Plan
de Tratamiento de Riesgos de Seguridad y Privacidad de la Información
2023

@AlcGuatape

JUAN PÉREZ
Alcalde

Guatapé Emprende

Alcaldía de Guatapé

MUNICIPIO DE GUATAPE – ANTIOQUIA

PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN 2023

JUAN SEBASTIAN PEREZ FLOREZ
Alcalde Municipal

DANIELA GUARÍN CARDONA
Secretaria de Gobierno y Servicios Administrativos

MARTHA NURY CARDONA GARCÍA
Técnico Operativo Gestión Documental

FICHA DEL DOCUMENTO

Titulo:	**PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN**
Sumario:	Este documento tiene por objeto Desarrollar e implementar el Plan de tratamiento de Riesgos de Seguridad y Privacidad de la Información del Municipio de Guatapé, en busca de minimizar los riesgos de pérdida de activos de la información en la alcaldía Municipal de Guatapé, mediante la implementación de un plan de tratamiento de gestión de riesgos de seguridad y privacidad de la información institucional
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:	Daniela Guarín Cardona
Fecha de Aprobación:	23 de enero de 2023
Versión aprobada:	4.0
Idioma	Español

Contenido

1. INTRODUCCION

Administrar eficientemente 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.

La adecuada gestión de los riesgos reduce las pérdidas y brindan protección de la información, permitiendo conocer las debilidades que afectan durante todo el ciclo de vida del servicio.

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

Minimizar los riesgos de pérdida de activos de la información en la alcaldía Municipal de Guatapé, mediante la implementación de un plan de tratamiento de gestión de riesgos de seguridad y privacidad de la información institucional

2.2 Objetivos Específicos

- Identificar los activos de información y determinar aquellos s que se les debe brindar mayor protección.
- Levantar la matriz de calificación, evaluación y respuesta a los riesgos para identificar los riesgos que deben ser controlados con prioridad.
- Realizar la Matriz de clasificación y valoración de los controles para definir controles que permitan disminuir los valores de exposición del riesgo.
- Identificar los riesgos asociados a los procesos y los activos de información y construir el mapa de riesgos
- Capacitar los funcionarios y contratistas en temas relacionados con el tratamiento de los riesgos

3. ALCANCE

El plan pretende fortalecer la implementación de acciones para el tratamiento 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, direccionados siempre a la seguridad informática de la plataforma tecnológica del Municipio de Guatapé frente a posibles ciber-amenazas.

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 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
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.
- **Causa**: Elemento específico que origina el evento.
- **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.).
- **Controles**: Procesos, políticas y/o actividades que pueden modificar el riesgo.
- **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. GESTIÓN DE RIESGOS

La definición estandarizada de riesgo proviene de la Organización Internacional de Normalización (ISO), definiéndolo como “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”.

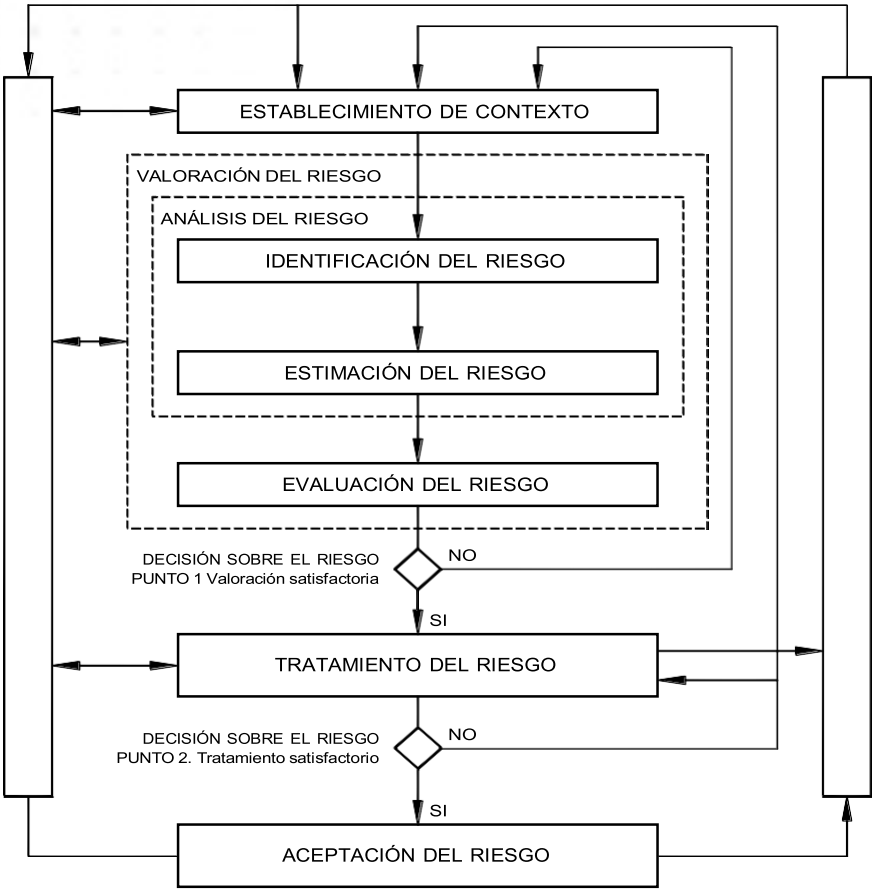

Imagen 1. Proceso para gestión de riesgos de acuerdo
Fuente: Norma ISO 27001

6.1 CONTEXTO ESTRATÉGICO

Aunque la protección de la información digital se ve amenazada frecuentemente por errores cometidos por los usuarios, en la Alcaldía de Guatapé se han identificados 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 dichos procesos, 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

6.2.1 Identificar 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.

Para la identificación de los activos de Información se tendrán en cuenta las recomendaciones datas por MINTIC por ello se considerarán los criterios de Confidencialidad, Integridad y Disponibilidad de acuerdo a la siguiente calificación:

CONFIDENCIALIDAD	INTEGRIDAD	DISPONIBILIDAD
INFORMACIÓN PUBLICA RESERVADA	ALTA (A)	ALTA (1)
INFORMACIÓN PUBLICA CLASIFICADA	MEDIA (M)	MEDIA (2)
INFORMACIÓN PÚBLICA	BAJA (B)	BAJA (3)
NO CLASIFICADA	NO CLASIFICADA	NO CLASIFICADA

Imagen 3. Criterios de clasificación.
Fuente: Guia Nro 5 para la Gestión y Clasificación de Activos de Información. MNTIC-2016

ALTA	Activos de información en los cuales la clasificación de la información en dos (2) o todas las propiedades (confidencialidad, integridad, y disponibilidad) es alta.
MEDIA	Activos de información en los cuales la clasificación de la información es alta en una (1) de sus propiedades o al menos una de ellas es de nivel medio.
BAJA	Activos de información en los cuales la clasificación de la información en todos sus niveles es baja.

Imagen 4. Niveles de Clasificación.
Fuente: Guía Nro 5 para la Gestión y Clasificación de Activos de Información. MNTIC-2016

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.

Las actividades a realizar para obtener un inventario de activos son Definición, Revisión, Actualización y Publicación, las cuales se reflejan documentalmente en laMatriz de Inventario y Clasificación de Activos de Información

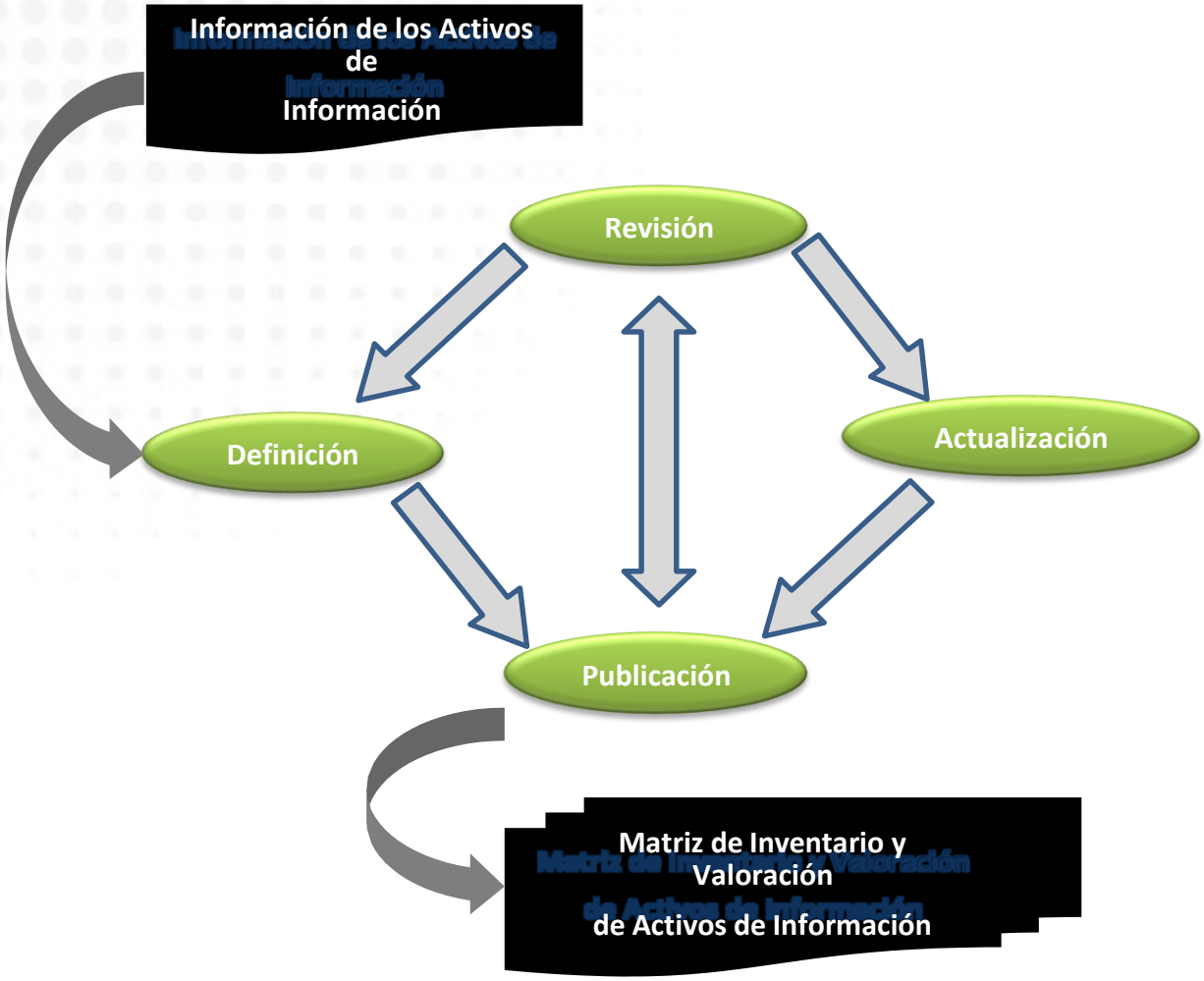

Imagen 5. Procedimiento para el Inventario de Activos
Fuente: Guía Nro 5 Guía para la Gestión y Clasificaciónde Activos de Información. MNTIC-2016

6.2.2 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.

A continuación, se enuncian vulnerabilidades conocidas y métodos para la valoración de la misma

TIPO DE ACTIVO	EJEMPLOS DE VULNERABILIDADES	EJEMPLOS DE AMENAZAS
HARDWARE	Mantenimiento insuficiente/Instalación fallida de los medios de almacenamiento	Incumplimiento en el mantenimiento del sistema de información.
	Susceptibilidad a la humedad, el polvo y la suciedad	Polvo, corrosión y congelamiento
	Sensibilidad a la radiación electromagnética	Radiación electromagnética
	Ausencia de un eficiente control de cambios en laconfiguración	Error en el uso
	Susceptibilidad a las variaciones de voltaje	Pérdida del suministro de energía
	Susceptibilidad a las variaciones de temperatura	Fenómenos meteorológicos
	Almacenamiento sin protección	Hurtos medios o documentos.
	Falta de cuidado en ladisposición final	Hurtos medios odocumentos.
	Copia no controlada	Hurtos medios o documentos.
SOFTWARE	Ausencia o insuficiencia de pruebas de software	Abuso de los derechos
	Defectos bien conocidos en el software	Abuso de los derechos
	Ausencia de “terminaciónde sesión” cuando se abandona la estación de trabajo	Abuso de los derechos
	Disposición o reutilización de los medios de almacenamiento sinborrado adecuado	Abuso de los derechos
	Asignación errada de losderechos de acceso	Abuso de los derechos
	Software ampliamente distribuido	Corrupción de datos
	En términos de tiempo utilización de datos errados en los programas de aplicación	Corrupción de datos
	Interfaz de usuario compleja	Error en el uso
	Ausencia de documentación	Error en el uso
	Configuración incorrecta de parámetros	Error en el uso
	Fechas incorrectas	Error en el uso
	Ausencia de mecanismos de identificación y autentificación, como la autentificación de usuario	Falsificación de derechos
	Tablas de contraseñas sin protección	Falsificación de derechos
	Gestión deficiente de lascontraseñas	Falsificación de derechos
	Habilitación de servicios innecesarios	Procesamiento ilegal de datos

	Software nuevo o inmaduro	Mal funcionamiento del software
	Especificaciones incompletas o no claraspara los desarrolladores	Mal funcionamiento del software
	Ausencia de control de cambios eficaz	Mal funcionamiento del software
	Descarga y uso no controlado de software	Manipulación con software
	Ausencia de copias de respaldo	Manipulación con software
	Ausencia de protecciónfísica de la edificación, puertas y ventanas	Hurto de medios o documentos
	Fallas en la producción de informes de gestión	Uso no autorizado del equipo
RED	Ausencia de pruebas deenvío o recepción de mensajes	Negación de acciones
	Líneas de comunicación sin protección	Escucha encubierta
	Tráfico sensible sin Protección	Escucha encubierta
	Conexión deficiente delos cables	Fallas del equipo de telecomunicaciones
	Punto único de fallas	Fallas del equipo de telecomunicaciones
	Ausencia de identificación y autentificación de emisory receptor	Falsificación de derechos
	Arquitectura insegura dela red	Espionaje remoto
	Transferencia de contraseñas en claro	Espionaje remoto
	Gestión inadecuada de la red (tolerancia a fallas enel enrutamiento)	Saturación del sistemade información
	Conexiones de red pública sin protección	Uso no autorizado del equipo
PERSONAL	Ausencia del personal	Incumplimiento en la disponibilidad del personal
	Procedimientos inadecuados de contratación	Destrucción de equipos y medios
	Entrenamiento insuficiente en seguridad	Error en el uso
	Uso incorrecto de software y hardware	Error en el uso
	Falta de conciencia acerca de la seguridad	Error en el uso
	Ausencia de mecanismos demonitoreo	Procesamiento ilegal de los datos
	Trabajo no supervisado del personal externo o delimpieza	Hurto de medios o documentos.
	Ausencia de políticas para el uso correcto de los medios de telecomunicaciones y mensajería	Uso no autorizado del equipo
ORGANIZAC	Ausencia de auditorias	Abuso de los derechos

IONAL	Ausencia de procedimientos de identificación y valoración de riesgos	Abuso de los derechos
	Ausencia de reportes de fallas en los registros de administradores y operadores	Abuso de los derechos
	Respuesta inadecuadade mantenimiento del servicio	Incumplimiento en el mantenimiento del sistema de información
	Ausencia de procedimientos de control de cambios	Incumplimiento en el mantenimiento del sistema de información
	Ausencia de procedimiento formal para la documentacióndel MSPI	Corrupción de datos
	Ausencia de asignación adecuada de responsabilidades en seguridad de la información	Negación de acciones
	Ausencia de planes de continuidad	Falla del equipo
	Ausencia de políticas sobre el uso de correo electrónico	Error en el uso
	Ausencia de procedimientos para introducción del software en los sistemasoperativos	Error en el uso
	Ausencia de procedimientos del cumplimiento de las disposiciones con los derechos intelectuales.	Uso de software falsificado o copiado

Tabla 3: Lista de Vulnerabildiadedes.
Fuente: MINTIC: Seguridad y Privacidad de la Información, Guía de Gestión de riesgos, nro. 7, 2016

A continuación, se relacionan los posibles aspectos que generan vulnerabilidad en los activos de información:

VULNERA-BILIDAD	DESCRIPCIÓN	CAUSA	EFECTO	CLASIFICA-CIÓN
*Fallas eléctricas	Las conexiones no son suficiente. No cumplen con las exigencias. La infraestructura de la red se debe actualizar(hay cables sueltos, puntos de red que no funcionan)	Se han creado nuevos puestos de trabajo	Posible pérdida de la información	Riesgo tecnológico. Riesgo físico Riesgo humano
Afectación de activos de información y	Desconocimiento de las políticas y normas de	Falta de socialización.	Acciones no adecuadas en el tratamiento de	Riesgo tecnológico

activos informáticos	seguridad de la información	Falta de capacitación de la políticas y normas de seguridad	los activos de información e informáticos	Riesgo en el servicio. Riesgo de la información Riesgo en personal
Pérdida de tiempo o productivo en funciones laborales	La red implementada no es la adecuada para la estructura física y la cantidad de equipos informáticos. Las fallas en la señal de internet	Red inalámbrica ya que no hay suficientes puntos para cableado	Señal débil en oficinas. Retraso en los procesos	Riesgo tecnológico Riesgo en el servicio. Riesgo de la información Riesgo en personal
Incumplimiento de las actividades de seguridad de la información	El personal encargado de sistemas no es suficiente. No se siguen protocolos y normas para garantizar la seguridad de la información en la entidad.	No existe personal encargado del proceso de aseguramiento de la información	Ausencia de transferencia de conocimiento y falta de capacitación	Riesgo tecnológico Riesgo en el servicio. Riesgo de la información Riesgo en personal
Confidencialidad e integridad de la información	Se trabaja en la campaña cero papel	Exposición de datos importantes y reservados en e papel reutilizable.	Incumplimiento de la confidencialidad e integridad de la información	Riesgo de información
Pérdida total de la información	No se cuenta con los tipos de extintores adecuados para usarlos en caso de necesidad	No se cuenta con los tipos de extintores adecuados para usarlos en caso de necesidad	Extintores vencidos.	Riesgo tecnológico Riesgo en el servicio. Riesgo de la información Riesgo en personal
Pérdida de información	Los funcionarios no realizan copias frecuentes de seguridad de los archivos más relevantes e importantes. Uso de memorias y	No hacen copias de seguridad No se hace control del uso	Posible pérdida de información Infección por virus	Riesgo en el servicio. Riesgo de la información Riesgo tecnológico

	unidades extraibles			
Pérdida de la información y/o deterioro físico	La documentación en físico está siendo archivada en sitios no adecuados.	Continuar con la digitalización de la información	Deterioro de documentos	Riesgo de información
Transición IPV4 a IPV6	No existe transición de protocolo de IP	No existe transición de protocolo de IP	No existe transición de protocolo de IP	Riesgo tecnológico

Tabla 4. Aspecto que generan Vulnerabildiadedes.
Fuente: MINTIC: Seguridad y Privacidad de la Información, Guía de Gestión de riesgos, nro. 7, 2016

6.2.3 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.
A continuación se describen una serie de amenazas comunes (Fuente: Guiad e riegos, MINTIC)

D= Deliberadas, A= Accidentales, E= Ambientales

TIPO	AMENAZA	ORIGEN
Daño físico	Fuego	A, D, E
	Agua	A, D, E
	Contaminación	A, D, E
	Accidente Importante	A, D, E
	Destrucción del equipo o medios	A, D, E
	Polvo, corrosión, congelamiento	A, D, E
Eventos naturales	Fenómenos climáticos	E
	Fenómenos sísmicos	E
	Fenómenos volcánicos	E
	Fenómenos meteorológico	E
	Inundación	E

Perdida de los servicios esenciales	Fallas en el sistema de suministro de aguao aire acondicionado	E
	Perdida de suministro de energía	E
	Falla en equipo de telecomunicaciones	D,A
Perturbación debida a la radiación	Radiación electromagnética	E
	Radiación térmica	E
	Impulsos electromagnéticos	E
Compromiso de la información	Interceptación de señales de interferencia comprometida	D
	Espionaje remoto	D
	Escucha encubierta	D
	Hurto de medios o documentos	D
	Hurto de equipo	D
	Recuperación de medios reciclados o desechados	
	Divulgación	D
	Datos provenientes de fuentes no confiables	D
	Manipulación con hardware	D
	Manipulación con software	D
	Detección de la posición	D
Fallas técnicas	Fallas del equipo	A,D,E
	Mal funcionamiento del equipo	A, D,E
	Saturación del sistema de información	A
	Mal funcionamiento del software	D, E
	Incumplimiento en el mantenimiento delsistema de información.	D
Acciones no autorizadas	Uso no autorizado del equipo	D
	Copia fraudulenta del software	D
	Uso de software falso o copiado	D
	Corrupción de los datos	D
	Procesamiento ilegal de datos	D
Compromiso de las funciones	Error en el uso	D
	Abuso de derechos	D
	Falsificación de derechos	D
	Negación de acciones	D
	Incumplimiento en la disponibilidad delpersonal	D

Tabla 5. Clasificación de las amenazas.
Fuente: MINTIC: Seguridad y Privacidad de la Información, Guía de Gestión de riesgos, nro. 7, 2016

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	Rebelión Estatus Dinero	• Piratería • Ingeniería Social • Intrusión, accesos forzados al sistema • Acceso no autorizado
Criminal de lacomputación	Destrucción de la información, Divulgación ilegal de la información Ganancia monetaria Alteración no autorizada de los datos	• 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 6. Lista de amenazas humanas.
Fuente: MINTIC: Seguridad y Privacidad de la Información, Guía de Gestión de riesgos, Nro 7.2016

6.2.4 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

6.2.5 Plan de tratamiento del riesgo:

En este punto se establecen acciones para el tratamiento de los riesgos en función de los puntos anteriores y de la política definida por la dirección. Y se establecen los controles adecuados para cada riesgo, los cuales irán orientados a: Asumir el riesgo, Reducir el riesgo, Eliminar el riesgo y Transferir el riesgo

Una vez se levante la Matriz de calificación, evaluación y respuesta a los riesgos se deben definir controles que permitan disminuir los valores de exposición del riesgo, y luego se debe hacer un recalculo comparando nuevamente con los criterios establecidos y así buscar un nivel aceptable del riesgo en cada proceso para los temas de Seguridad; en la definición de éstos nuevos controles

Para hacer una clasificación y valoración de los controles, se debe tener en cuenta los dos tipos de Controles, Preventivos y Correctivos:

- Preventivos: aquellos que actúan para eliminar las casas de riesgo para prevenir su ocurrencia o materialización
- Correctivos: aquellos que permiten el restablecimiento de la actividad, después de ser detectado un evento no deseable, también permiten la modificación de las acciones que proporcionaron su ocurrencia

7. MAPA DE RUTA Y PRESUPUESTO

Una vez se da claridad sobre las acciones que debe implementar el Municipio de Guatapé para gestión de manera adecuada los riesgos se presenta a continuación el siguiente Plan para el tratamiento de los riesgos:

ACTIVIDAD	RESPONSABLE	2023 TRIMESTRES				INDICADOR		PRESUPUESTO
		I	II	III	IV			
Identificar los activos de Información	Área de Gestión Documental					Activos de Información: Formula: Cantidad de políticas diseñadas * 100/ Cantidad de políticas a diseñar		5.000.000
Levantar la matriz de calificación, evaluación y respuesta a los riesgos	Coordinador de Soporte Técnico					Matriz de calificación, evaluación y respuesta a los riesgos. Fórmula Matriz de califi, evaluac de riegos realizada * 100/ Número de matrices de calif.y evaluación proyectadas		3.000.000
Realizar la Matriz de clasificación y valoración de los controles	Coordinador de Soporte Técnico					Matriz de calificación, evaluación y respuesta a los riesgos. Fórmula Matriz de clasif, y valorac. de controles realizada * 100/ Número de matrices de control proyectadas		2.000.000
Realizar el mapa de riesgo y aplicar acciones	Coordinador de Soporte Técnico					Mapa de riegos Fórmula Matriz de clasif, y valorac. de controles realizada * 100/ Número de matrices de control proyectadas		3.000.000
Capacitar los funcionarios y contratistas en temas relacionados con el tratamiento de los riesgos	Coordinador de Soporte Técnico					Capacitación a funcionarios sobre riesgos informáticos Formula Nro de capacitaciones realizadas*100/Nro de Capacitaciones proyectadas		5.000.000
TOTAL								18’000.000

Tabla 7. Mapa de Ruta y presupuesto

8. BIBLIOGRAFIA

- ✓ Guía de Gestión de Riesgos. Seguridad y Privacidad de la Información. Ministerio de las Tic, 2016
- ✓ Guía para la Gestión y Clasificaciónde Activos de Información. Seguridad y Privacidad de la Información. Ministerio de las Tic, 2016

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