2026

PLAN DE TRATAMIENTO RIESGO DE SEGURIDAD DIGITAL

ALCALDÍA DE
BUCARAMANGA

MUNICIPIO DE BUCARAMANGA

Versión 4.0

PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD DIGITAL

MUNICIPIO DE BUCARAMANGA

Asesor de Despacho	Gestión de las TIC
	Mejoramiento Continuo

CONTROL DE CAMBIOS			
VERSIÓN	**FECHA**	**DESCRIPCIÓN DE AJUSTES**	**RESPONSABLE**
0.0	19-11-2019	Creación documento	Profesional Universitario
1.0	22-02-2022	Revisión y actualización	Profesional Universitario
2.0	13-12-2023	Revisión y actualización	Profesional Universitario
3.0	31-01-2025	Revisión y actualización	Profesional Universitario
4.0	30-01-2026	Se actualizó el plan de acción de actividades para 2025 para los riesgos definidos en el mapa de riesgos.	Asesor TIC

Nota: El control de cambios en el documento, se refiere a cualquier ajuste que se efectúe sobre el documento.

Si la aprobación se realizó mediante acta de alguno de los comités internos, por favor especificar acta y mes del desarrollo de la misma en la "*Descripción de Ajustes"*

Si este documento se encuentra impreso no se garantiza su vigencia, por lo tanto, es copia No Controlada. La versión vigente reposará en las carpetas del SGC de la Alcaldía de Bucaramanga.

CONTENIDO

1. INTRODUCCIÓN 3
2. OBJETIVO 3
2.1 OBJETIVOS ESPECÍFICOS 3
3. ALCANCE 3
4. DEFINCIONES Y/O ABREVITURAS 4
5. RESPONSABLES 5
5.1 ROLES PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD DIGITAL 5
6. CONDICIONES GENERALES 7
7. DOCUMENTOS DE REFERENCIA 7
8. NORMATIVIDAD 7
9. DESCRIPCIÓN Y/O DESARROLLO 10
9.1 CATEGORÍAS DE RIESGOS 10
9.2 IDENTIFICACIÓN DEL RIESGO 10
9.3 DESCRIPCIÓN DE CAUSAS 10
9.4 CONSECUENCIAS 11
9.5 BARRERAS DE SEGURIDAD EXISTENTES 11
9.6 VISIÓN PROCESO DE GESTIÓN DE RIESGO EN LA SEGURIDAD DIGITAL 11
9.7 ESTABLECIMIENTO DEL CONTEXTO DE RIESGOS DE SEGURIDAD DIGITAL 12
9.8 VALORACIÓN DE LOS RIESGOS DE SEGURIDAD DIGITAL 13
9.8.1 Identificación del riesgo 13
9.8.2. Estimación del riesgo 15
9.8.3 Determinación del riesgo inherente y residual 17
9.8.4 Evaluación de los riesgos 18
9.8.5 Mapa de riesgos de Seguridad de la Información 18
9.8.6 Tratamiento de los riesgos de Seguridad Digital 19
9.8.7 Monitoreo y seguimiento de los riesgos de Seguridad de la Información 19

CONTENIDO DE TABLA

Tabla 1 Roles y responsabilidades 5
Tabla 2 Normatividad 9

CONTENIDO DE ILUSTRACIÓN

Ilustración 1 Modelo de gestión de riesgos de seguridad digital basada tanta en la norma ISO/IEC 31000 ..... **Error! Bookmark not defined.**
Ilustración 2 Criterios para definir el nivel de probabilidad Riesgos en activos de información Adaptado para la Alcaldía de la Guía de Riesgos DAFP, 2022 16
Ilustración 3 Criterios para definir el nivel de impacto Riesgos en activos de información 16
Ilustración 4 Matriz de riesgo 17
Ilustración 5 Esquema general de Matriz de Riesgo Institucional y Zonas de Riesgo Institucional para la Alcaldía – adaptado del DAFP. 17

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.

2. OBJETIVO

Desarrollar e implementar el plan de tratamiento de riesgos de seguridad digital para la Alcaldía de Bucaramanga durante la vigencia 2026, con el fin de identificar, evaluar y mitigar los riesgos asociados a la gestión de la información y la infraestructura tecnológica, asegurando la protección de los datos y el cumplimiento de las normativas vigentes, contribuyendo a una gestión pública más segura, eficiente y confiable.

2.1 OBJETIVOS ESPECÍFICOS

- Identificar y evaluar riesgos de seguridad digital en la infraestructura tecnológica y procesos de información de la Alcaldía.
- Implementar controles de seguridad para mitigar los riesgos y proteger la información sensible.
- Capacitar al personal en buenas prácticas y políticas de seguridad digital.
- Monitorear y actualizar continuamente el plan de seguridad para adaptarse a nuevas amenazas y normativas.

3. ALCANCE

El Plan de Tratamiento de Riesgos de Seguridad Digital aplica a todos los procesos, sistemas y recursos tecnológicos de la Alcaldía de Bucaramanga que gestionen información institucional, con el fin de identificar, evaluar y mitigar los riesgos, garantizando la protección de los datos y el cumplimiento de la normativa vigente en 2026.

4. 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 esta (sistemas, soportes, edificios, personas…) que tenga valor para la organización. (ISO/IEC 27000).

- **Amenazas:** Causa potencial de un incidente no deseado, que puede provocar o 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 auditoría y obviamente para determinar el grado en el que se cumplen los criterios de auditoría. (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 oentidad. (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.

5. RESPONSABLES

Asesor de despacho Oficina Asesora TIC

5.1 Roles plan de tratamiento de Riesgos de Seguridad Digital

En esta sección se definen los roles y responsabilidades asignados dentro del Plan de Tratamiento de Riesgos de Seguridad Digital, con el objetivo de asegurar su correcta implementación y cumplimiento.

Tabla 1 Roles y responsabilidades

LÍNEAS DE DEFENSA	RESPONSABLE	DESCRIPCION
Estratégica	Alta Dirección - alcalde Municipal, Comité Institucional de	• Establecer y aprobar el PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD DIGITAL
	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 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.

Fuente: Elaboración propia

6. CONDICIONES GENERALES

El Documento de Tratamiento de Seguridad Digital aplica a todos los procesos, dependencias, servidores públicos, contratistas y terceros que tengan acceso o manejo de los activos de información de la entidad, sin importar el medio o formato en que estos se gestionen. Las medidas y controles definidos deberán implementarse de forma gradual, considerando el nivel de riesgo, la criticidad de los activos, la disponibilidad de recursos y las prioridades institucionales, en coherencia con el Mapa de Riesgos Institucional y el Mapa de Riesgos de Seguridad de la Información.

La implementación y el seguimiento de las acciones de tratamiento son responsabilidad de los líderes de proceso y las áreas correspondientes, con el acompañamiento de la Oficina TIC y la Oficina de Control Interno. Este documento será revisado y actualizado periódicamente, o cuando se presenten cambios relevantes en el entorno institucional, tecnológico o normativo, y su incumplimiento podrá generar consecuencias operativas, legales o disciplinarias conforme a la normatividad vigente.

7. DOCUMENTOS DE REFERENCIA

Todos los documentos nombrados se relacionan en el LISTADO MAESTRO DE DOCUMENTOS DEL SISTEMA INTEGRADO DE GESTION DE LAS TIC Código: F-GDO-8600-238,37-002

8. 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	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 de2019

Tabla 2 Normatividad

Fuente: Elaboración propia

9. DESCRIPCIÓN Y/O DESARROLLO

Este Plan de Tratamiento de Seguridad Digital establece las acciones necesarias para mitigar los riesgos que amenazan los activos de información de la entidad. A través de la implementación de controles técnicos y administrativos, se busca reducir la vulnerabilidad frente a ataques cibernéticos y asegurar la continuidad operativa. El documento garantiza el cumplimiento normativo y protege la confidencialidad, integridad y disponibilidad de los datos institucionales. Así, se fortalece la resiliencia tecnológica y se promueve una cultura de gestión del riesgo proactiva y alineada con los objetivos estratégicos.

9.1 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.

9.2 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.

9.3 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.

9.4 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.

9.5 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).

9.6 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:

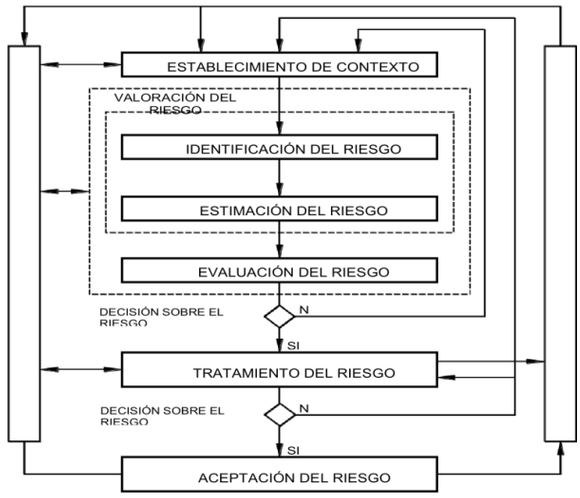

Ilustración 1 Modelo de gestión de riesgos de seguridad digital basada tanta en la norma ISO/IEC 31000

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

9.7 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:

- 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.

- 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.

- 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.

9.8 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

9.8.1 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**

✓ **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.

✓ **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.

✓ **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**

✓ **Hardware**: Consta de todos los elementos físicos que dan soporte a los procesos (PC, portátiles, servidores, impresoras, discos, documentos en papel, etc.).

✓ **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.)

✓ **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.)

✓ **Personal**: Consiste en todos los grupos de personas involucradas en el sistema de información (usuarios, desarrolladores, responsables, etc.)

✓ **Sitio**: Comprende todos los lugares en los cuales se pueden aplicar los medios de seguridad de la organización (Edificios, salas, y sus servicios, etc.)

✓ **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.

9.8.2. 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%	

Ilustración 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	

Ilustración 3 Criterios para definir el nivel de impacto Riesgos en activos de información

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.

9.8.3 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.

Ilustración 4 Matriz de riesgo

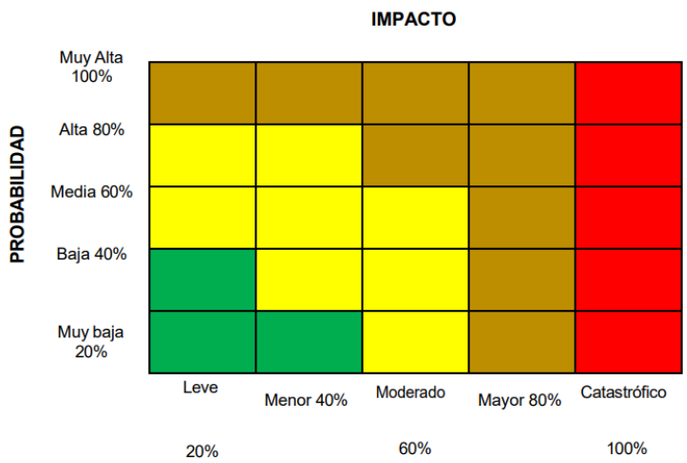

Ilustración 5 Esquema general de Matriz de Riesgo Institucional y Zonas de Riesgo Institucional para la Alcaldía – adaptado del DAFP.

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.

9.8.4 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.

9.8.5 Mapa de riesgos de Seguridad de la Información

En coherencia con los resultados obtenidos durante la vigencia anterior, y considerando la efectividad de la estrategia implementada, para el año 2026 la Alcaldía de Bucaramanga dará continuidad al proceso de actualización de los Mapas de Riesgos de Seguridad de la Información. Esta continuidad permitirá fortalecer el enfoque preventivo, asegurar la trazabilidad de los riesgos identificados y mantener la alineación con los objetivos institucionales y normativos en materia de seguridad de la información.

La actualización de los mapas de riesgos se realizará de manera articulada con los líderes de proceso, jefes de las dependencias y enlaces designados por cada dependencia, garantizando así un enfoque participativo, integral y acorde con la realidad operativa de cada proceso. Este ejercicio permitirá identificar oportunamente nuevas amenazas, vulnerabilidades y riesgos emergentes, así como ajustar los controles existentes frente a cambios tecnológicos, organizacionales o normativos.

Desde la Oficina Asesora TIC, en su rol de segunda línea de defensa, se liderará y acompañará estratégicamente el proceso, brindando lineamientos técnicos, metodológicos y de seguridad de la información, así como asesoría permanente a las dependencias. Este acompañamiento busca fortalecer la gestión del riesgo, promover la cultura de seguridad de la información y asegurar la correcta implementación de las acciones definidas, contribuyendo al cumplimiento del Modelo Integrado de Planeación y Gestión (MIPG) y a la protección de los activos de información de la entidad.

9.8.6 Tratamiento de los riesgos de Seguridad Digital

Como resultado de la etapa de evaluación del riesgo, se contará con una lista priorizada de riesgos o con una matriz de riesgos que permita identificar los niveles de riesgo de acuerdo con su zona de ubicación. Con base en esta valoración y en los criterios definidos dentro del contexto de la gestión del riesgo, se deberá seleccionar la(s) estrategia(s) de tratamiento más adecuada(s), tales como aceptar, reducir, compartir o evitar el riesgo.

En concordancia con la Guía para la Administración del Riesgo del Departamento Administrativo de la Función Pública (DAFP), cada líder de proceso o jefe de dependencia será el responsable directo de la formulación, ejecución y cumplimiento de los planes de acción asociados a los riesgos identificados en su respectivo ámbito de gestión. Cada dependencia deberá establecer acciones concretas orientadas a mitigar los riesgos, de acuerdo con su nivel de impacto y probabilidad, garantizando la implementación o fortalecimiento de los controles definidos.

La Oficina Asesora TIC, en su rol de segunda línea de defensa, brindará acompañamiento y orientación técnica para la formulación de los planes de acción, así como para el seguimiento a su implementación, con el fin de fortalecer los controles existentes y contribuir a la protección de los activos de información institucionales.

9.8.7 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 contextualiza runa toma de decisiones demanera oportuna.

ALCALDÍA DE
BUCARAMANGA