o una actividad del proceso	Afecta a un grupo de servidores del proceso
MENOR	Si el hecho llegara a presentarse, tendría bajo impacto o efecto	Afecta el cumplimiento de las metas del proceso	Genera ajustes en los procedimientos	La pérdida financiera afecta algunos servicios administrativos	Genera investigaciones disciplinarias, fiscales y/o penales	Afecta el proceso	Afecta a los servidores del proceso
MODERADO	Si el hecho llegara a presentarse tendría medianas consecuencias o	Afecta el cumplimiento de las metas de un grupo de procesos	Genera ajustes o cambios en los procesos	La pérdida financiera afecta considerablemente la prestación del servicio	Genera interrupciones en la prestación del bien o servicio	Afecta varios procesos de la institución	Afecta a todos los servidores de la institución
MAYOR	Si el hecho llegara a presentarse	Afecta el cumplimiento de las	Genera intermitencia en el	La pérdida financiera afecta	Genera sanciones	Afecta a toda la	Afecta el



Tuluá

de la gente para la gente

	tendría altas consecuencias o efectos	metas	servicio	considerablemente el presupuesto		entidad	sector
CATASTRÓFICO	Si el hecho llegara a presentarse tendría desastrosas consecuencias o efectos	Afecta el cumplimiento de las metas del sector y del gobierno	Genera paro total de la institución	Afecta al presupuesto de otras entidades	Genera cierre definitivo de la institución	Afecta al Departamento o	Afecta al Departamento, Gobierno, Todos los usuarios

Para la definición del impacto se debe tener en cuenta la clasificación del riesgo (Estratégico, operativo, financieros, cumplimiento, tecnología, imagen) de acuerdo con la clase del riesgo y la magnitud del impacto se debe determinar el nivel en el que se encuentra.

✓ Evaluación del riesgo

Permite comparar los resultados de la calificación, con los criterios definidos para establecer el grado de exposición al riesgo; de esta forma, se define la zona de ubicación del riesgo inherente (antes de la definición de controles). La evaluación del riesgo se calcula con base en variables cuantitativas y cualitativas.

PROBABILIDAD	IMPACTO				
	Insignificante	Menor	Moderado	Mayor	Catastrófico
Raro	B	B	B	M	M
Improbable	B	M	M	A	A
Moderado	B	M	A	A	E
Probable	M	A	A	E	E
Casi certeza	M	A	E	E	E

Color	Zona de riesgo
B	Zona de riesgo baja
M	Zona de riesgo moderada
A	Zona de riesgo alta
E	Zona de riesgo extrema

Con la evaluación del riesgo, previa a la formulación de controles se obtiene la ubicación del riesgo en la matriz de evaluación; esto se denomina evaluación del riesgo inherente.

✓ Desarrollo práctico – Análisis

Formato de Análisis de riesgos, el cual hace parte del proceso Administración del Modelo Integrado de Planeación y Gestión MIPG, donde se debe relacionar la siguiente información:

- **Riesgo:** Relacionar el riesgo redactado en el formato Identificación de riesgos
- **Calificación de probabilidad:** de acuerdo con la información cuantitativa y cualitativa.
- **Calificación de impacto:** de acuerdo con la información cuantitativa y cualitativa.
- **Clasificación del riesgo:** Ver componentes de la identificación del riesgo, en el apartado de clasificación de los riesgos.
- **Evaluación:** surge del cruce de los resultados cuantitativos de la calificación para probabilidad e impacto;

✓ MANEJO DE RIESGOS

Una vez determinada la zona donde está ubicado el riesgo, y dependiendo de las opciones de manejo, se deben formular las acciones orientadas al mejoramiento y fortalecimiento de los controles identificados. Las acciones que se definan para el manejo del riesgo deben contemplar:

- Corregir las fallas identificadas en los controles según la evaluación realizada a cada uno.
- Reforzar o fortalecer los controles existentes.

Si la evaluación del riesgo residual, lo ubica en la zona baja no se deben formular acciones de manejo, el manejo estará únicamente enfocado en garantizar que los controles previamente establecidos operan de manera adecuada. Los riesgos ubicados en las zonas moderada, alta o extrema, exigen realizar acciones que fortalezcan los puntos débiles identificados en la evaluación de los controles.

✓ Desarrollo práctico – Manejo del riesgo

La información correspondiente al plan de manejo se debe registrar en el formato Manejo del riesgo. Siguiendo el desarrollo de la Matriz de Riesgos con el apoyo del Departamento de Planeación Municipal.

• SEGUIMIENTO DE RIESGOS

Cada cuatro meses Control Interno realizará seguimiento a todo el componente de administración de riesgos y verificará aspectos como:

- Cumplimiento de las políticas y directrices para la administración del riesgo: metodología de Administración del Riesgo (diseño y funcionamiento).
- Administración de los riesgos por proceso e institucionales: calificación y evaluación, efectividad de los controles y cumplimiento de las acciones.

Aspecto para tener en cuenta:

Los resultados de la evaluación y las observaciones de la persona que haga las veces de Control Interno deben ser presentados a la Alta Dirección, para que se tomen las decisiones pertinentes que garanticen la sostenibilidad de la Administración del Riesgo en la Alcaldía municipal de Tuluá.

Grupo Objetivo	Estrategia de divulgación	Responsable
Alta Dirección	Talleres de Socialización	Director del Departamento Administrativo TIC
Comunidad en general	Publicación en el sitio web de la Alcaldía	Director del Departamento Administrativo TIC