Municipio de Guatapé
Departamento de Antioquia

@alcguatape

2024

Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información

MUNICIPIO DE GUATAPÉ - ANTIOQUIA

PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN
2024

DAVID ESTEBAN FRANCO VALLEJO
Alcalde Municipal

CARLOS HERNAN ESPINOSA CORREA
Secretario de Gobierno y Servicios Administrativos

MARTHA NURY CARDONA GARCIA
Técnico Operativo en Gestión Documental

FICHA DEL DOCUMENTO

Título	**PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN**
Sumario	Este documento tiene por objeto definir y aplicar los lineamientos para tratar de manera integral los riesgos de Seguridad y Privacidad de la Información a los que el Municipio de Guatapé pueda estar expuesto, en procura de proteger y preservar la integridad, confidencialidad, disponibilidad, privacidad y autenticidad de la información
Palabras claves	Seguridad, Privacidad, Confidencialidad, Municipio de Guatapé. Riesgos, amenazas, vulnerabilidad, activos de información
Formato	PDF
Dependencia	Gestión Documental
Autor (es)	Martha Nury Cardona García
Revisó	Carlos Hernán Espinosa Correa
Fecha de aprobación	Enero 29 de 2024
Versión aprobada	5.0
Idioma	Español

TABLA DE CONTENIDO

Contenido

1. INTRODUCCION

A través de la elaboración del Plan de Tratamiento de Riesgos se busca plantear medidas para mitigar los riesgos presentes en su análisis (perdida de confidencialidad, perdida de integridad y perdida de disponibilidad de los activos de información) evitando situaciones que generen incertidumbre en el cumplimiento de los objetivos institucionales.

Gestionar correctamente la seguridad de la información y riesgos de seguridad digital de los sistemas de información de la entidad, así como en los activos que participan en sus procesos y que se encuentran expuestos, permite garantizar la confidencialidad, integridad y disponibilidad de la información a través de la aplicación de las opciones apropiadas de tratamiento de riesgos de Seguridad de la información y seguridad digital, teniendo en cuenta la evaluación de los resultados de la valoración de los riesgos del Sistema de Gestión de Seguridad de la Información y en concordancia a la normativa aplicable.

Con la ejecución de este Plan se implementan de controles y acciones tendientes a la mitigación de los riesgos del proceso de gestión tecnológica, hallazgos de auditorías internas y apoya el cumplimiento del Modelo integrado de planeación y gestión del MINTIC,dentro de su política de gobierno Digital.

2. OBJETIVOS

2.1 Objetivo General

Definir y aplicar los lineamientos para tratar de manera integral los riesgos de Seguridad y Privacidad de la Información a los que el Municipio de Guatapé pueda estar expuesto, en procura de proteger y preservar la integridad, confidencialidad, disponibilidad, privacidad y autenticidad de la información

2.2 Objetivos Específicos

- Actualizar el inventario de activos de información de la entidad
- Actualizar el mapa de riesgos de información de la entidad.
- Definir los controles que permitan disminuir los valores de exposición del riesgo.
- Sensibilizar a los funcionarios y contratistas en temas relacionados con el tratamiento de los riesgos.

3. ALCANCE

Realizar una eficiente gestión de riesgos de seguridad y privacidad de la información, de acuerdo a los lineamientos emitidos por el Ministerio de Tecnologías de la Información y las Comunicaciones y el departamento administrativo de la función pública, que permita integrar en los procesos de la entidad, buenas prácticas que contribuyan a la toma de decisiones y prevenir incidentes que puedan afectar el logro de los objetivos.

4. 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 las Comunicaciones
CONPES 3854 de 2016	Política Nacional de Seguridad Digital
Manual para la Implementación	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

de la Política de Gobierno Digital	
NTC / ISO 27001:2013	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. TIC, que son habilitados por tres elementos transversales: Seguridad de la Información, Arquitectura y Servicios Ciudadanos Digitales Página 4 de 12 NTC / ISO 27001:2013 Tecnología de la información. Técnicas de seguridad. Sistemas de gestión de la seguridad de la información (SGSI).
NTC/ISO 31000:2009	Gestión del Riesgo. Principios y directrices

Tabla 1. Marco Normativo

5. DEFINICIONES

- ✓ **Activo**: cualquier elemento que tenga valor para la organización.
- ✓ **Análisis del riesgo**: Se estima el riesgo con el fin de proporcionar bases que logre laevaluación y la naturaleza del riesgo.
- ✓ **Contexto externo:** Ambiente externo en el cual la organización busca alcanzar susobjetivos (tecnológico, legal, regional, etc.).
- ✓ **Contexto interno**: Ambiente interno en el cual la organización busca alcanzar susobjetivos (gobierno, políticas, estructura organizacional, etc.).
- ✓ **Riesgo aceptable**: Riesgo en que la organización decide que puede convivir y/o soportar dado a sus obligaciones legales, contractuales y/o intereses propios.
- ✓ **Riesgo residual**: Nivel de riesgo que permanece luego de tomar medidas de tratamiento.
- ✓ **Riesgo**: Posibilidad **de riesgos**: Términos de referencia frente a los cuales se evaluará laimportancia del riesgo.
- ✓ **Evaluación del Riesgo**: Comparar los resultados del análisis de riesgo frente a loscontroles implementados, con el fin de determinar el riesgo final.
- ✓ **Evento**: Posible ocurrencia de Incidente o amenaza de Seguridad de la Información.
- ✓ **Fuente**: Elemento que por sí solo o en combinación tiene el potencial intrínseco paradar lugar a riesgo; a fuente del riesgo puede ser tangible o intangible.
- ✓ **Gestión del riesgo**: Actividades coordinadas para dirigir y controlar una organizacióncon respecto al riesgo.
- ✓ **Riesgo de seguridad digital**: combinación de amenazas y vulnerabilidades en el entorno digital. Puede debilitar el logro de objetivos económicos y sociales, así como afectar la soberanía nacional, la integridad territorial, el orden constitucional y los intereses nacionales. Incluye aspectos relacionados con el ambiente físico, digital y laspersonas.

6. DESARROLLO METODOLÓGICO

La Organización Internacional de Normalización (ISO), define los riegos comoo “la posibilidad de que una amenaza determinada explote las vulnerabilidades

de un activo o grupo de activos y por lo tanto causa daño a la organización".

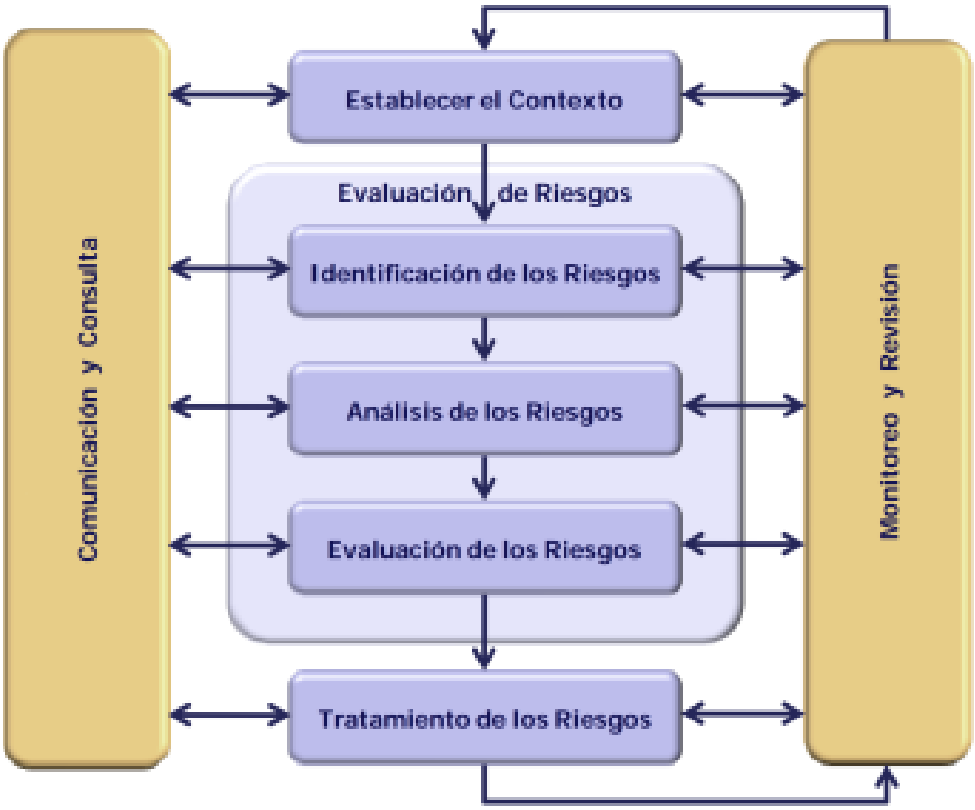

Imagen 1. Proceso para gestión de riesgos
Fuente: Norma ISO 27001

6.1 CONTEXTO ESTRATÉGICO

A partir del contexto es posible establecer las posibles causas de los riesgos a identificar..

Aunque la protección de la información digital se ve amenazada frecuentemente por errores cometidos por los usuarios, en la Alcaldía de Guatapé se han identificado algunos factores que afectan directamente la seguridad de la información.

- La red de interna ha mejorado debido a que se implementó nueva infraestructura con más puntos de red y servidor y la señal se torna débil o no llega a algunas oficinas y por seguridad se separó la red LAN de la red wifi.

- Se han dispuesto nuevos puntos de red según se han ido presentando las necesidades.

- No se ha construido la política de seguridad y privacidad de la de la información y por ello no se tienen muy claras las reglas básicas del cuidado tanto de los equipos informáticos y como de la información física y digital, algunas son:

  - ✓ Bebidas y alimentos cerca a los equipos de cómputo, cualquier derrame de líquidos afectan los activos de información y de informática.
  - ✓ En algunos papeles reutilizables se encontró información que debe ser reservada, identificándose la falta de confidencialidad y privacidad.
  - ✓ En algunas secretarías de la alcaldía no existen los equipos de cómputo suficientes para el uso de la totalidad de su personal. Existe un riesgo de pérdida de información ya que deben compartir los recursos informáticos.
  - ✓ La información es llevada en memorias o discos duros portátiles personales, por ende la información sale de la entidad.
  - ✓ No hay control para el uso de memorias portátiles en los equipos de la Alcaldía, exponiendo a perder la información por virus no detectados o daños irreparables del hardware.

Una vez ejecutado el presente plan se tendrá un diagnóstico más acertado del contexto estratégico de la entidad, precisando cuál será el contexto en el que se desenvolverá, qué procesos involucrará, cual es el flujo de dicho o dichosprocesos, y de ésta forma identificar sus objetivos y finalmente, de allí obtener los riesgos de Seguridad asociados.

6.2 IDENTIFICACION Y ESTIMACION DEL RIESGO

El objetivo es **d**eterminar los factores que causen pérdida potencial, y llegar a comprender el cómo, donde, y por qué podría ocurrir.

Dentro de las actividades para identificar los riesgos, la entidad establecerá las causas internas y/o externas, y establecerá los activos críticos para asociarlos a los procesos correspondientes y de allí generar el listado de procesoscríticos.

Los riesgos se pueden clasificar en estratégicos, de imagen, operativos, financieros, de cumplimiento y tecnológicos, de acuerdo a clasificación propuesta por el DAFP

Riesgo Estratégico: Se asocia con la forma en que se administra la Entidad. El manejo del riesgo estratégico se enfoca a asuntos globales relacionados con la misión y el cumplimiento de los objetivos estratégicos, la clara definición de políticas, diseño y conceptualización de la entidad por parte de la alta gerencia.
Riesgos de Imagen: Están relacionados con la percepción y la confianza por parte de la ciudadanía hacia la institución.
Riesgos Operativos: Comprenden riesgos provenientes del funcionamiento y operatividad de los sistemas de información institucional, de la definición de los procesos, de la estructura de la entidad, de la articulación entre dependencias.
Riesgos Financieros: Se relacionan con el manejo de los recursos de la entidad que incluyen: la ejecución presupuestal, la elaboración de los estados financieros, los pagos, manejos de excedentes de tesorería y el manejo sobre los bienes.
Riesgos de Cumplimiento: Se asocian con la capacidad de la entidad para cumplir con los requisitos legales, contractuales, de ética pública y en general con su compromiso ante la comunidad.
Riesgos de Tecnología: Están relacionados con la capacidad tecnológica de la Entidad para satisfacer sus necesidades actuales y futuras y el cumplimiento de la misión.

Tabla 2: Clasificación de los riesgos.
Fuente: Guía de Riesgos DAFP

6.3 EVALUACIÓN DEL RIESGO

Dentro de tratamiento de los riesgos es fundamental realizar la evaluación de los riesgos y aunque hay varias metodologías para dicha evaluación, para el Municipio de Guatapé se aplicará la metodología sugerida por la Norma ISO 27001

Las fases de esta metodología son los siguientes:

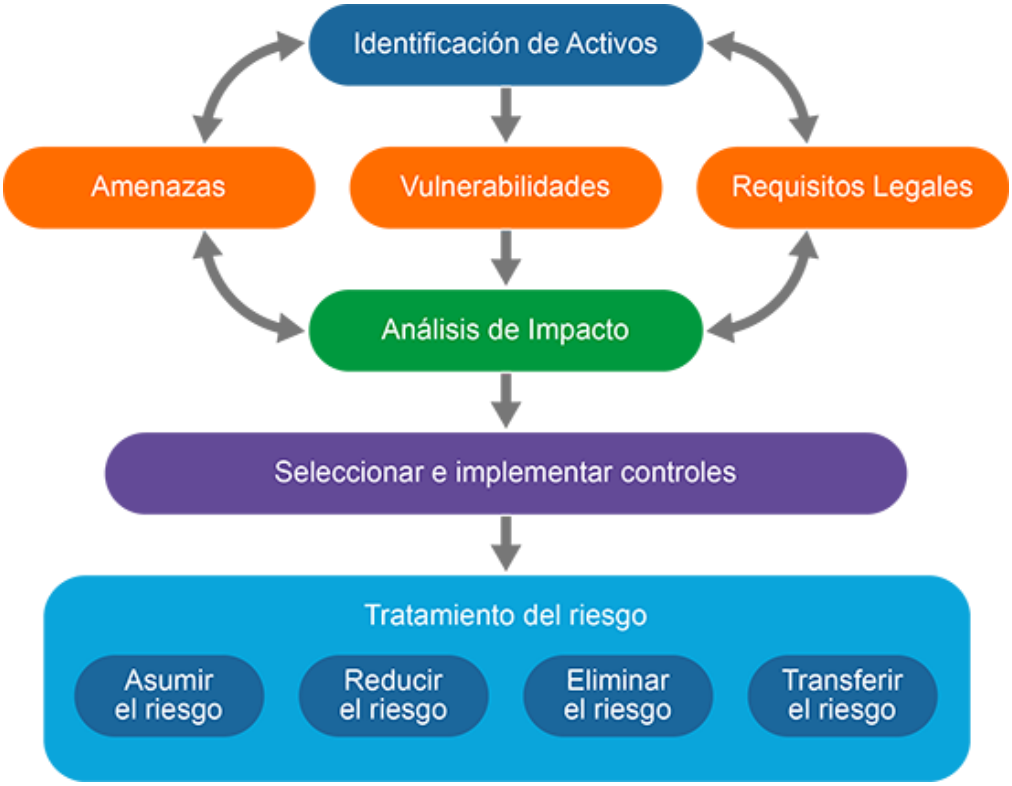

Imagen 2. Proceso para la evaluación del riesgos informativo.
Fuente: Norma ISO 27001

6.3.1 Establecer los Activos de Información:

Consiste en identificar los activos y sus responsables, entendiendo por activo todo aquello que tiene valor para la organización, incluyendo soportes físicos (edificios o equipamientos), intelectuales o informativas (Ideas, aplicaciones, proyectos …) así como la marca, la reputación etc.

La identificación del inventario de activos de información, permite clasificar los activos a los que se les debe brindar mayor protección, pues identifica claramente sus características y rol al interior de un proceso.

Imagen 5. Clasificación de Activos de Información
Fuente: ISO 27001 disponible en https://es.linkedin.com/pulse/la-clasificaci%C3%B3n-y-gesti%C3%B3n-de-activos-informaci%C3%B3n-binaps-suite

6.3.2 Identificar las Vulnerabilidades:

Se deben identificar para cada activo: aquellas debilidades propias del activo que lo hacen susceptible de sufrir ataques o daños.

Para realizar una correcta identificación de vulnerabilidades es necesario conocer la lista de amenazas comunes, la lista de inventario de activos y el listado de controles existentes.

6.3.3 Identificar las amenazas:

Son aquellas cosas que puedan suceder y dañar el activo de la información, tales como desastres naturales, incendios o ataques de virus, espionaje etc.

Considerando que las amenazas pueden ser de origen natural o humano y podrían ser accidentales o deliberadas, se recomiendaidentificar todos los orígenes de las amenazas accidentales como deliberadas.)

Algunas amenazas pueden afectar a más de un activo y en tales casos pueden causar diferentes impactos dependiendo de los activos que se vean afectados.

Es recomendable tener particular atención a las fuentes de amenazas humanas. Estas se desglosan específicamente en la siguiente tabla:

FUENTE DE AMENAZA	MOTIVACION	ACCIONES AMENAZANTES
Pirata informático, intruso ilegal	RebeliónEstatus Dinero	● Piratería ● Ingeniería Social ● Intrusión, accesos forzados al sistema ● Acceso no autorizado
Criminal de la computación	Destrucción de la información, Divulgación ilegal de la información Ganancia monetaria Alteración no autorizada de losdatos	● Crimen por computador ● Acto fraudulento ● Soborno de la información ● Suplantación deidentidad ● Intrusión en el sistema
Terrorismo	Chantaje Destrucción Explotación Venganza Ganancia política Cubrimiento de losmedios de comunicación	● Bomba/Terrorismo ● Guerra de la información ● Ataques contra elsistema DDoS ● Penetración en el sistema ● Manipulación en el sistema
Espionaje industrial(inteligencia empresas, gobiernos	Ventaja competitiva Espionaje económico	● Ventaja de defensa ● Ventaja política ● Explotación económica

Tabla 3. Lista de amenazas humanas.
Fuente: MINTIC: Seguridad y Privacidad de la Información, Guía de Gestión de riesgos, Nro 7.2016

6.3.4 Cálculo del riesgo:

Este se realiza a partir de la probabilidad de ocurrencia del riesgo y el impacto que este tiene sobre la organización (Riesgo = impacto x probabilidad de la amenaza). Con este procedimiento determinamos los riesgos que deben ser controlados con prioridad.

Una vez identificados los activos, el municipio procederá a levantar la matriz de Calificación, Evaluación y respuesta del Riesgos:

PROBABILIDAD	IMPACTO				
	Insignificante (1)	Menor (2)	Moderado (3)	Mayor (4)	Catastrófico (5)
Raro (1)	B	B	M	A	A
Improbable (2)	B	B	M	A	E
Posible (3)	B	M	A	E	E
Probable (4)	M	A	A	E	E
Casi Seguro (5)	A	A	E	E	E

B: Zona de riesgo Baja: Asumir el riesgo
M: Zona de riesgo *Moderada*: Asumir el riesgo, Reducir el riesgo
A: Zona de riesgo *Alta*: Reducir el riesgo, Evitar, Compartir o Transferir
E: Zona de riesgo *Extrema*: Reducir el riesgo, Evitar, Compartir o Transferir

Imagen 6. Matriz de Calificación, Evaluación y respuesta del Riesgos
Fuete: Guía de Riegos DAFP

7. MONITOREO Y REVISION DE INDICADORES

Esta fase se realiza con uno indicadores que están orientados principalmente a determinar el porcentaje de ejecución de las actividades plantadas en el Plan de tratamiento de riesgos de seguridad de la información.

8. CRONOGRAMA DE ACTIVIDADES

Como actividades del Plan para el tratamiento de los riesgos de seguridad y privacidad de la información se plantean las siguientes actividades:

ACTIVIDAD	RESPONSABLE	2024 TRIMESTRES				INDICADOR
		I	II	III	IV	
Actualizar el Inventario de Activos de Información	Responsable de los Sistemas Informáticos					Documento actualizado con el Inventario de Activos de Información y publicado en la página web de la entidad.
Actualización del Mapa de Riesgos de seguridad y privacidad de la Información	Responsable de los Sistemas Informáticos					Mapa de riesgos de información actualizado.
Sensibilizar a los funcionarios y contratistas en temas relacionados con el tratamiento de los riesgos de información	Responsable TIC					Capacitación a funcionarios sobre riesgos informáticos Formula Nro de capacitaciones realizadas*100/Nro de Capacitaciones proyectadas
Implementar controles para el tratamiento de riesgos de privacidad y seguridad de la información.	Responsable TIC					Controles implementados
Monitoreo y Revisión de Indicadores	Responsable TIC -Gestión Documental					Informe final de ejecución del Plan de Tratamiento de Seguridad Y Privacidad de la Informacion
TOTAL						

Tabla 4. Mapa de Ruta

9. BIBLIOGRAFIA

- ✓ Guía de Gestión de Riesgos. Seguridad y Privacidad de la Información. Ministerio de las Tic, 2016. Disponible en https://www.mintic.gov.co/gestionti/615/articles-5482_G7_Gestion_Riesgos.pdf

- ✓ Guía para la Gestión y Clasificaciónde Activos de Información. Seguridad y Privacidad de la Información. Ministerio de las Tic, 2016. Disponible en https://www.mintic.gov.co/gestionti/615/articles-5482_G5_Gestion_Clasificacion.pdf

CONTROL DE CAMBIOS

Fecha	Versión	Descripción
Enero/2020	1	Versión inicial del documento
Enero/2021	2	Actualización de Plan
Enero/2022	3	Actualización del Plan
Enero/ 2023	4	Actualización del Plan
Enero/2024	5	Actualización del Plan por cambio de vigencia