

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

OFICINA TIC | Tecnologías de la Información y las Comunicaciones

TABLA DE CONTENIDO

INTRODUCCIÓN	3
OBJETIVOS	4
ALCANCE	4
DEFINICIONES.....	4
MARCO NORMATIVO	5
VISION GENERAL PARA ADMINISTRACIÓN DEL RIESGO DE SEGURIDAD DE LA INFORMACIÓN.....	6
METODOLOGÍA PHVA.....	7
PLAN DE TRATAMIENTO DE RIESGOS	7

Calle 14 # 21-32 Barrio Cooperativo. Código Postal: 507001 PBX: 3203509652. Línea de Atención al Usuario: 01 8000 112 996 Correo Electrónico: tic@acacias.gov.co Página Web: www.acacias.gov.co Twitter: @Alcaldiaacacias Facebook: Alcaldía de Acacias

INTRODUCCIÓN

La Alcaldía Municipal de Acacias, presenta a las partes interesadas el plan de tratamiento de riesgos de la seguridad y privacidad de la información, en el que determina la información como uno de los activos más importantes de la entidad, basado en la gestión de riesgos, preservando la confidencialidad, integridad y disponibilidad de la información permitiendo mitigar posibles afectaciones a los activos que apoyan al cumplimiento de los objetivos de la Administración Municipal.

Así mismo, este plan contempla la importancia de realizar medidas de control y evaluación que contribuyan a gestionar y reducir las vulnerabilidades a las cuales se encuentra expuesta la entidad, por medio de la matriz de seguridad digital que contempla la asignación de valores y atributos a la probabilidad de ocurrencia de una amenaza afectando la seguridad de los activos de información, al igual que los valores y atributos sobre el impacto que afectan a la Alcaldía de Acacias, producto de la materialización de los riesgos. Adicionalmente, en la matriz se encuentran identificados los controles existentes y la evaluación del riesgo residual que necesariamente debe ser gestionada a través de implementación de controles propuestos en el tratamiento de los riesgos. Lo anterior dando cumplimiento a la normativa establecida por el estado colombiano, CONPES 3854 de 2016, Modelo de Seguridad y Privacidad de MINTIC y lo establecido en el decreto 1008 de 14 de junio 2018.

OBJETIVOS

OBJETIVO GENERAL

- Controlar y minimizar los riesgos de seguridad de la información pertenecientes a la Alcaldía Municipal de Acacias

OBJETIVOS ESPECIFICOS

- Brindar protección a los activos de información mediante la implementación de acciones eficaces y seguras en la Alcaldía de Acacias
- Hacer seguimiento a los riesgos en los procesos de la Alcaldía de Acacias, que puedan afectar la integridad, confidencialidad y disponibilidad de la información
- Cumplir con los requisitos legales y reglamentarios pertinentes a la legislación colombiana

ALCANCE

El plan de tratamiento de riesgos tiene alcance para todos procesos de la Alcaldía de Acacias, en concordancia con las normatividades vigentes nacionales en seguridad y privacidad de la información.

DEFINICIONES

Riesgo: Es un escenario bajo el cual una amenaza puede explotar una vulnerabilidad generando un impacto negativo al negocio evitando cumplir con sus objetivos.

Amenaza: Es un ente o escenario interno o externo que puede hacer uso de una vulnerabilidad para generar un perjuicio o impacto negativo en la institución (materializar el riesgo).

Vulnerabilidad: Es una falencia o debilidad que puede estar presente en la tecnología, las personas o en las políticas y procedimientos.

Probabilidad: Es la posibilidad de la amenaza aproveche la vulnerabilidad para materializar el riesgo.

Impacto: Son las consecuencias que genera un riesgo una vez se materialice.

Control o Medida: Acciones o mecanismos definidos para prevenir o reducir el impacto de los eventos que ponen en riesgo, la adecuada ejecución de las actividades y tareas requeridas para el logro de objetivos de los procesos de una entidad.

MARCO NORMATIVO

Decreto 1078 de 2015	Por medio del cual se expide el Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones
Decreto 1008 de 2018	Por el cual se establecen los lineamientos generales de la política de Gobierno Digital y se subroga el capítulo 1 del título 9 de la parte 2 del libro 2 del Decreto 1078 de 2015, Decreto Único Reglamentario del sector de Tecnologías de la información y Comunicaciones.
Manual para la Implementación de la Política de Gobierno Digital	Implementación de la política de Gobierno Digital. Decreto 1008 de 2018 (Compilado en el Decreto 1078 de 2015, capítulo 1, título 9, parte 2, libro 2) Versión 7, abril de 2019.
Modelo de Seguridad y privacidad de la información -MSP	Se encuentra alineado con el Marco de Referencia de Arquitectura TI y soporta transversalmente los otros componentes de la Política de Gobierno Digital, TIC para el Estado y TIC para la Sociedad, que son habilitados por tres elementos transversales: Seguridad de la Información, Arquitectura y Servicios Ciudadanos Digitales.



VISION GENERAL PARA ADMINISTRACIÓN DEL RIESGO DE SEGURIDAD DE LA INFORMACIÓN

- Proceso para la administración del riesgo en seguridad de la información

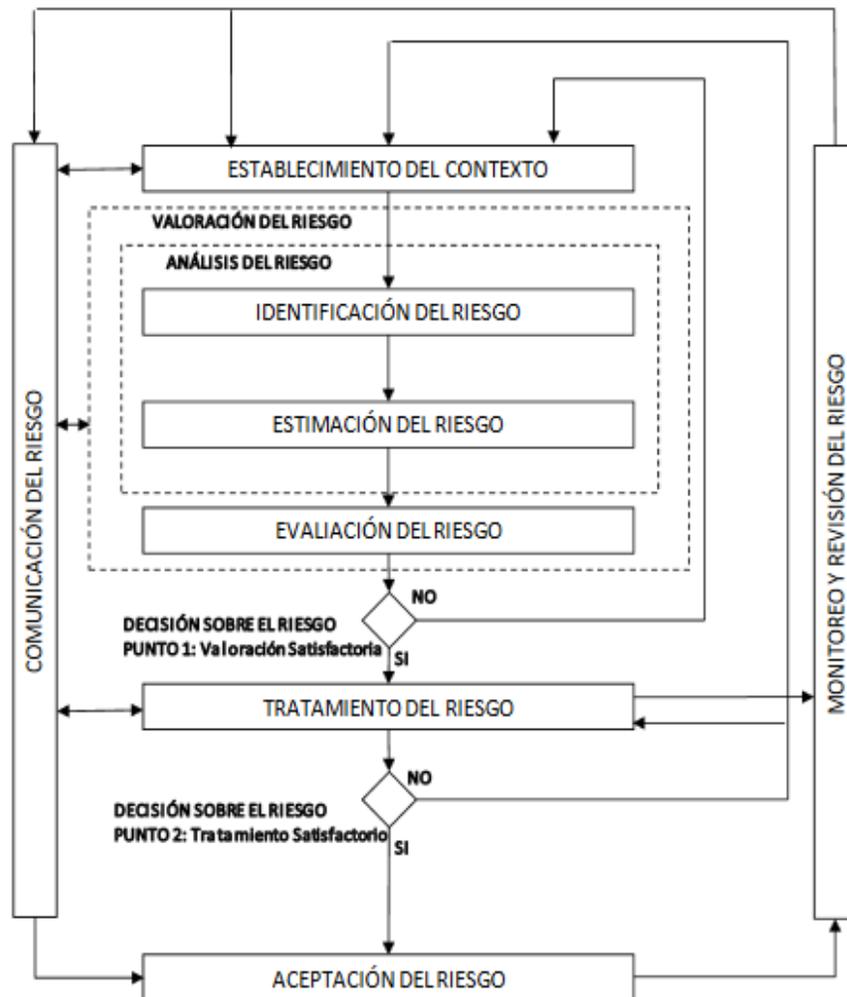


Imagen 1. Tomado de la NTC-ISO/IEC 27005

METODOLOGÍA PHVA

Las actividades de gestión del riesgo en la seguridad de la información para las cuatro fases del proceso de Modelo de seguridad y privacidad de la información, toma como base la metodología PHVA y los lineamientos emitidos por MINTIC.

ETAPAS DEL MSP	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 Continuo de los Riesgos
Mejora Continua	Mantener y Mejorar el Proceso de Gestión del Riesgo en la seguridad de la información.

Tabla 1. Etapas de la Gestión del Riesgo a lo Largo del MSP

PLAN DE TRATAMIENTO DE RIESGOS

El Plan de Tratamiento de Riesgos contempla la definición de las actividades a desarrollar en aras de mitigar los riesgos sobre los activos, estas actividades se estructuraron de la siguiente manera:

No	Actividad	Fecha de Inicio	Fecha Final	Responsable	Producto o resultado esperado
1	Actualización metodología de Riesgos de Seguridad y Privacidad.	01-Feb-2022	18-Abr-2022	Profesional Oficina TIC/ Profesional Gobierno Digital/ Profesional SPI	GTIC - F - 37 Mapa de Riesgos de Seguridad Digital V4
2	Información sobre la evaluación de riesgos de seguridad.	19-Abr-2022	29-Jul-2022	Profesional Oficina TIC/ Profesional Gobierno Digital/ Profesional SPI	Comunicaciones internas / Correo electrónico



No	Actividad	Fecha de Inicio	Fecha Final	Responsable	Producto o resultado esperado
3	Identificación y Análisis de Riesgos Seguridad de la información	01-Mar-2022	30-Dic-2022	Profesional Oficina TIC/ Profesional Gobierno Digital/ Profesional SPI	GTIC - F - 37 Mapa de Riesgos de Seguridad Digital V4
4	Publicación de riesgos de seguridad de información	02-May-2022	30-Dic-2022	Profesional Oficina TIC/ Profesional Gobierno Digital/ Profesional SPI	Link de transparencia
5	Tratamiento de Riesgos Seguridad de la Información	01-Mar-2022	30-Dic-2022	Profesional Oficina TIC/ Profesional Gobierno Digital/ Profesional SPI	Actas de reunión / correos electrónicos
6	Información de seguridad Seguimiento de Riesgos y Revisión-Informe	01-Ago-2022	30-Dic-2022	Profesional Oficina TIC/ Profesional Gobierno Digital/ Profesional SPI	Informe de riesgos

DOCUMENTOS Y REGISTROS RELACIONADOS

Código	Nombre
GTIC-F-37	Mapa de Riesgos de Seguridad Digital V4
GSIG-F-33	Actas de Reunión

CONTROL DE CAMBIOS

Fecha de Aprobación	Código	Versión	Descripción y Razón del Cambio
28/01/2021	GTIC-PL-10	1	Creación del Documento
26/01/2022	GTIC-PL-10	2	Actualización del plan

ELABORÓ	REVISÓ	APROBÓ
Nombre: RODOLFO DÍAZ CLAVIJO Cargo: Profesional Universitario	Nombre: ESTHER RODRÍGUEZ GARAVITO Cargo: Profesional Especializado SIG	Nombre: EDILBERTO ROMERO T Cargo: Jefe Oficina TICS