PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN	
Documento	Plan de Tratamiento de Riesgos de Seguridad de la Información.
Versión	5.0
Descripción	Documento con la actualización del Plan de Tratamiento de Riesgos de Seguridad de la Información, Este documento define el marco de actuación y las actividades adecuadas para el proceso de gestión de riesgos de seguridad de la información en la Alcaldía Distrital de Barrancabermeja.
Fecha	20/01/2023

Control de Cambios		
Versión	Fecha	Descripción
1.0	30/01/2018	Creación
2.0	30/01/2019	Actualización
3.0	30/10/2020	Actualización
4.0	16/12/2021	Actualización
5.0	**20/02/2023**	**Actualización**

Versión	Fecha	Descripción	Elaboró	Aprobó
5.0	20/01/2023	Actualización del Documento	Ing. Marino Rodríguez Palacios	Ing. Adriana Marcela Carvajal Quintero Secretaria de las TIC, Ciencia e Innovación

CONTENIDO

INTRODUCCIÓN

La Alcaldía Distrital de Barrancabermeja maneja datos en sus procesos, trámites, servicios, sistemas, infraestructura tecnológica y en general en todos sus activos de información que, sin un debido tratamiento de riesgos para salvaguardar la información frente a posibles incidentes de seguridad que pueden generar fuga, robo o modificación no autorizada de la información, afectando los procesos y el logro de los objetivos institucionales. La información referente a los procesos es almacenada y tratada tanto de forma física como digital y se hace necesario brindar una adecuada protección adoptando estrategias y mecanismos que garanticen su integridad, confidencialidad y disponibilidad.

El Ministerio de las Tecnologías de la Información y las Comunicaciones (MinTIC) a través del Manual de Gobierno Digital establece lineamientos para el uso y aprovechamiento eficiente de las TIC en las entidades del estado, así mismo busca fortalecer el funcionamiento de los procesos tanto internos como externos de las entidades públicas por medio del uso de las Tecnologías de la Información y consolidar la relación del estado con la sociedad en un entorno confiable y digital.

La política de Gobierno Digital contempla tres habilitadores transversales que son esenciales para el avance y el cumplimiento de los propósitos de la política, uno de ellos es el de Seguridad y Privacidad de la Información que tiene como objetivo orientar a las entidades públicas para que adopten lineamientos y buenas prácticas de seguridad con el fin de proteger la información de sus procesos misionales, trámites y servicios, así como de su infraestructura tecnológica y activos de información, sustentado en el Modelo de Seguridad y Privacidad de la Información (MSPI).

El Modelo de Seguridad y Privacidad de la Información (MSPI) basado en los tres pilares fundamentales como lo son la Integridad, confidencialidad y la disponibilidad de la información establece una serie de lineamientos enfocados a garantizar las mejores prácticas en Seguridad y Privacidad de la Información promoviendo estrategias que permitan establecer una adecuada gestión de riesgos de seguridad de la información, el cual es indispensable para el cumplimiento de los objetivos misionales y la toma de decisiones por parte de la entidad.

De acuerdo a lo mencionado anteriormente, la Alcaldía Distrital de Barrancabermeja define el siguiente Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la información para la vigencia 2022, el cual se encuentra alineado con las directrices establecidas en la Política de Administración del Riesgo de la entidad. Este plan establece un marco de actuación y define los procedimientos y actividades necesarios para lograr una adecuada administración del riesgo y ejecución de controles, estableciendo una estrategia de seguridad digital efectiva que permita mitigar los riesgos asociados a los activos de información de la entidad.

OBJETIVO GENERAL

Definir e implementar los lineamientos que permitan tratar de manera adecuada e integral los riesgos de seguridad y privacidad de la información, estableciendo un marco de actuación y definiendo una estrategia para identificar y controlar posibles afectaciones a los activos de información que soportan los procesos misionales y el logro de los objetivos institucionales en la Alcaldía Distrital de Barrancabermeja.

PROPÓSITOS

- Establecer lineamientos para la identificación, análisis, valoración y tratamiento de los riesgos de seguridad digital para los activos de información de la entidad,

- Implementar acciones preventivas y correctivas con el fin de anticipar eventos no deseados.

- Gestionar los riesgos de seguridad y privacidad de la información de acuerdo al contexto organizacional y los procesos institucionales.

- Cumplir con los requisitos legales y normativos pertinentes con la gestión de riesgos de seguridad y privacidad de la información e incidentes de seguridad digital.

- Establecer una guía de gestión de riesgos de seguridad y privacidad de la información para los líderes de proceso y servidores públicos de la Alcaldía Distrital de Barrancabermeja.

ALCANCE

Los lineamientos establecidos en el presente plan de tratamiento de riesgos de seguridad y privacidad de la información son aplicables a los procesos misionales, de apoyo, de evaluación y estratégicos, así mismo deberán ser aplicados por funcionarios, contratistas, proveedores y partes interesadas vinculadas a la entidad y que en el ejercicio de sus funciones accedan a los activos de información de la Alcaldía Distrital de Barrancabermeja.

MARCO NORMATIVO

La actualización del siguiente Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información se define teniendo en cuenta la normatividad descrita a continuación.

NORMATIVIDAD	ACTUALIZACIÓN	DESCRIPCIÓN
Guía de Administración del Riesgo (DAFP) V5	2020	Guía para la administración del riesgo y el diseño de controles en entidades públicas.
Guía No.7 de Riesgos MINTIC	2016	Guía de Gestión de Riesgos No.7
Resolución Número 00500 de marzo 10 de 2021	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
Anexo 1. Modelo de Seguridad y Privacidad de la Información	2021	Documento Maestro del Modelo de Seguridad y Privacidad de la Información Versión 4.
Norma técnica colombiana NTC - ISO/IEC 27001	2013	Estándar internacional para la implementación de un Sistema de Gestión de Seguridad de la Información.
Decreto 1078 de 2015	2021	Por medio del cual se expide el Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones
Decreto 1008 de 2018	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.
Documento CONPES 3854	2016	Política Nacional de Seguridad Digital.
Documento CONPES 3995	2020	Política Nacional de Confianza y Seguridad Digital.

Ley 1712 de 2014	2014	Por medio de la cual se crea la Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional y se dictan otras disposiciones.
Ley 1581 de 2012	2012	Por la cual se dictan disposiciones generales para la protección de datos personales.

Tabla 1. Marco Normativo

DEFINICIONES

Activos de Información: Hace referencia a los elementos de hardware y de software de procesamiento, almacenamiento y comunicaciones, bases de datos y procesos, procedimientos y recursos humanos asociados con el manejo de los datos y la información misional, operativa y administrativa de cada entidad, órgano u organismo.

Amenaza: Causa potencial de un incidente no deseado, que puede provocar daños a un sistema o a la organización.

Bases de Datos Personales: Conjunto organizado de datos personales que sea objeto de tratamiento.

Causa: todos aquellos factores internos y externos que solos o en combinación con otros, pueden producir la materialización de un riesgo.

Contexto interno

Ambiente interno en el cual la organización busca alcanzar sus objetivos.

Contexto externo

Ambiente externo en el cual la organización busca alcanzar sus objetivos.

Control: Medida que permite reducir o mitigar el riesgo.

Entorno digital: Ambiente, tanto físico como virtual sobre el cual se soporta la economía digital. Siendo esta última la economía basada en tecnologías, cuyo desarrollo y despliegue se produce en un ecosistema caracterizado por la creciente y acelerada convergencia entre diversas tecnologías, que se concreta en redes de comunicación, equipos de hardware, servicios de procesamiento y tecnologías web.

Factores de Riesgo: Son las fuentes generadoras de riesgos.

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.

Impacto: Las consecuencias que puede ocasionar a la organización la materialización del riesgo.

Incidente: Cualquier evento adverso real o sospechado, intencionado o no intencionado, que puede cambiar el curso esperado de una actividad en el entorno digital.

Información Pública: Es toda información que un sujeto obligado genere, obtenga, adquiera, o controle en su calidad de tal.

Información Pública Clasificada: Es aquella información que estando en poder o custodia de un sujeto obligado en su calidad de tal, pertenece al ámbito propio, particular y privado o semiprivado de una persona natural o jurídica por lo que su acceso podrá ser negado o exceptuado, siempre que se trate de las circunstancias legítimas y necesarias y los derechos particulares o privados consagrados en el artículo 18 de la Ley 1712 de 2014.

Información Pública Reservada: Es aquella información que estando en poder o custodia de un sujeto obligado en su calidad de tal, es exceptuada de acceso a la ciudadanía por daño a intereses públicos y bajo cumplimiento de la totalidad de los requisitos consagrados en el artículo 19 de la Ley 1712 de 2014.

MGRSD: Modelo de Gestión de Riesgos de Seguridad Digital.

Nivel de riesgo: Es el valor que se determina a partir de combinar la probabilidad de ocurrencia de un evento potencialmente dañino y la magnitud del impacto que este evento traería sobre la capacidad institucional de alcanzar los objetivos.

Probabilidad: Se entiende la posibilidad de ocurrencia del riesgo. Estará asociada a la exposición al riesgo del proceso o actividad que se esté analizando. La probabilidad inherente será el número de veces que se pasa por el punto de riesgo en el periodo de un año.

Propietario: Es una parte designada de la entidad, un cargo, proceso, o grupo de trabajo que tiene la responsabilidad de garantizar que la información y los activos asociados con el proceso se clasifican adecuadamente.

Riesgo: Efecto que se causa sobre los objetivos de las entidades, debido a eventos potenciales.

Riesgo de Seguridad de la Información: 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/IEC 27000).

Riesgo informático: Posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información. (ISO Guía73:2002).

Riesgo Inherente: Nivel de riesgo propio de la actividad. El resultado de combinar la probabilidad con el impacto, nos permite determinar el nivel del riesgo inherente, dentro de unas escalas de severidad.

Riesgo Residual: El resultado de aplicar la efectividad de los controles al riesgo inherente.

Seguridad de la información: Preservación de la confidencialidad, integridad, y disponibilidad de la información en cualquier medio: impreso o digital.

Seguridad digital: Preservación de la confidencialidad, integridad, y disponibilidad de la información que se encuentra en medios digitales.

Vulnerabilidad: Es una debilidad, atributo o falta de control que puede ser explotada por una o más amenazas.

POLÍTICA DE ADMINISTRACIÓN DEL RIESGO

La Alcaldía Distrital de Barrancabermeja definió su Política de Administración del Riesgo, la cual se encuentra alineada a la metodología planteada por el Departamento Administrativo de la Función Pública y las demás disposiciones legales y normativas impartidas sobre la materia. Esta política establece los lineamientos para la administración de los riesgos incluidos los de seguridad de la información y permite fomentar una cultura de mejoramiento continuo en sus procesos mediante acciones preventivas y correctivas para asumir, reducir y mitigar los riesgos e implementar los controles necesarios para anticiparse a eventos indeseados.

El presente plan de tratamiento de riesgos se encuentra alineado con la Política de Riesgos de la entidad, este plan de tratamiento pretende definir las acciones y métodos a seguir para gestionar los riesgos de seguridad de la información de manera integral, identificando las necesidades de la entidad con respecto a los requisitos para la protección de la confidencialidad, integridad y disponibilidad de todos los activos de información.

PLANIFICACIÓN

IDENTIFICACIÓN DEL RIESGO

IDENTIFICACIÓN DE LAS ÁREAS DE IMPACTO

En este punto se debe tener en cuenta la consecuencia económica o reputacional a la que se encuentra expuesta la Alcaldía Distrital de Barrancabermeja, si el riesgo llega a materializarse.

- Afectación económica
- Afectación reputacional

Designación de roles y responsabilidades

Para el presente plan de tratamiento de riesgos de seguridad de la información se describen las responsabilidades definidas en la Política de Administración del Riesgo de la Alcaldía Distrital de Barrancabermeja.

LINEA DE ESTRATEGICA: Alta Dirección, Comité Institucional de Coordinación de Control Interno y Comité Institucional de Gestión y Desempeño.

PRIMERA LINEA DE DEFENSA: Los líderes de los procesos con el apoyo de sus grupos de trabajo.

SEGUNDA LINEA DE DEFENSA: Secretaría de Planeación Municipal, Oficina Asesora de Prensa, Comunicaciones y Protocolo, Secretaría de las Tecnologías de la Información y Comunicaciones, TIC.

TERCERA LÍNEA DE DEFENSA: Oficina Asesora de Control Interno.

IDENTIFICACIÓN DE LAS ÁREAS DE FACTORES DE RIESGO

Define las fuentes generadoras del riesgo. A continuación, se describen algunos factores de riesgo que podrán ser tenidos en cuenta durante el proceso de gestión de riesgos de seguridad de la información.

FACTOR	DEFINICIÓN	DESCRIPCIÓN
Procesos	Eventos relacionados con errores en las actividades que deben realizar los servidores de la organización.	Falta de procedimientos
		Errores de grabación, autorización
		Errores en cálculos para pagos internos y externos
		Falta de capacitación, temas relacionados con el personal
Talento humano	Incluye seguridad y salud en el trabajo. Se analiza posible dolo e intención frente a la corrupción.	Hurto de activos
		Posibles comportamientos no éticos de los empleados
		Fraude interno (corrupción, soborno)
Tecnología		Daño de equipos
		Caída de aplicaciones

	Eventos relacionados con la infraestructura tecnológica de la entidad.	Caída de redes
		Errores en programas
Infraestructura	Eventos relacionados con la infraestructura física de la entidad.	Derrumbes
		Incendios
		Inundaciones
		Daños a activos fijos
Evento externo	Situaciones externas que afectan la entidad.	Suplantación de identidad
		Asalto a la oficina
		Atentados, vandalismo, orden público

Tabla 2. Factores de Riesgo.
Fuente: Adaptado Guía de Administración del Riesgo (DAFP)

CLASIFICACIÓN DEL RIESGO

Define las fuentes generadoras del riesgo. A continuación, se describen algunos factores de riesgo que podrán ser tenidos en cuenta durante el proceso de gestión de riesgos de seguridad de la información.

CLASIFICACIÓN DEL RIESGO	
Ejecución y administración de procesos	Pérdidas derivadas de errores en la ejecución y administración de procesos.
Fraude externo	Pérdida derivada de actos de fraude por personas ajenas a la organización (no participa personal de la entidad).
Fraude interno	Pérdida debido a actos de fraude, actuaciones irregulares, comisión de hechos delictivos abuso de confianza, apropiación indebida, incumplimiento de regulaciones legales o internas de la entidad en las cuales están involucrado por lo menos 1 participante interno de la organización, son realizadas de forma intencional y/o con ánimo de lucro para sí mismo o para terceros.
Fallas tecnológicas	Errores en hardware, software, telecomunicaciones, interrupción de servicios básicos.
Relaciones laborales	Pérdidas que surgen de acciones contrarias a las leyes o acuerdos de empleo, salud o seguridad, del pago de demandas por daños personales o de discriminación.
Usuarios, productos y prácticas	Fallas negligentes o involuntarias de las obligaciones frente a los usuarios y que impiden satisfacer una obligación profesional frente a éstos.
Daños a activos fijos/ eventos externos	Pérdida por daños o extravíos de los activos fijos por desastres naturales u otros riesgos/eventos externos como atentados, vandalismo, orden público.

Tabla 3. Factores de Riesgo.
Fuente: Adaptado Guía de Administración del Riesgo (DAFP)

IDENTIFICACIÓN Y GESTIÓN DE LOS ACTIVOS DE INFORMACIÓN

Dentro del proceso de gestión del riesgo es indispensable contar con el inventario de activos de información identificados para cada uno de los procesos de la entidad.

La consolidación del inventario de activos de información permite organizar y clasificar los activos facilitando la implementación de controles y medidas de seguridad de acuerdo a su nivel de criticidad.

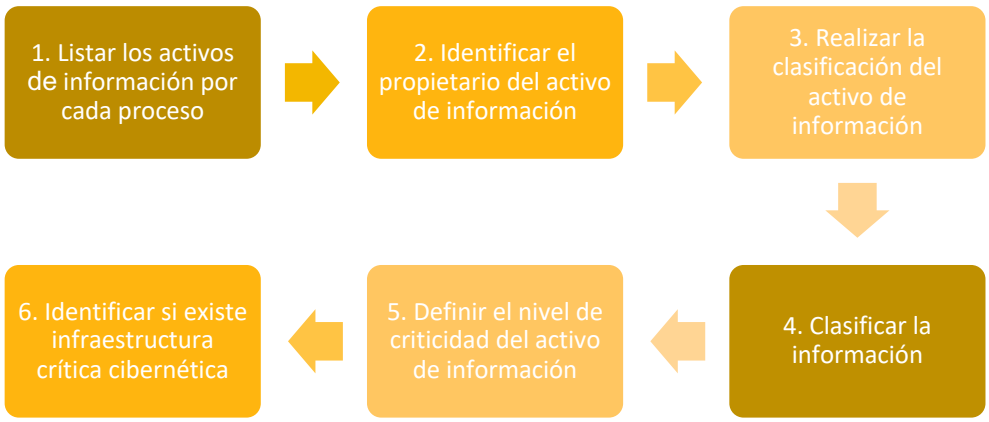

Imagen1. Identificación de Activos de Información.
Fuente: Modelo de gestión de riesgos de seguridad Digital (MINTIC)

1. Listar los activos de información por cada proceso

Listar los activos de información según el alcance establecido y de acuerdo al mapa de procesos de la Alcaldía de Barrancabermeja.

2. Identificar el propietario del activo de información

La entidad debe designar una parte, cargo, líder de proceso, grupo de trabajo o jefe de oficina que asuma la responsabilidad de garantizar que los activos de información que soportan la operación de los procesos de la entidad cuenten con una adecuada protección.

3. Realizar la clasificación del activo de información

Según la naturaleza de cada activo, este debe pertenecer a un determinado grupo o contar con una clasificación especifica.

TIPO DE ACTIVO	DESCRIPCIÓN
Información	Información almacenada en formatos físicos (papel, carpetas, CD, DVD) o en formatos digitales o electrónicos (ficheros en bases de datos, correos electrónicos, archivos o servidores), teniendo en cuenta lo anterior, se puede distinguir como información: Contratos, acuerdos de confidencialidad, manuales de usuario, procedimientos operativos o de soporte, planes para la continuidad del negocio, registros contables, estados financieros, archivos ofimáticos, documentos y registros del sistema integrado de gestión, bases de datos con información personal o con información relevante para algún proceso (bases de datos de nóminas, estados financieros) entre otros.
Software	Activo informático lógico como programas, herramientas ofimáticas o sistemas lógicos para la ejecución de las actividades.
Hardware	Equipos físicos de cómputo y de comunicaciones como, servidores, que por su criticidad son considerados activos de información.
Intangibles	Se consideran intangibles aquellos activos inmateriales que otorgan a la entidad una ventaja competitiva relevante, uno de ellos es la imagen corporativa, reputación, entre otros.
Componentes de red	Medios necesarios para realizar la conexión de los elementos de hardware y software en una red, por ejemplo, el cableado estructurado y tarjetas de red, routers, switches, entre otros.
Personas	Aquellos roles que, por su conocimiento, experiencia y criticidad para el proceso, son considerados activos de información, por ejemplo: personal con experiencia y capacitado para realizar una tarea específica en la ejecución de las actividades.
Instalaciones	Espacio o área asignada para alojar y salvaguardar los datos considerados como activos críticos para la empresa.

Tabla 4. Tipología de Activos de Información.
Fuente: Modelo de gestión de riesgos de seguridad Digital (MINTIC)

4. Clasificar la información

El método de clasificación establecido tiene como principio rector la confidencialidad de la información, teniendo en cuenta lo establecido en la Ley 1712 de 2014 y Ley 1581 de 2012, así

mismo define los principios fundamentales de confidencialidad, integridad y disponibilidad como propiedades donde para cada una se deben definir criterios propios para un adecuado tratamiento de los activos.

CONFIDENCIALIDAD	DESCRIPCIÓN	INTEGRIDAD	DISPONIBILIDAD
Información Pública Reservada	Es aquella información que estando en poder o custodia de un sujeto obligado en su calidad de tal, es exceptuada de acceso a la ciudadanía por daño a intereses públicos y bajo cumplimiento de la totalidad de los requisitos consagrados en el artículo 19 de la ley 1712 de 2014 Ej.: defensa y seguridad nacional, derechos de infancia y adolescencia, salud pública.	ALTA	ALTA
Información Pública Clasificada	Es aquella información que estando en poder o custodia de un sujeto obligado en su calidad de tal, pertenece al ámbito propio, particular y privado o semiprivado de una persona natural o jurídica por lo que su acceso podrá ser negado o exceptuado, siempre que se trate de las circunstancias legítimas y necesarias y los derechos particulares o privados consagrados en el artículo 18 de la ley 1712 de 2014. Ej: datos personales y secretos comerciales.	MEDIA	MEDIA
Información Pública	Es toda información que un sujeto obligado genere, obtenga, adquiera, o controle en su calidad de tal.	BAJA	BAJA

Tabla 5. Criterios de Clasificación de la Información.
Fuente: Guía para la Gestión y Clasificación de Activos de Información - (MINTIC)

5. Definir el nivel de criticidad del activo de información

Para este punto la entidad debe definir los niveles (que significa criticidad ALTA, MEDIA y BAJA) para valorar los activos identificados frente a los principios de confidencialidad, integridad y disponibilidad, estableciendo el nivel de importancia o criticidad para el proceso.

NIVEL	DESCRIPCION
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.

Tabla 6. Niveles de Clasificación.
Fuente: Guía para la Gestión y Clasificación de Activos de Información - (MINTIC)

6. Identificar si existe infraestructura crítica cibernética

Se debe identificar si dentro de la entidad se cuenta con un activo de información considerado como Infraestructura Critica Cibernética ICC, teniendo en cuenta los siguientes criterios frente a su impacto o afectación:

TIPO IMPACTO	Impacto Social (0,5%) de Población Nacional	Impacto Económico PIB de un Día o 0,123% del PIB Anual	Impacto Ambiental
AFECTACIÓN	250.000 personas $464.619.736 3 años en recuperación	250.000 personas $464.619.736 3 años en recuperación	250.000 personas $464.619.736 3 años en recuperación

Tabla 7. Identificación de infraestructura crítica cibernética (ICC).
Fuente: Guía para la Gestión y Clasificación de Activos de Información - (MINTIC)

La entidad debe establecer si para el proceso de gestión de riesgos tiene en cuenta todos los activos de información identificados o si por el contrario solo se aplicaría a los activos que contengan un nivel de criticidad alto.

IDENTIFICACIÓN DEL RIESGO INHERENTE

Para el proceso de gestión de riesgos de seguridad de la información es fundamental identificar los siguientes riesgos inherentes.

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

Según lo estipulado por la Guía de Administración del riesgo emitida por el Departamento Administrativo de la Función Pública (DAFP) se establece que “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.”

IDENTIFICACIÓN DE AMENAZAS Y VULNERABILIDADES

La amenaza desde un enfoque de seguridad de la información tiene el potencial de explotar una vulnerabilidad y causar daño sobre los activos de información que soportan la operación de los procesos y por ende los servicios prestados por la Alcaldía Distrital de Barrancabermeja. Algunas amenazas de llegar a materializarse pueden causar afectación a varios activos y en algunos casos puede causar diferentes impactos de acuerdo al nivel de criticidad del activo afectado.

A continuación, se describen algunos ejemplos de amenazas y vulnerabilidades que se pueden tener en cuenta.

Tipo de activo	Vulnerabilidades	Amenazas
Hardware	Almacenamiento de medios sin protección	Hurto de medios o documentos
	Mantenimiento insuficiente/ Instalación fallida de los medios de almacenamiento	Incumplimiento en el mantenimiento del sistema de información
	Ausencia de esquemas de reemplazo periódico	Destrucción de equipos o medios
	Susceptibilidad a la humedad, el polvo y la suciedad	Polvo, corrosión y congelamiento

	Sensibilidad a la radiación electromagnética	Radiación electromagnética
Software	Ausencia de parches de seguridad	Abuso de los derechos
	Ausencia de “terminación de sesión” cuando se abandona la estación de trabajo	Abuso de los derechos
	Asignación errada de los derechos de acceso	Abuso de los derechos
	Ausencia de documentación	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 las contraseñas	Falsificación de derechos
	Habilitación de servicios innecesarios	Procesamiento ilegal de datos
	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
Red	Líneas de comunicación sin protección	Escucha encubierta
	Líneas de comunicación sin protección	Escucha encubierta
	Tráfico sensible sin protección	Escucha encubierta
	Conexión deficiente de los cables	Fallas del equipo de telecomunicaciones
	Punto único de fallas	Fallas del equipo de telecomunicaciones
	Arquitectura insegura de la red	Espionaje remoto
	Conexiones de red pública sin protección	Uso no autorizado del equipo
Información	Falta de controles de acceso físico	Hurto de información

Personal	Falta de capacitación en las herramientas	Error en el uso
	Ausencia del personal	Incumplimiento en la disponibilidad del personal
	Uso incorrecto de software y hardware	Error en el uso
	Ausencia de políticas para el uso correcto de los medios de telecomunicaciones y mensajería	Uso no autorizado del equipo
Organización	Ausencia de políticas de seguridad	Abuso de los derechos
	Ausencia de procedimiento formal para el registro y retiro de usuarios	Abuso de los derechos
	Ausencia de proceso formal para la revisión de los derechos de acceso	Abuso de los derechos
	Ausencia de procedimientos de monitoreo de los recursos de procesamiento de la información	Abuso de los derechos
	Ausencia de procedimientos de identificación y valoración de riesgos	Abuso de los derechos
	Respuesta inadecuada de mantenimiento del servicio	Incumplimiento en el mantenimiento del sistema de información
	Ausencia de políticas sobre el uso de correo electrónico	Error en el uso

Tabla 8. Amenazas y vulnerabilidades.
Fuente: Guía para la Gestión y Clasificación de Activos de Información - (MINTIC)

Es necesario tener en cuenta en esta fase que la sola presencia de una vulnerabilidad de un activo o de un control no causa daños por sí misma, para que la vulnerabilidad pueda ser afectada debe existir una amenaza que pueda explotar dicha vulnerabilidad.

VALORACIÓN DEL RIESGO

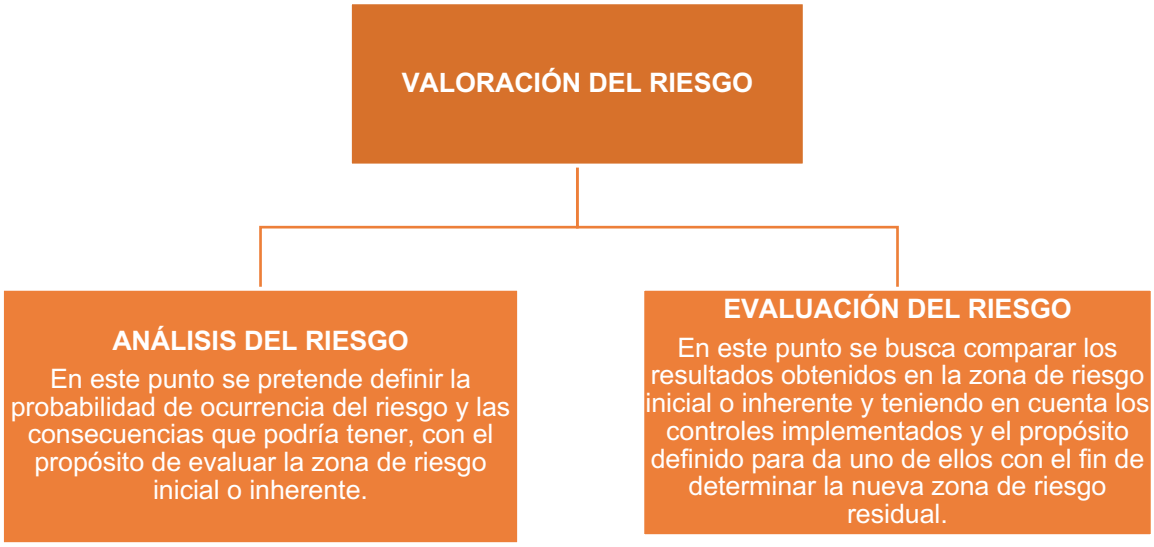

Imagen2. Valoración del riesgo.
Fuente: Elaboración propia

ANÁLISIS DEL RIESGO

En esta etapa se pretende definir la probabilidad de ocurrencia del riesgo y las consecuencias que podría tener, con el propósito de evaluar la zona de riesgo inicial o inherente.

TABLA DE PROBABILIDAD			
CALIFICACIÓN	**NIVEL**	**FRECUENCIA DE LA ACTIVIDAD**	**PROBABILIDAD**
Muy Baja	1	La actividad se realiza 4 veces por año	20%
Baja	2	La actividad se realiza mínimo 5 veces y máximo 12 veces al año	40%
Media	3	La actividad se realiza mínimo 13 veces y	60%

		máximo 365 veces al año	
Alta	4	La actividad se realiza mínimo 365 veces y máximo 3660 veces al año	80%
Muy Alta	5	La actividad se realiza mínimo 3661 veces o más al año	100%

Tabla 9. Tabla de probabilidad.
Fuente: Guía de administración del riesgo V5 (DAFP)

TABLA DE IMPACTO				
CALIFICACIÓN	**NIVEL**	**AFECTACION ECONOMICA**	**REPUTACIONAL**	**PORCENTAJE**
Insignificante	1	Afectación menor a 10 SMLMV	Solo de conocimiento de algunos funcionarios	20%
Menor	2	Mayores o iguales a 10 SMLMV y menores a 21 SMLMV	De conocimiento general de la entidad a nivel interno, de alta dirección y nivel directivo	40%
Moderado	3	Mayores o iguales a 21 SMLMV y menores a 318 SMLMV	Afecta imagen con algunos usuarios que impacten significativamente los objetivos	60%
Mayor	4	Mayores o iguales a 318 SMLMV y menores a 2120 SMLMV	Deterioro de imagen con efecto publicitario negativo a nivel municipal o departamental	80%
Catastrófico	5	Mayores a a 2120 SMLMV	Deterioro de imagen a nivel nacional, con efecto publicitario negativo a nivel país	100%

Tabla 10. Tabla de impacto.
Fuente: Guía de administración del riesgo V5 (DAFP)

Determinar la probabilidad: Se entiende como la posibilidad de ocurrencia del riesgo. Para efectos de este análisis, la probabilidad de ocurrencia estará asociada a la exposición al riesgo del proceso o actividad que se esté analizando. De este modo, la probabilidad inherente será el número de veces que se pasa por el punto de riesgo en el periodo de 1 año.

EVALUACIÓN DEL RIESGO

En este punto se busca comparar los resultados obtenidos en la zona de riesgo inicial o inherente y teniendo en cuenta los controles implementados y el propósito definido para cada uno de ellos con el fin de determinar la nueva zona de riesgo residual.

IDENTIFICACIÓN DE CONTROLES EXISTENTES

En este paso se debe realizar la identificación y la evaluación de los controles existentes para cada uno de los riesgos identificados, esto con el fin de evaluar la efectividad de los controles previamente implementados durante la identificación de los riesgos, así mismo se podrá identificar si existe duplicidad en algunos controles o si por el contrario estos no han sido efectivos o están siendo mal ejecutados.

MANEJO DE LOS RIESGOS

La política de Administración del Riesgo de la Alcaldía Distrital de Barrancabermeja definió los mecanismos para el manejo de los riesgos, basado en los lineamientos definidos en la Guía de Riesgos del DAFP los cuales serán adaptados para el siguiente plan de tratamiento de riesgos de seguridad de la información.

Aceptar el Riesgo: Después de realizar un análisis y considerar los niveles de riesgo se determina asumir el mismo conociendo los efectos de su posible materialización.

Evitar el Riesgo: Después de realizar un análisis y considerar que el riesgo se encuentra en un nivel muy alto, se puede determinar la no ejecución de la acción que genera el riesgo.

Reducir el Riesgo: Después de realizar un análisis y considerar que el nivel de riesgo es alto; se determina tratarlo mediante transferencia o mitigación del mismo.

Dentro de esta etapa se definen dos acciones para el manejo de los riesgos:

Transferir: Después del análisis de riesgos se contempla la estrategia de tercerizar el proceso que conlleva el riesgo o de trasladar el riesgo a través de seguros o pólizas, pero teniendo en cuenta que la responsabilidad reputacional sigue siendo de la entidad.

Mitigar: Después de considerar los niveles de riesgo una vez realizado el análisis, se deben implementar acciones a través de un plan de tratamiento que permitan mitigar el riesgo.

PLAN DE TRARAMIENTO DE RIESGOS

Durante el plan de tratamiento de riesgos para la vigencia 2023 se deben desarrollar todas las actividades para la implementación de controles y medidas de seguridad que permitan mitigar los riesgos logrando alcanzar niveles aceptables. Estas actividades deben ser alcanzables y medibles en el tiempo, estableciendo responsables y fechas de cumplimiento.

CRONOGRAMA

PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN VIGENCIA 2023					
ID	**ACTIVIDAD**	**FECHA INICIAL (MES)**	**FECHA DE CUMPLIMIENTO (MES)**	**RESPONSABLE**	**RESULTADO O PRODUCTO**
1	Informar, educar y capacitar a las partes involucradas sobre la Política de Seguridad y Privacidad de la Información y el proceso de Gestión de Riesgos de Seguridad de la Información	Febrero	Diciembre	Oficina Asesora de Prensa, Comunicaciones y Protocolo Secretaría de las TIC, Ciencia e Innovación	Plan de Capacitación y Sensibilización en Seguridad y Privacidad de la Información.
2	Identificación, clasificación y valoración de los activos de información de los procesos involucrados	Febrero	Marzo	Responsable de cada proceso y/o jefe de dependencia	Inventario de activos de información consolidado y

					valorado frente a los principios de confidencialidad, integridad y disponibilidad.
3	Definición de la herramienta para la gestión de riesgos de seguridad de la información	Febrero	Abril	Oficina Asesora de Control Interno Secretaría de las TIC, Ciencia e Innovación	Herramienta con la matriz de riesgos de seguridad de la información
4	Identificación y valoración de los riesgos de seguridad de la información y los controles existentes	Febrero	Abril	Los líderes de los procesos en conjunto con sus equipos de trabajo	Mapa de riesgos de seguridad de la información
5	Definición de los planes de tratamiento de riesgos de seguridad de la información	Febrero	Abril	Los líderes de los procesos en conjunto con sus equipos de trabajo	Mapa de riesgos de seguridad de la información
6	Aceptación y Aprobación del Mapa de Riesgos y planes de tratamiento	Febrero	Abril	Secretaría de Planeación Municipal Oficina Asesora de Control Interno	Mapa de riesgos consolidado
7	Ejecución de los controles y actividades definidas en el plan de tratamiento de riesgos	Febrero	Diciembre	Los líderes de los procesos en conjunto con sus equipos de trabajo	Informe con evidencias de las acciones implementadas
8	Seguimiento y control a la implementación del mapa de riesgos de seguridad de la información	Febrero	Diciembre	Secretaría de Planeación Municipal Oficina Asesora de Control Interno	Informe de seguimiento con hallazgos y oportunidades de mejora
9	Medición del Desempeño	Febrero	Diciembre	Oficina Asesora de Control Interno Comité Institucional de Gestión y Desempeño	Informe de auditoría presentado a la Línea Estratégica

Tabla 10. Cronograma de actividades.

Fuente: Elaboración propia

Para el desarrollo y el cumplimiento de las actividades definidas en el plan de tratamiento de riesgos, se debe contar con el apoyo de la alta dirección garantizando la disponibilidad de recursos humanos, técnicos, financieros y administrativos que faciliten el cumplimiento de las actividades.

EVALUACIÓN DEL DESEMPEÑO

En esta etapa es necesario realizar seguimiento y monitoreo a las actividades de control definidas en las fases anteriores incluyendo las medidas establecidas en el plan de tratamiento de riesgos, así mismo se deben definir mecanismos de medición como indicadores de gestión enfocados a medir el cumplimiento de los objetivos propuestos para el proceso de gestión de riesgos de seguridad de la información en la Alcaldía Distrital de Barrancabermeja.

REPORTE DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN

La Alcaldía Distrital de Barrancabermeja deberá contar con un mecanismo para el reporte de incidentes relacionado con la información y los activos que soportan la operación de los procesos institucionales, principalmente para los incidentes que se hayan materializado, esto con el fin de identificar posibles deficiencias en la implementación de controles y garantizar que se tomen las acciones pertinentes para retroalimentar y fortalecer el proceso de gestión de riesgos de seguridad de la información en la entidad.

MEJORA CONTINUA

La Alcaldía Distrital de Barrancabermeja debe garantizar la mejora continua del proceso de gestión de riesgos de seguridad de la información, estableciendo mecanismos para mitigar el impacto cuando existan hallazgos o incidentes de seguridad encontrados en auditorias o revisiones ejecutadas por las partes competentes. Así mismo se deben identificar e investigar las causas y las consecuencias derivadas de los hallazgos encontrados, fortaleciendo las medidas de protección y rediseñando las actividades dirigidas a mitigar los riesgos.

INTEGRACIÓN DEL PROCESO DE GESTIÓN DE RIESGOS DE SEGURIDAD DIGITAL CON EL MODELO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN (MSPI)

El MSPI establece los lineamientos para la implementación de un Sistema de Gestión de Seguridad de la Información, dentro de los puntos más relevantes se destacan la gestión de riesgos y el ciclo de operación PHVA (Planear, Hacer, Verificar y Actuar) el cual permite diseñar, gestionar, implementar y mantener adecuadamente todos los mecanismos de seguridad y privacidad de la información al interior de las entidades del estado. Para la Alcaldía Distrital de Barrancabermeja es fundamental implementar una metodología adecuada y eficiente para su proceso de gestión y tratamiento de riesgos de seguridad digital y articuladamente avanzar en la consolidación del MSPI a través de su implementación en todos los procesos institucionales.

El proceso de gestión de riesgos de seguridad de la información adoptado por la Alcaldía Distrital de Barrancabermeja se articula con las fases y la metodología planteada por el ciclo de operación PHVA del Modelo de Seguridad y Privacidad de la Información (MSPI),
A continuación, se describen las fases adoptadas para la gestión y tratamiento de riesgos de seguridad de la información:

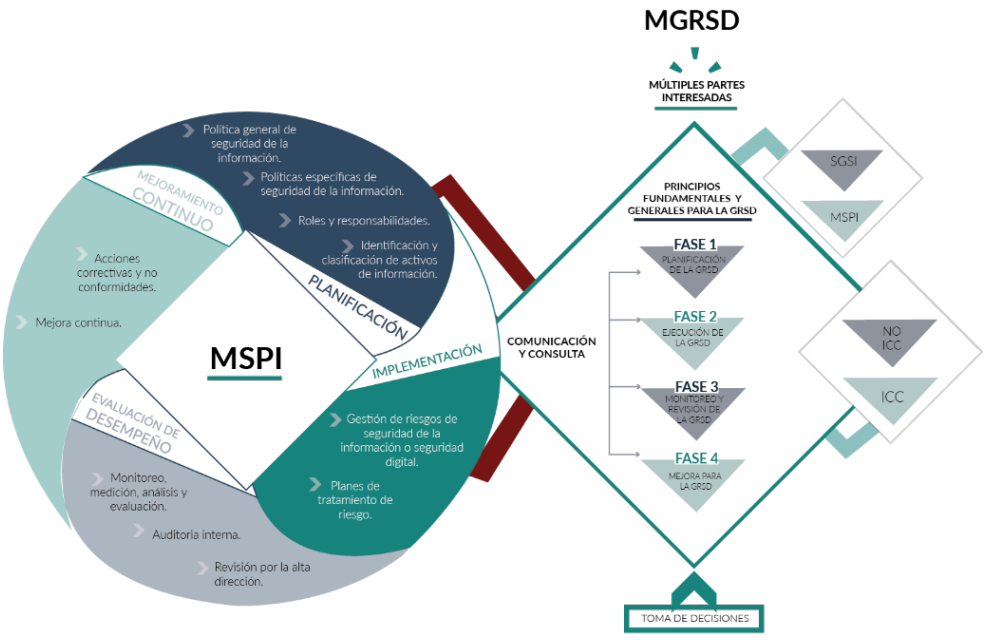

Imagen 3. Interacción entre el MSPI y el MGRSD.
Fuente: Modelo de gestión de riesgos de seguridad Digital (MINTIC)

CICLO DE OPERACIÓN CON UN ENFOQUE DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN.

PLANIFICACIÓN

- Identificación del riesgo
- Identificación de las áreas de impacto
- Identificación de los factores de riesgo
- Identificación y valoración de los activos de información
- Identificación de amenazas y vulnerabilidades
- Verificación de los controles existentes
- Valoración del riesgo
- Análisis del riesgo
- Evaluación del riesgo
- Definición del plan de tratamiento de riesgos de seguridad de la información

OPERACIÓN

- Implementación del plan de tratamiento de riesgos de seguridad de la información

EVALUACIÓN DEL DESEMPEÑO

- Revisión y monitoreo de las actividades definidas en el plan de tratamiento de riesgos.
- Medición del desempeño
- Verificación de incidentes de seguridad
- Informe a la alta gerencia

MEJORA CONTINUA

- Plan de comunicaciones
- Rediseño de actividades