PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD DIGITAL
2024

Alcaldía de Bucaramanga
Oficina Asesora TIC
2024

TABLA DE CONTENIDO

1. OBJETIVO

Este plan establece una guía para el control y minimización de los de los riesgos de seguridad digital y así proteger la privacidad de la información y los datos tanto de los procesos como de las personas vinculadas con la información de la institución.

1.1. Objetivos específicos

- Lograr un diagnóstico real de la situación actual de la institución en materia de riesgos de seguridad digital.
- Aplicar las metodologías, mejores prácticas y recomendaciones dadas por la función pública y el MinTIC para el Tratamiento de Riesgos de Seguridad Digital.
- Optimización de los recursos de la institución en la aplicación del Plan de Tratamiento de Riesgos de Seguridad Digital.

2. ALCANCE

El plan de tratamiento de riesgos de seguridad digital aplica a todos los procesos de la institución los cuales manejen, procesen o interactúen con información institucional.

3. DEFINCIONES Y/O ABREVITURAS

- **Activo**: En relación con la seguridad de la información, se refiere a cualquier información o elemento relacionado con el tratamiento de la misma (sistemas, soportes, edificios, personas…) que tenga valor para la organización. (ISO/IEC 27000).

- **Amenazas:** Causa potencial de un incidente no deseado, que puede provocar daños a un sistema o a la organización. (ISO/IEC 27000).

- **Análisis de Riesgo:** Proceso para comprender la naturaleza del riesgo y determinar el nivel de riesgo.

- **Auditoría:** Proceso sistemático, independiente y documentado para obtener evidencias de auditoria y obviamente para determinar el grado en el que se cumplen los criterios de auditoria. (ISO/IEC 27000).

- **Ciberseguridad:** Capacidad del Estado para minimizar el nivel de riesgo al que están expuestos los ciudadanos, ante amenazas o incidentes de naturaleza cibernética.

- **Ciberespacio:** Ámbito o espacio hipotético o imaginario de quienes se encuentran inmersos en la civilización electrónica, la informática y la cibernética. (CONPES 3701, Tomado de la Academia de la lengua española). Control Las políticas, los procedimientos, las prácticas y las estructuras organizativas concebidas para mantener los riesgos de seguridad de la información por debajo del nivel de riesgo asumido. Control es también utilizado como sinónimo de salvaguarda o contramedida. En una definición más simple, es una medida que modifica el riesgo

- **Declaración de aplicabilidad:** Documento que enumera los controles aplicados por el Sistema de Gestión de Seguridad de la Información – SGSI, de la organización tras el resultado de los procesos de evaluación y tratamiento de riesgos y su justificación, así como la justificación de las exclusiones de controles del anexo A de ISO 27001. (ISO/IEC 27000).

- **Gestión de incidentes de seguridad de la información** Procesos para detectar, reportar, evaluar, responder, tratar y aprender de los incidentes de seguridad de la información. (ISO/IEC 27000).

- **Plan de continuidad del negocio:** Plan orientado a permitir la continuación de las principales funciones misionales o del negocio en el caso de un evento imprevisto que las ponga en peligro. (ISO/IEC 27000).

- **Plan de tratamiento de riesgos:** Documento que define las acciones para gestionar los riesgos de seguridad de la información inaceptables e implantar los controles necesarios

- **Riesgo:** Posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información. Suele considerarse como una combinación de la probabilidad de un evento y sus consecuencias. (ISO/IC 27000).

- **Seguridad de la información:** Preservación de la confidencialidad, integridad, y disponibilidad de la información. (ISO/IEC 27000).

- **Sistema de Gestión de Seguridad de la Información SGSI:** Conjunto de elementos interrelacionados interactuantes (estructura organizativa, políticas, planificación de actividades, responsabilidades, procesos, procedimientos y recursos) que utiliza una organización para establecer una política y unos objetivos de seguridad de la información y alcanzar dichos objetivos, basándose en un enfoque de gestión y de mejora continua. (ISO/IEC 27000).

- **Trazabilidad:** Cualidad que permite que todas las acciones realizadas sobre la información o un sistema de tratamiento de la información sean asociadas de modo inequívoco a un individuo o entidad. (ISO/IEC 27000).

- **Vulnerabilidad:** Debilidad de un activo o control que puede ser explotada por una o más amenazas. (ISO/IEC 27000).
- **Parte interesada**: Persona u organización que puede afectar a, ser afectada por o percibirse a sí misma como afectada por una decisión o actividad.

4. RESPONSABLE

La estructura organizacional de los procesos responsables de la realización del plan es la siguiente:

LÍNEAS DE DEFENSA	RESPONSABLE	RESPONSABILIDAD FRENTE AL RIESGO
Estratégica	Alta Dirección - Alcalde Municipal, Comité Institucional de	• Establecer y aprobar la Política de Administración del Riesgo y su actualización.

	Coordinación de Control Interno	• Analizar los cambios en el contexto interno y externo que puedan tener un impacto en la operación de la entidad y generar cambios en la estructura de riesgos y controles. • Evaluar el estado del Sistema de Control Interno y aprobar las modificaciones, actualizaciones y acciones de fortalecimiento de este.
Primera Línea	Líderes de Proceso	• Identificar y valorar los riesgos. Definir, aplicar y hacer seguimiento a los controles para mitigar los riesgos. • Realizar las acciones necesarias con su respectivo seguimiento, para evitar la materialización de los riesgos. • Informar a la Secretaría de Planeación los riesgos materializados. • Reportar los avances y evidencias de la gestión de los riesgos.
Segunda Línea	Secretaría de Planeación	• Asesorar en el análisis del contexto interno y externo, para la definición de la política de riesgo, el establecimiento de los niveles de impacto y el nivel de aceptación del riesgo. • Consolidar los Mapas de Riesgos (de gestión, de corrupción). • Acompañar, orientar y entrenar a los líderes de procesos en la identificación, análisis y valoración del riesgo.

Tercera Línea	Oficina de Control Interno de Gestión	• Asesorar y orientar sobre la metodología para la identificación, análisis y valoración del riesgo. • Analizar el diseño e idoneidad de los controles establecidos en los procesos. • Realizar seguimiento a los riesgos consolidados en el mapa de riesgos de gestión (dos veces al año), mapa de riesgos de corrupción (tres veces al año). • Recomendar mejoras a la política de administración del riesgo.

5. DOCUMENTOS DE REFERENCIA

- Decreto Nacional 767 de 2022, "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".
- Resolución 746 de 2022 expedida por el Ministerio de TIC, ""Por la cual se fortalece el Modelo de Seguridad y Privacidad de la Información y se definen lineamientos adicionales a los establecidos en la Resolución No. 500 de 2021".
- Guía DAFP Guía para la Administración del Riesgo, "Guía para la Administración del Riesgo y el diseño de controles en entidades públicas (Versión 6)".
- Decreto Nacional 612 de 2018, "Por el cual se fijan directrices para la integración de los planes institucionales y estratégicos al Plan de Acción por parte de las entidades del Estado", donde se encuentra el presente Plan Estratégico de Seguridad de la Información (PESI) como uno de los requisitos a desarrollar para cumplir con esta normativa.
- Resolución 500 de 2021 expedida por el Ministerio de TIC, "Por la cual se establecen los lineamientos y estándares para la estrategia de seguridad digital y se adopta el modelo de seguridad y privacidad como habilitador de la política de Gobierno Digital".
- CONPES 3995 de 2020, "Política Nacional de Confianza y Seguridad digital".
- Manual de Gobierno Digital – MINTIC.
- Modelo de Seguridad y Privacidad de la Información – MINTIC.
- Ley Estatutaria 1581 de 2012. Ley de Protección de Datos Personales.
- Resolución Municipal 0350 del 28 de noviembre de 2023 .
- Política de Tratamiento de Datos Personales del Municipio de Bucaramanga.
- Resolución 350 de la Alcaldía de Bucaramanga de 28 de Noviembre de 2023.
- Resolución 139 de la Alcaldía de Bucaramanga de 17 de abril de 2023.
- Plan de Recuperación ante Desastres (DRP) de la Alcaldía de Bucaramanga.
- Plan Estratégico de Seguridad y Privacidad de la Información de la Alcaldía de Bucaramanga.

.

6. NORMATIVIDAD

NORMA	DESCRIPCIÓN
LEY 1928 DE 2018	Por medio de la cual se aprueba el «CONVENIO SOBRE LA ciberdelincuencia», adoptado el 23 de noviembre de 2001, en Budapest.

DECRETO 0035 DE 2019	Por el cual se modifica, adiciona y ajusta el decreto 098 de 2018, en desarrollo del comité institucional de gestión y desempeño
DECRETO LEY 2106 DE 2019	Por el cual se dictan normas para simplificar, suprimir y reformar trámites, procesos y procedimientos innecesarios existentes en la administración pública
LEY 2294 DE 2023	Por el cual se expide el Plan Nacional de Desarrollo 2022-2026 - Colombia Potencia Mundial de la vida.
DECRETO 338 DE 2022	Por el cual se adiciona el Titulo 21 a la Parte 2 del Libro 2 del Decreto Único 1078 de 2015, Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones, con el fin de establecer los lineamientos generales para fortalecer la gobernanza de la seguridad digital, se crea el Modelo y las instancias de Gobernanza de Seguridad Digital y se dictan otras disposiciones
RESOLUCIÓN N° 1519 DEL 24 DE AGOSTO DE 2020	Por la cual se definen los estándares y directrices para publicar la información señalada en la Ley 1712 del 2014 y se definen los requisitos materia de acceso a la información pública, accesibilidad web, seguridad digital, y datos abiertos
RESOLUCIÓN NÚMERO 002256 DE NOVIEMBRE 06 DE 2020	Por la cual se actualiza la Política General de Seguridad y Privacidad de la Información, Seguridad Digital y Continuidad de la Operación de los Servicios del Ministerio/Fondo Único de Tecnologías de la Información y las Comunicaciones, se definen lineamientos frente al uso y manejo de la información y se derogan las Resoluciones 2999 de 2008 y 1124 de 2020.
RESOLUCIÓN N° 500 DE 2021	Por la cual se establecen los lineamientos y estándares para la estrategia de seguridad digital y se adopta el modelo de seguridad y privacidad como habilitador de la política de Gobierno Digital.
DIRECTIVA PRESIDENCIAL 03 DE 2021	Lineamientos para el uso de servicios en la nube, inteligencia digital, seguridad digital y gestión de datos.
RESOLUCIÓN 746 DE 2022	Por la cual se fortalece el Modelo de Seguridad y Privacidad de la Información y se definen lineamientos adicionales a los establecidos en la Resolución número 500 de 2021.

MODELO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN - MSPI	Imparte lineamientos en materia de implementación y adopción de buenas prácticas, tomando como referencia estándares internacionales, con el objetivo de orientar la gestión e implementación adecuada del ciclo de vida de la seguridad de la información (Planeación, Implementación, Evaluación, Mejora Continua), permitiendo habilitar la implementación de la Política de Gobierno Digital.
MODELO INTEGRADO DE PLANEACIÓN Y GESTIÓN - MIPG	Simplifica e integra los sistemas de desarrollo administrativo y gestión de calidad y los articula con el sistema de control interno de la entidad.
ISO 27001:2022	Normativa internacional que provee requerimientos para la implementación del Sistema de Gestión de Seguridad de información
ISO 27002:2013	Brinda pautas para los estándares de seguridad de la información de la organización y las prácticas de gestión de la seguridad de la información, incluida la selección, implementación y gestión de controles teniendo en cuenta los entornos de riesgo de seguridad de la información de la organización.
ISO 27005:2022	Gestión de riesgos de seguridad de la información.
ISO 22301:2019	Requerimientos para gestión de la continuidad del negocio; seguridad y resiliencia.
ISO/CEI 27035-3:2020	Gestión de incidentes de seguridad de la información. Parte 3: Directrices para las operaciones de respuesta a incidentes de TIC.
CONPES 3701 DE 2011	Lineamientos de política para ciberseguridad y ciberdefensa.
CONPES 3854 DE 2016	Política Nacional de Seguridad Digital
CONPES 3920 DE 2018	Política Nacional de Explotación de Datos (Big Data).
CONPES 3995 DE 2020	Política Nacional de Confianza y Seguridad Digital- Establece medidas para ampliar la confianza digital y mejorar la seguridad
DECRETO 681 DE 2020	Por el cual se adiciona el título 19 a la parte 2 del decreto 1078 de 2015, decreto único reglamentario del sector de tecnologías de la información y las comunicaciones, para establecer las reglas para implementar el artículo 154 de la ley 1955 de 2019

7. DESCRIPCIÓN Y/O DESARROLLO

7.1 INTRODUCCIÓN

La Alcaldía de Bucaramanga en busca de la mejora continua implementa un método lógico y sistemático que permita identificar, analizar, evaluar, tratar, monitorear y comunicar los riesgos asociados al manejo de la información institucional, para lograr que estos no afecten de una manera relevante a la misma.

La institución en su quehacer diario utiliza TIC en cuanto a captura, procesamiento y reporte de información tanto internamente como externamente para comunicarse con los diferentes entes descentralizados, lo cual implica que la institución sea vulnerable a ataques mal intencionados o mala manipulación de la información lo que acarrea problemas económicos, legales, y administrativos por lo cual este documento busca establecer un línea de trabajo que permita a la entidad sortear los riesgos que lo rodean y lograr que su información este segura.

7.2 CATEGORÍAS DE RIESGOS

- **ET - Estratégicos:** Relacionados a lineamientos, políticas, estrategias o directrices no adecuadas o no convenientes para la Entidad.
- **OP - Operativo:** Relacionado a procesos, conductas o actividades inapropiadas, contrarias al deber ser o que presente una posible brecha frente a la calidad esperada.
- **FA - Financiero:** Relacionado con la asignación, suficiencia o recaudo de recursos económicos que puedan afectar a corto, mediano o largo plazo financieramente a los procesos o la entidad.
- **TEC - Tecnológico:** Relacionado al uso, manejo o disposición de equipos biomédicos, industriales o de cómputo y periféricos.

7.3 IDENTIFICACIÓN DEL RIESGO

Identificación de los riesgos inherentes de seguridad de la información. Se definen tres (3) riesgos inherentes de seguridad de la información:

- Pérdida de la confidencialidad
- Pérdida de la integridad
- Pérdida de la disponibilidad

Para cada riesgo, se deben asociar el grupo de activos o activos específicos del proceso, y conjuntamente analizar las posibles amenazas y vulnerabilidades que podrían causar su materialización.

Los riesgos de seguridad de la información forman parte de los riesgos de proceso, y por tanto se contempla dentro de la metodología descrita en la presente Política de Administración de Riesgos, aplicable a todos los procesos de la Administración Municipal, teniendo en cuenta, además, aspectos descritos en el Anexo 6 Lineamientos para la Gestión del Riesgo de Seguridad digital en Entidades Públicas – Guía riesgos 2022.

7.4 DESCRIPCIÓN DE CAUSAS

Se describen las causas asociadas al riesgo identificado, pueden ser intrínsecas: atribuidas a personas, métodos, materiales, equipos, instalaciones, directamente involucradas en el proceso o externas: cuando provienen del entorno en el que se desarrolla el proceso.

7.5 CONSECUENCIAS

Se describen los efectos asociados a la materialización del riesgo, que incidan sobre el objetivo del proceso o la Entidad. Pueden agruparse en: Daños a pacientes o trabajadores, Pérdidas económicas, Perjuicio de la imagen, Sanciones legales, reproceso, Demoras, Insatisfacción, entre otras.

7.6 BARRERAS DE SEGURIDAD EXISTENTES

Se describen los controles implementados o barreras que existen actualmente para evitar la materialización del riesgo, se pueden encontrar en los protocolos o procedimientos documentados, en las guías de reacción inmediata o en los correctos

de buenas prácticas de seguridad del paciente, adicionalmente este apartado es importante mencionar que existen acciones y buenas prácticas mencionadas en este documento que son complementarias y apoyan los controles, acciones , actividades y planes de control documentados en el Plan de Recuperación ante Desastres – DRP (PL-TIC-1400-170-001) y el Plan Estratégico de Seguridad y Privacidad de la Información de Alcaldía de Bucaramanga (PL-TIC-1400-170-009).

7.7 VISIÓN PROCESO DE GESTIÓN DE RIESGO EN LA SEGURIDAD DIGITAL

A continuación, se presenta el modelo de gestión de riesgos de seguridad digital diseñada basada tanta en la norma ISO/IEC 31000 como en la ISO 27005 y en la Política de Administración del Riesgo V.7.0 aprobado por la Alcaldía de Bucaramanga para la adecuada administración de riesgos en la seguridad de la información; los elementos que lo componen son:

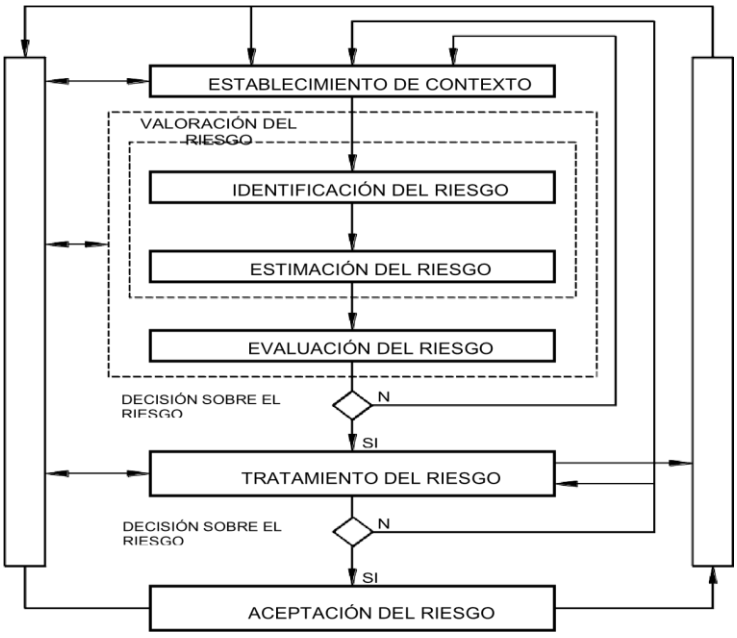

Figura 1. Modelo de gestión de riesgos de seguridad digital diseñada basada tanta en la norma ISO/IEC 31000

La gestión de riesgos de seguridad de la información deberá ser iterativa para las actividades de valoración de riesgos y/o tratamiento de estos.

7.7.1 ESTABLECIMIENTO DEL CONTEXTO DE RIESGOS DE SEGURIDAD DIGITAL

El contexto de gestión de riesgos de seguridad digital define los criterios básicos que serán necesarios para enfocar el ejercicio por parte de la Alcaldía de Bucaramanga y obtener los resultados esperados, basándose en, la identificación de las fuentes que pueden dar origen a los riesgos y oportunidades en los procesos de la Alcaldía de Bucaramanga, en el análisis de las debilidades y amenazas asociadas, en la valoración de los riesgos en términos de sus consecuencias para la Entidad y en la probabilidad de su ocurrencia, al igual que en la construcción de acciones de mitigación en beneficio de lograr y mantener niveles de riesgos aceptables para la Entidad.

Como criterios para la gestión de riesgos de seguridad de la información se establecen:

7.7.1.1 Criterios de evaluación del riesgo de seguridad digital

La evaluación de los riesgos de seguridad de la información se enfocará en:

- El valor estratégico del proceso de información en la Alcaldía de Bucaramanga.
- La criticidad de los activos de información involucrados.
- Los requisitos legales y reglamentarios, así como las obligaciones contractuales.
- La importancia de la disponibilidad, integridad y confidencialidad para las operaciones de la Alcaldía de Bucaramanga.
- Las expectativas y percepciones de las partes interesadas y las consecuencias negativas para el buen nombre y reputación de la Alcaldía de Bucaramanga.

7.7.1.2 Criterios de Impacto

Los criterios de impacto se especificarán en términos del grado, daño o de los costos para la Alcaldía de Bucaramanga, causados por un evento de seguridad de la información, considerando aspectos tales como:

- Nivel de clasificación de los activos de información impactados.
- Brechas en la seguridad de la información (pérdida de la confidencialidad, integridad y disponibilidad).
- Operaciones deterioradas (afectación a partes internas o terceras partes).

- Pérdida del negocio y del valor financiero.
- Alteración de planes o fechas límites.
- Daños en la reputación.
- Incumplimiento de los requisitos legales, reglamentarios o contractuales.

7.7.1.3 Criterios de Aceptación

Los criterios de aceptación dependerán con frecuencia de las políticas, metas, objetivos de la Alcaldía de Bucaramanga y de las partes interesadas.

7.8 VALORACIÓN DE LOS RIESGOS DE SEGURIDAD DIGITAL

Previo a la valoración de riesgos de seguridad de la información se determina la relevancia de identificar un inventario de activos de información de los procesos, el cual será la base del enfoque de la valoración de los riesgos de seguridad de la información.

Se deberán identificar, describir cuantitativa o cualitativamente y priorizarse frente a los criterios de evaluación del riesgo y los objetivos relevantes para la Alcaldía de Bucaramanga, esta fase consta de las siguientes etapas:
La valoración del Riesgo de seguridad de la información consta de las siguientes actividades:

- Análisis del riesgo
  - ✓ Identificación de los riesgos
  - ✓ Estimación del riesgo
- Evaluación del riesgo

7.8.1 Identificación del riesgo

Para la evaluación de riesgos de seguridad digital en primer lugar se deberán identificar los activos de información por proceso en evaluación.

Los **activos de información** se clasifican en dos tipos:

Primarios

a. **Procesos o subprocesos y actividades del Negocio:** procesos cuya pérdida o degradación hacen imposible llevar a cabo la misión de la organización; procesos que contienen procesos secretos o que implican tecnología propietaria; procesos que, si se modifican, pueden afectar de manera muy significativa el cumplimiento de la misión de la organización; procesos que son necesarios para el cumplimiento de los requisitos contractuales, legales o reglamentarios.

b. **Información**: información vital para la ejecución de la misión o el negocio de la organización; información personal que se puede definir específicamente en el sentido de las leyes relacionadas con la privacidad; información estratégica que se requiere para alcanzar los objetivos determinados por las orientaciones estratégicas; información del alto costo cuya recolección, almacenamiento, procesamiento y transmisión exigen un largo periodo de tiempo y/o implican un alto costo de adquisición, etc.

c. **Actividades y procesos de negocio**: que tienen que ver con propiedad intelectual, los que si se degradan hacen imposible la ejecución de las tareas de la empresa, los necesarios para el cumplimiento legal o contractual, etc.

De Soporte

a. **Hardware**: Consta de todos los elementos físicos que dan soporte a los procesos (PC, portátiles, servidores, impresoras, discos, documentos en papel, etc.).
b. **Software**: Consiste en todos los programas que contribuyen al funcionamiento de un conjunto de procesamiento de datos (sistemas operativos, paquetes de software o estándar, aplicaciones, mantenimiento o administración, etc.)
c. **Redes**: Consiste en todos los dispositivos de telecomunicaciones utilizados para interconectar varios computadores remotos físicamente o los elementos de un sistema de información (conmutadores, cableado, puntos de acceso, etc.)
d. **Personal**: Consiste en todos los grupos de personas involucradas en el sistema de información (usuarios, desarrolladores, responsables, etc.)

e. **Sitio**: Comprende todos los lugares en los cuales se pueden aplicar los medios de seguridad de la organización (Edificios, salas, y sus servicios, etc.)
f. **Estructura organizativa**: responsables, áreas, contratistas, etc.

Después de tener una relación con todos los activos se han de conocer las **amenazas** que pueden causar daños en la información, los procesos y los soportes. La identificación de las amenazas y la valoración de los daños que pueden producir se puede obtener preguntando a los propietarios de los activos, usuarios, expertos, etc.

Posterior a la identificación del listado de activos, sus amenazas y las medidas que ya se han tomado, a continuación, se revisarán las **vulnerabilidades** que podrían aprovechar las amenazas y causar daños a los activos de información de la Alcaldía de Bucaramanga. Existen distintos métodos para analizar amenazas, por ejemplo:

- Entrevistas con líderes de procesos y usuarios
- Inspección física
- Uso de las herramientas para el escaneo automatizado

Para cada una de las **amenazas** analizaremos las **vulnerabilidades** (debilidades) que podrían ser explotadas.

Finalmente se identificarán las **consecuencias**, es decir, cómo estas amenazas y vulnerabilidades podrían afectar la confidencialidad, integridad y disponibilidad de los activos de información.

7.8.2 Estimación del riesgo

La estimación del riesgo busca establecer la *probabilidad* de ocurrencia de los riesgos y el *impacto* de sus consecuencias, calificándolos y evaluándolos con el fin de obtener información para establecer el nivel de riesgo, su priorización y estrategia de tratamiento de estos. El objetivo de esta etapa es el de establecer una valoración y priorización de los riesgos.

Para adelantar la estimación del riesgo se deben considerar los siguientes aspectos:

- **Probabilidad**: La posibilidad de ocurrencia del riesgo, representa el número de veces que el riesgo se ha presentado en un determinado tiempo o pudiese presentarse. Es importante destacar que la siguiente tabla define la probabilidad de que una amenaza se aproveche de la vulnerabilidad del activo de información en cuestión:

	Frecuencia de la Actividad	Probabilidad	Relación – Controles
Muy Baja	La actividad que conlleva el riesgo se ejecuta como máximos 2 veces por año	20%	Los controles de seguridad existentes son seguros y hasta el momento han suministrado un adecuado nivel de protección. En el futuro no se esperan incidentes nuevos.
Baja	La actividad que conlleva el riesgo se ejecuta de 3 a 24 veces por año	40%	
Media	La actividad que conlleva el riesgo se ejecuta de 24 a 500 veces por año	60%	Los controles de seguridad existentes son moderados y en general han suministrado un adecuado nivel de protección. Es posible la ocurrencia de nuevos incidentes, pero no muy probable.
Alta	La actividad que conlleva el riesgo se ejecuta mínimo 500 veces al año y máximo 5000 veces por año	80%	Los controles de seguridad existentes son bajos o ineficaces. Existe una gran probabilidad de que haya incidentes así en el futuro.
Muy Alta	La actividad que conlleva el riesgo se ejecuta más de 5000 veces por año	100%	

Figura 2. Criterios para definir el nivel de probabilidad Riesgos en activos de información
Adaptado para la Alcaldía de la Guía de Riesgos DAFP, 2022

- **Impacto**: Hace referencia a las consecuencias que puede ocasionar a la Alcaldía de Bucaramanga la materialización del riesgo; se refiere a la magnitud de sus efectos.

	Afectación económica	Reputacional	Relación – Confidencialidad/Integridad/Disponibilidad
Leve 20%	Afectación menor a 10 SMLMV	El riesgo afecta la imagen de algún área de la organización.	La pérdida de confidencialidad, disponibilidad o integridad no afecta las finanzas, las obligaciones legales o contractuales o el prestigio de la entidad.
Menor 40%	Entre 10 y 50 SMLMV	El riesgo afecta la imagen de la entidad internamente, de conocimiento general nivel interno, de junta directiva y accionistas y/o de proveedores	
Moderado 60%	Entre 50 y 100 SMLMV	El riesgo afecta la imagen de la entidad con algunos usuarios de relevancia frente al logro de los objetivos	La pérdida de confidencialidad, disponibilidad o integridad causa gastos y tiene consecuencias bajas o moderadas sobre obligaciones legales o contractuales o sobre el prestigio de la entidad.
Mayor 80%	Entre 100 y 500 SMLMV	El riesgo afecta la imagen de la entidad con efecto publicitario sostenido a nivel de sector administrativo, nivel departamental o municipal.	La pérdida de confidencialidad, disponibilidad o integridad tiene consecuencias importantes y/o inmediatas sobre las finanzas, las operaciones, las obligaciones legales o contractuales o el prestigio de la organización.
Catastrófico 100%	Mayor a 500 SMLMV	El riesgo afecta la imagen de la entidad a nivel nacional, con efecto publicitario sostenido a nivel país	

Figura 3. Criterios para definir el nivel de impacto Riesgos en activos de información Adaptado para la Alcaldía de la Guía de Riesgos DAFP, 2022

Se sugiere realizar este análisis con todas o las personas que más conozcan del proceso, y que por sus conocimientos o experiencia puedan determinar el impacto y la probabilidad del riesgo de acuerdo con los rangos señalados en las tablas que se muestran más adelante. Como criterios para la estimación del riesgo desde el enfoque de impacto y consecuencias se podrán tener en cuenta: pérdidas financieras, costes de reparación o sustitución, interrupción del servicio, disminución del rendimiento, infracciones legales, pérdida de ventaja competitiva, daños personales, entre otros.

Además de medir las posibles consecuencias se deberán analizar o estimar la probabilidad de ocurrencia de situaciones que generen impactos sobre los activos de información o la operación del negocio.

7.8.3 Determinación del riesgo inherente y residual

El análisis del riesgo determinado por su probabilidad e impacto permite tener una primera evaluación del riesgo inherente (escenario sin controles) y ver el grado de exposición al riesgo que tiene la entidad. La exposición al riesgo es la ponderación de la probabilidad e impacto, y se puede ver gráficamente en la matriz de riesgo, instrumento que muestra las zonas de riesgos y que facilita el análisis gráfico. Permite

analizar de manera global los riesgos que deben priorizarse según la zona en que quedan ubicados los mismos (zona de riesgo bajo, moderado, alto o extremo) facilitando la organización de prioridades para la decisión del tratamiento e implementación de planes de acción.

De acuerdo plan de tratamiento de riesgos de seguridad digital en el cual se especifica que la exposición al riesgo es la ponderación de la probabilidad e impacto (Riesgo = Probabilidad * Impacto).

En la siguiente tabla se muestra la matriz de riesgo, instrumento que muestra las zonas de riesgo y que facilita el análisis gráfico.

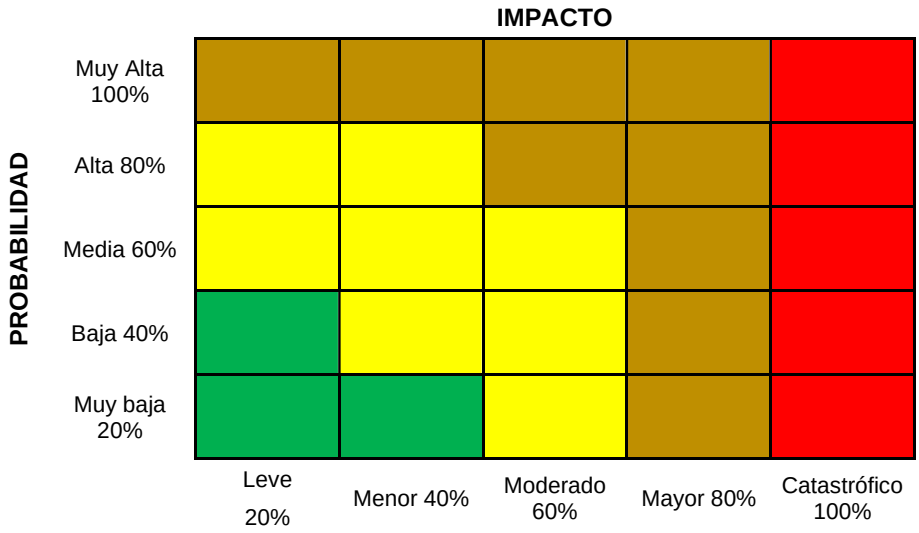

Figura 4. Esquema general de Matriz de Riesgo Institucional y Zonas de Riesgo Institucional para la Alcaldía – adaptado del DAFP.

Esta herramienta permite analizar de manera global los riesgos que deben priorizarse según la zona en que quedan ubicados (zona de riesgo BAJO, MODERADO, ALTO o EXTREMO) facilitando la organización de prioridades para la decisión del tratamiento e implementación de planes de acción.

7.8.4 Evaluación de los riesgos

Una vez se valoran los impactos, la probabilidad y las consecuencias de los escenarios de incidentes sobre los activos de información, se obtendrán los niveles de riesgo, para los cuales se deberán comparar frente a los criterios básicos del contexto, para una adecuada y pertinente toma de decisiones basada en riesgos de seguridad de la información y en beneficio de reducir su impacto a la Alta Entidad.

7.9 MAPA DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN

Como parte integral de este plan se anexan los riesgos incluidos en el mapa de riesgos de seguridad de la información, el cual determina la acciones y actividades necesarias para la garantizar la correcta implementación de este, a continuación de menciona de manera general los riesgos establecidos para el año 2024 y se anexa el formato F-TIC-1400-23837-047-MATRIZ-MAPA-RIESGOS-SEG-INFORMACION-2023, el cual contiene el detalle de cada una de las acciones.

No	ACTIVO DE INFORMACIÓN	AMENAZAS (CAUSA INMEDIATA)	VULNERABILIDADES (CAUSA RAIZ)	TIPO DE RIESGO	DESCRIPCIÓN DEL RIESGO	PLAN DE ACCIÓN
1	Sistemas de Información, Aplicativos Software y Bases de Datos	Perdida de información reservada por un ataque informático	Ausencia de mecanismos alternos de respaldo	Perdida de disponibilidad	La ausencia de mecanismos alternos de respaldo podría desencadenar en perdida de información reservada y/o confidencial por un ataque informático sobre las bases de datos y los sistemas de información críticos.	Realizar (1) una supervisión diaria de la sincronización y correcta ejecución de todas las copias de seguridad de las bases de datos, sistemas de información e información institucional custodiada por la Oficina Asesora TIC.

2	Sistemas de Información y Aplicativos Software	Ejecución de código malicioso y/o compromiso de la integridad y disponibilidad de los sistemas	Ausencia de parches de seguridad y omisión en la actualización de las aplicaciones a sus versiones más recientes.	Perdida de Integridad	La ausencia de actualizaciones de seguridad en las aplicaciones podría poner en riesgo la integridad y disponibilidad de los sistemas, permitiendo la ejecución de código malicioso.	Realizar (2) dos análisis de vulnerabilidades en el año de manera semestral sobre los sistemas de información críticos . Implementación de dos(2) planes de remediación de acuerdo con los análisis de vulnerabilidades detectadas en los análisis realizados.
3	Sistemas de información, equipos de infraestructura y bases de datos	Daños o afectación de los servicios y de la infraestructura tecnológica	Falta de mantenimiento sobre los elementos físicos y lógicos que componen la infraestructura tecnológica: cableado, racks, aire acondicionado, sistemas de extinción de incendios (detectores de humo, extinguidores etc.), UPS, planta eléctrica, servidores físicos y virtualizados.	Perdida de Disponibilidad	La falta de mantenimiento tanto en los elementos físicos como lógicos de la infraestructura tecnológica podría ocasionar pérdida de disponibilidad de los sistemas críticos que respaldan los diversos servicios y procesos de la entidad.	Realizar dos (2) dos mantenimientos preventivos durante el año donde se incluyan tanto los elementos lógicos y físicos que componen la infraestructura tecnológica.

4	Servidores, sistemas de almacenamiento, bases de datos, sistemas de información	Daños e interrupción de los servicios y de la infraestructura tecnológica	Ausencia en la definición y ejecución de un plan de recuperación ante desastres tecnológicos	Perdida de Disponibilidad	La falta de claridad en la definición y ejecución de un plan de recuperación ante desastres tecnológicos podría dar lugar a la indisponibilidad en la prestación de servicios de la entidad debido a daños o interrupciones en los sistemas e infraestructura tecnológica.	Implementar el plan de recuperación ante desastres tecnológicos el cual debe incluir la realización de dos (2) pruebas a las actividades establecidas en dicho plan.
5	Sistemas de Información y Aplicativos Software	Ataques de ingeniería social	Falta de definición en implementación de estrategias de capacitación, sensibilización y entrenamiento en temas relacionados con Seguridad de la Información y Ciberseguridad.	Perdida de la Confidencialidad	La ausencia de capacitación, sensibilización y entrenamiento en seguridad y ciberseguridad para todas las partes interesadas podría comprometer la confidencialidad de la información en diversos sistemas y activos por medio de un ataque de ingeniería social.	Implementar una estrategia de sensibilización que incluya al menos cuatro (4) capacitaciones a nivel de seguridad de la información en temáticas de ingeniería social, phishing, ataques de suplantación de identidad, políticas de tratamiento de datos y seguridad de la información, entre otras.

6	Equipo de seguridad perimetral (Firewall) Consola de antivirus Software de monitoreo de red PRTG Consola de office 365	Vulneración de los controles de seguridad	Falta de adecuado monitoreo y seguimiento de los incidentes de seguridad y ciberseguridad	Perdida de la Integridad	La falta de un monitoreo y seguimiento efectivos de los incidentes de seguridad y ciberseguridad podría propiciar la vulneración de los controles de seguridad, comprometiendo así la integridad de los diversos activos de información de le Entidad.	Realizar un (1) informe cuatrimestral que incluya la relación de los eventos o incidentes que se hayan presentado y que representen riesgos para la información y la infraestructura tecnológica de la entidad
7	Sistemas de información Plataformas de administración	Abuso de los derechos	Ausencia de mecanismos de monitoreo para supervisar la gestión realizada por los administradores de las plataformas	Perdida de la Integridad	La ausencia de mecanismos de monitoreo para supervisar la gestión efectuada por los administradores de las plataformas podría dar lugar a actividades inapropiadas que atenten contra la seguridad y privacidad de la información en los sistemas y aplicaciones.	Realizar (1) un monitoreo trimestral de las actividades realizadas por los administradores de las diferentes plataformas tecnológicas y sistemas de información.

7.10 TRATAMIENTO DE LOS RIESGOS DE SEGURIDAD DIGITAL

Como resultado de la etapa de evaluación del riesgo tendremos una lista ordenada de riesgos o una matriz con la identificación de los niveles de riesgo de acuerdo con la zona de ubicación, por tanto, se deberá elegir la(s) estrategia(s) de tratamiento del riesgo en virtud de su valoración y de los criterios establecidos en el contexto de gestión de riesgos.

De acuerdo con el nivel evaluación de los riesgos, se deberá seleccionar la opción de tratamiento adecuada por cada uno de los riesgos identificados; el costo/beneficio del tratamiento deberá ser un factor de decisión relevante para la decisión.

TIPO DE RIESGO	RESPONSABLE	ACCIÓN
Riesgo de Corrupción	**Líder de Proceso y Asesor TIC Despacho Alcalde**	•Informar al Proceso de Planeación y Direccionamiento Estratégico sobre el hecho encontrado. • Una vez surtido el conducto regular establecido por la entidad y dependiendo del alcance (normatividad asociada al hecho de corrupción materializado), tramitar la denuncia ante la instancia de control correspondiente. • Identificar las acciones correctivas necesarias y documentarlas en el Plan de mejoramiento. • Efectuar el análisis de causas y determinar acciones preventivas y de mejora. • Actualizar el mapa de riesgos.
	Oficina de Control Interno de Gestión	• Informar al Líder del proceso, quien analizará la situación y definirá las acciones a que haya lugar. • Una vez surtido el conducto regular establecido por la entidad y dependiendo del alcance (normatividad asociada al hecho de corrupción materializado), realizar la denuncia ante la instancia de control correspondiente. • Informar a la segunda línea de defensa con el fin de facilitar el inicio de las acciones correspondientes con el líder del proceso, para revisar el mapa de riesgos
Riesgos de Gestión y Seguridad de la Información (Zona Extrema,	**Líder de Proceso y Asesor Oficina TIC despacho Alcalde**	• Proceder de manera inmediata a aplicar el plan de contingencia o de tratamiento de incidentes de seguridad de la información que permita la continuidad del servicio o el restablecimiento del mismo (si es el caso), documentar en el Plan de mejoramiento. • Iniciar el análisis de causas y determinar acciones preventivas y de mejora, documentar en el Plan de

Alta y Moderada)		Mejoramiento Institucional y replantear los riesgos del proceso. • Analizar y actualizar el mapa de riesgos. • Informar al Proceso de Planeación y Direccionamiento Estratégico sobre el hallazgo y las acciones tomadas.
		• Establecer acciones correctivas al interior de cada proceso, a cargo del líder respectivo y verificar la calificación y ubicación del riesgo para su inclusión en el mapa de riesgos.
Riesgos de Gestión y Seguridad de la Información (Zona Extrema, Alta y Moderada)	**Oficina de Control Interno de Gestión**	•Informar al líder del proceso sobre el hecho encontrado. • Informar a la segunda línea de defensa con el fin de facilitar el inicio de las acciones correspondientes con el líder del proceso, para revisar el mapa de riesgos. • Acompañar al líder del proceso en la revisión, análisis y toma de acciones correspondientes para resolver el hecho. • Verificar que se tomaron las acciones y se actualizó el mapa de riesgos correspondiente.
Riesgos de Proceso y Seguridad de la Información (Zona Baja)		•Informar al líder del proceso sobre el hecho • Informar a la segunda línea de defensa con el fin facilitar el inicio de las acciones correspondientes con el líder del proceso, para revisar el mapa de riesgos. • Acompañar al líder del proceso en la revisión, análisis y toma de acciones correspondientes para resolver el hecho. • Verificar que se tomaron las acciones y se actualizó el mapa de riesgos correspondiente.

El resultado de esta fase se concreta en un plan de tratamiento de riesgos, es decir, la selección y justificación de una o varias opciones para cada riesgo identificado, que permitan establecer la relación de riesgos residuales, es decir, aquellos que aún siguen existiendo a pesar de las medidas tomadas.

Nota: *Será conveniente que para la selección de los controles se consideren posibles restricciones o limitantes que impidan su elección tales como: restricciones de tiempo, financieras, técnicas, operativas, culturales, éticas, ambientales, legales, uso, de personal o las restricciones para la integración de controles nuevos y existentes. Adicionalmente se recomienda que para el periodo 2024 se realice una revisión del mapa de riesgos de seguridad de la información y se ajuste de acuerdo con lo que se estime conveniente.*

7.11 MONITOREO Y SEGUIMIENTO DE LOS RIESGOS DE SEGURIDAD DE LA INFORMACIÓN

Periódicamente se revisará el valor de los activos, impactos, amenazas, vulnerabilidades y probabilidades en busca de posibles cambios, que exijan la valoración iterativa de los riesgos de seguridad de la información.

Los riesgos son dinámicos como la misma Entidad por tanto podrá cambiar de forma o manera radical sin previo aviso. Por ello es necesaria una supervisión continua que detecte:

(1) nuevos activos o modificaciones en el valor de los activos,
(2) nuevas amenazas,
(3) cambios o aparición de nuevas vulnerabilidades,
(4) aumento de las consecuencias o impactos,
(5) incidentes de seguridad de la información.

Con el propósito de conocer los estados de cumplimiento de los objetivos de la gestión de los riesgos de seguridad de la información, se deberán definir esquemas de seguimiento y medición al sistema de gestión de riesgos de la seguridad de la información que permitan contextualizar una toma de decisiones de manera oportuna.

8. HISTORIAL DE CAMBIOS

VERSIÓN	DESCRIPCIÓN	FECHA
0.0	Original	19 de noviembre de 2019
1.0	Revisión y actualización	22 de febrero de 2023
2.0	Revisión y actualización	13 de diciembre de 2023