ALCALDÍA DE TULUÁ

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

Tabla de Contenido

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 perdidas 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 riegos.

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:

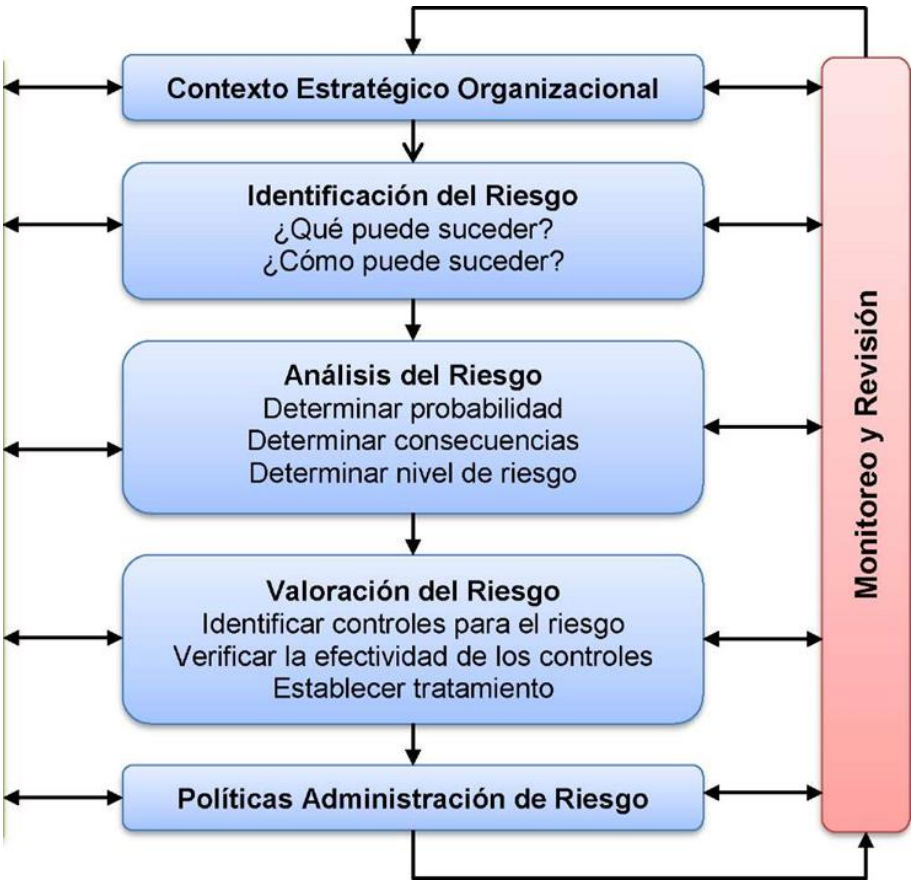
Recopilación de las mejores prácticas, nacionales e internacionales, para suministrar requisitos para el diagnóstico, planificación, implementación, gestión y mejoramiento continuo, del Modelo de Seguridad y Privacidad de la Información - MSPI de la Estrategia de Gobierno en Línea - GEL.

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, **H**ACER, **V**ERIFICAR, **A**CTUAR):

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:

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.

5. CRONOGRAMA

Actividad	Mes 1	Mes 2	Mes 3	Mes 4	Mes 5	Mes 6	Mes 7	Mes 8
Definición del contexto interno, externo y de los procesos de la entidad pública.								
Definición de la política de administración de riesgo.								
Designación de roles y responsabilidades.								
Definición de criterios de probabilidad, impacto y zonas de riesgo aceptable.								
Identificación de activos.								
Identificación de riesgos.								
Valoración de riesgos.								
Definición del tratamiento de los riesgos.								