	ALCALDÍA MUNICIPAL DE BARRANCABERMEJA	**VERSIÓN 1.0**

PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION

SECRETARIA DE TECNOLOGIA, INFORMACION Y COMUNICACIONES (TIC)

BARRANCABERMEJA, ENERO 2019

CONTENIDO

1. DERECHOS DE AUTOR 4

2. INTRODUCCIÓN 5

3. OBJETIVOS 6

4. ALCANCE 7

5. TERMINOS Y DEFINICIONES 8

6. ROLES Y RESPONSABILIDADES FRENTE A LA ADMINISTRACIÓN DEL RIESGO 12

7. POLÍTICA DE ADMINISTRACIÓN DEL RIESGO 13

8. ETAPAS PARA LA ADMINISTRACIÓN DEL RIESGO 14

9. VISION GENERAL DEL PROCESO DE GESTION DE RIESGO EN LA SEGURIDAD DE LA INFORMACION 15

10. ESTABLECIMIENTO DEL CONTEXTO DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN 16

10.1 Criterios de evaluación del riesgo de seguridad de la información: 17

10.2 Criterios de Impacto 17

11. VALORACIÓN DE LOS RIESGOS DE SEGURIDAD DE LA INFORMACIÓN 18

11.1 Identificación del riesgo 18

11.1.1 Primarios: 19

11.1.2 De Soporte 19

11.2 Estimación del riesgo 21

11.3 Formulario para el registro de la estimación de los riesgos de seguridad de la información: 22

11.4 Clasificación de los riesgos 25

11.5 Riesgos de Factores externos 26

11.6 Evaluación de los riesgos 28

12. TRATAMIENTO DE LOS RIESGOS DE SEGURIDAD DE LA INFORMACIÓN 28

13. MONITOREO Y SEGUIMIENTO DE LOS RIESGOS DE SEGURIDAD DE LA INFORMACIÓN 29

14. CRONOGRAMA VALORACION DE RIESGOS DE SEGURIDAD DE LA INFORMACION 30

15. DOCUMENTOS ASOCIADOS 31

16. RESPONSABLES DEL DOCUMENTO 32

1. DERECHOS DE AUTOR

Este documento hace parte del modelo integrado de planeación y gestión de la información de la Alcaldia de Barrancabermeja, por los (MIPG) Todas las referencias a los documentos del Modelo de Seguridad y Privacidad de la Información, con derechos reservados por parte de la Alcaldia Municipal de Barrancabermeja.

2. INTRODUCCIÓN

El departamento administrativo de la función pública establece que todos los entes nacionales y territoriales deben contar con un el plan de tratamiento de riesgos de seguridad y privacidad de la información. En este plan de sebe establecer un método lógico y sistemático para la administración, identificar, analizar, evaluar, tratar, monitorear y comunicar los riesgos asociados con la seguridad y privacidad de la información, que permitan minimizar la perdida de información como principal activo de la organización

Actualmente cualquier organización o empresa gestiona sus actividades a través de herramientas tecnológicas como sistema de información están expuestas a los riesgos asociados con la privacidad y seguridad de la información; por lo tanto, es necesario tomar las medidas, para identificar las causas y consecuencias de la materialización de dichos riesgos. Por esa razón, la presente guía tiene como objetivo orientar y facilitar la implementación y desarrollo de una forma eficaz, eficiente y efectiva de la gestión de los riesgos asociados con la seguridad y privacidad de la información, desde la identificación hasta el monitoreo; enfatiza en la importancia de la administración del riesgo, para facilitar su identificación, reconocimiento de las causas, efectos, definición de controles y generar los lineamientos para su adecuada gestión.

3. OBJETIVOS

Implementar el plan de tratamiento de riesgos que hace parte del Sistema de Gestión de Seguridad de la Información – SGSI; de tal forma que se definen y aplican los controles con los cuales se buscan mitigar la materialización de los riesgos de seguridad de la información. De esta forma se busca que, mediante el tratamiento de los riesgos y la mejora continua de la Seguridad y Privacidad de la Información, las partes interesadas tengan mayor confianza en el tratamiento de la información que se almacena y maneja en la Entidad.

4. ALCANCE

En este documento se detallan los riesgos asociados con el sistema de gestión de seguridad de la información - SGSI y su tratamiento será aplicado dentro de la Administración central Municipal a cualquier medio tecnológico de la entidad, a través de los principios básicos y metodológicos para la administración de los riesgos de seguridad de la información, así como las técnicas, actividades y formularios que permitan y faciliten el desarrollo de las etapas de reconocimiento del contexto, identificación de los riesgos de seguridad de la información , análisis y evaluación, opciones de tratamiento o manejo del riesgo; como las pautas y recomendaciones para su seguimiento, monitoreo y evaluación.

5. TERMINOS Y DEFINICIONES

Para la administración del riesgo, se tendrán en cuenta los siguientes términos y definiciones:

Administración de riesgos: análisis, evaluar, seguimiento y control conjunto de secuenciales que se deben desarrollar para el adecuado tratamiento de los riesgos.

Amenaza: Situación externa o interna que puede afectar su operación

Análisis del riesgo: Es la etapa donde se establece la probabilidad de ocurrencia y el impacto del riesgo antes de determinar y se determina el procedimiento.

Asumir el riesgo: Es aceptar el riesgo y mitigarlo.

Causa: medios, circunstancias y/o agentes que generan riesgos.

Calificación del riesgo: estimación de la probabilidad de ocurrencia del riesgo y el impacto que puede causar su materialización.

Compartir o transferir el riesgo: Opción de manejo que determina traspasar o compartir las pérdidas producto de la materialización de un riesgo con otras organizaciones mediante respaldo de información, servidores redundantes, servidores en la nube, outsourcing, seguros, sitios alternos etc.

Riesgo institucional: Son los que afectan de manera directa el cumplimiento de los objetivos o la misión institucional. Los riesgos institucionales, son producto del análisis de los riesgos por proceso y son denominados de este tipo cuando cumplen las siguientes características:

Consecuencia: efectos que se pueden presentar cuando un riesgo se materializa.

Contexto estratégico: Son las condiciones internas y del entorno, que pueden generar eventos que originan oportunidades o afectan negativamente el cumplimiento de la misión y objetivos de una institución.

Control: Conjunto de acciones que minimiza el impacto o la probabilidad de ocurrencia de un riesgo.

Control preventivo: Conjunto de acciones que eliminan o mitigan las causas del riesgo; está orientado a disminuir la probabilidad de ocurrencia del riesgo.

Control correctivo: Conjunto de acciones que mitigan las consecuencias del riesgo; está orientado a disminuir el nivel de impacto del riesgo.

Debilidad: Situación en la que el riesgo puede afectar negativamente a la entidad.

Evaluación del riesgo: Resultado del cruce cuantitativo de las calificaciones de probabilidad e impacto, para establecer la zona donde se ubicará el riesgo.

Evitar el riesgo: Opción de manejo que determina la formulación de acciones donde se prevenga la materialización del riesgo mediante el fortalecimiento de controles.

Frecuencia: Ocurrencia de un evento expresado como la cantidad de veces que ha ocurrido un evento en un tiempo.

Identificación del riesgo: Etapa donde se establece el riesgo con sus causas (asociadas a factores externos e internos de riesgo), consecuencias y se clasifica de acuerdo con los tipos de riesgo definidos

Impacto: Medida para estimar cuantitativa y cualitativamente el posible efecto de la materialización del riesgo.

Mapa de riesgos: Documento que, de manera sistemática, muestra el desarrollo de las etapas de la administración del riesgo.

Materialización del riesgo: Ocurrencia del riesgo identificado

Opciones de manejo: Posibilidades disponibles para administrar el riesgo posterior a la valoración de los controles definidos (asumir, reducir, evitar compartir o transferir el riesgo residual).

Plan de contingencia: Conjunto de acciones encaminadas a mitigar el riesgo para garantizar la continuidad del servicio

Probabilidad: Medida para estimar cuantitativa y cualitativamente la posibilidad de ocurrencia del riesgo.

Procedimiento: Conjunto de especificaciones, relaciones, responsabilidades, controles y ordenamiento de las actividades y tareas requeridas para cumplir con el proceso.

Proceso: conjunto de entradas tangibles o intangibles, suministradas por un proveedor, a estas entradas se les asigna recursos y se aplican controles, obteniendo salidas tangibles o intangibles, destinadas a un usuario, generando un impacto en estos. Se clasifican en estratégicos, misionales, de apoyo y de evaluación.

Riesgo: eventualidad que tendrá un impacto negativo sobre los objetivos institucionales o del proceso.

Riesgo inherente: Es aquel al que se enfrenta una entidad o proceso en ausencia de controles y/o acciones para modificar su probabilidad o impacto.

Los riesgos que se encuentran en zona alta o extrema: después de valorar el riesgo (identificación y evaluación de controles), el riesgo residual se ubica en zonas de riesgo alta o extrema, indicando que el grado de exposición a la materialización del riesgo aún se encuentra poco controlado.

Los riesgos que tengan incidencia en usuario o destinatario final externo: en el caso de la materialización del riesgo la afectación del usuario externo se presenta de manera directa.

Los riesgos de corrupción: todos los riesgos identificados que hagan referencia a situaciones de corrupción serán considerados como riesgos de tipo institucional.

Riesgo residual: Nivel de riesgo que permanece luego de determinar y aplicar controles para su administración.

Valoración del riesgo: establece la identificación y evaluación de los controles para prevenir la ocurrencia del riesgo o reducir los efectos de su materialización. En la etapa de valoración del riesgo se determina el riesgo residual, la opción de manejo a seguir, y si es necesita.

Servicio: Es el medio por el cual se entrega valor agregado a los clientes (dueño de proceso de negocio) para facilitar los resultados del negocio, que se quiere obtener.

6. ROLES Y RESPONSABILIDADES FRENTE A LA ADMINISTRACIÓN DEL RIESGO

El éxito de la administración del riesgo depende de la decidida participación de los directivos, servidores públicos y contratistas; por esto, es preciso identificar los actores que intervienen:

Alta Dirección: Aprueban las directrices para la administración del riesgo en la Entidad. La Alta Dirección es la responsable del fortalecimiento de la política de administración del riesgo.

Proceso Administración del Sistema Integrado de Gestión: Genera la metodología para la administración del riesgo de la Entidad, coordina, lidera, capacita y asesora en su aplicación.

Responsables de los procesos: Identifican, analizan, evalúan y valoran los riesgos de la entidad (por procesos e institucionales) al menos una vez al año. Si bien los Líderes SIG apoyan la ejecución de las etapas de gestión del riesgo a nivel de los procesos, esto no quiere decir que el proceso de administración de riesgos este solo bajo su responsabilidad. Al contrario, cada responsable de proceso se encarga de garantizar que en el proceso a su cargo se definan los riesgos que le competen, se establezcan las estrategias y responsabilidades para tratarlos y, sobre todo, que se llegue a cada funcionario que trabaja en dicho proceso. No se debe olvidar que son las personas que trabajan en cada

uno de los procesos los que mejor conocen los riesgos existentes en el desarrollo de sus actividades.

Servidores públicos y contratistas: ejecutar los controles y acciones definidas para la administración de los riesgos definidos, aportar en la identificación de posibles riesgos que puedan afectar la gestión de los procesos y/o de la entidad.

Quien haga las veces de Control Interno: debe realizar evaluación y seguimiento a la política, los procedimientos y los controles propios de la administración de riesgos.

Quienes deben mitigar el riesgo si es tecnológico: El Secretario TIC

Quien deben realiza hacer seguimiento y control al riesgo: control interno administrativo y Secretaria TIC.

7. POLÍTICA DE ADMINISTRACIÓN DEL RIESGO

La Secretaria TIC adelantará las acciones pertinentes para la implementación y mantenimiento del proceso de Administración del Riesgo, y para ello todos los servidores de la entidad se comprometen a:

1. Socializar las normas internas y externas relacionadas con la administración de los riesgos.
2. Fortalecer la cultura de administración de los riesgos para crear conciencia colectiva sobre los beneficios de su aplicación y los efectos nocivos de su desconocimiento.
3. Revisar los procesos y procedimientos permanentemente el análisis de riesgos con base en la aplicación de las metodologías adoptadas para el efecto.

4. Mantener un control permanente sobre los cambios en la calificación de los riesgos para realizar oportunamente los ajustes pertinentes.
5. Reportar los eventos de riesgo que se materialicen, utilizando los procedimientos e instrumentos establecidos para el efecto.
6. Desarrollar e implementar planes de contingencia para asegurar la continuidad de los procesos, en los eventos de materialización de los riesgos que afecten a los objetivos institucionales previstos y los intereses de los usuarios y partes interesadas.
7. Presentar propuestas de mejora continua que permitan optimizar la forma de realizar y gestionar las actividades de la entidad para así aumentar nuestra eficacia y efectividad.

Para lograr lo anteriormente enunciado la Alta Dirección y control interno administrativo asignará los recursos tanto humanos, presupuestales y tecnológicos necesarios que permitan realizar el seguimiento y evaluación a la implementación y efectividad de esta política.

De igual manera, la presente guía forma parte de la política de administración del riesgo, por cuanto detalla las directrices que deben tenerse en cuenta para la gestión del riesgo en la entidad y que tienen como propósito evitar la materialización del riesgo.

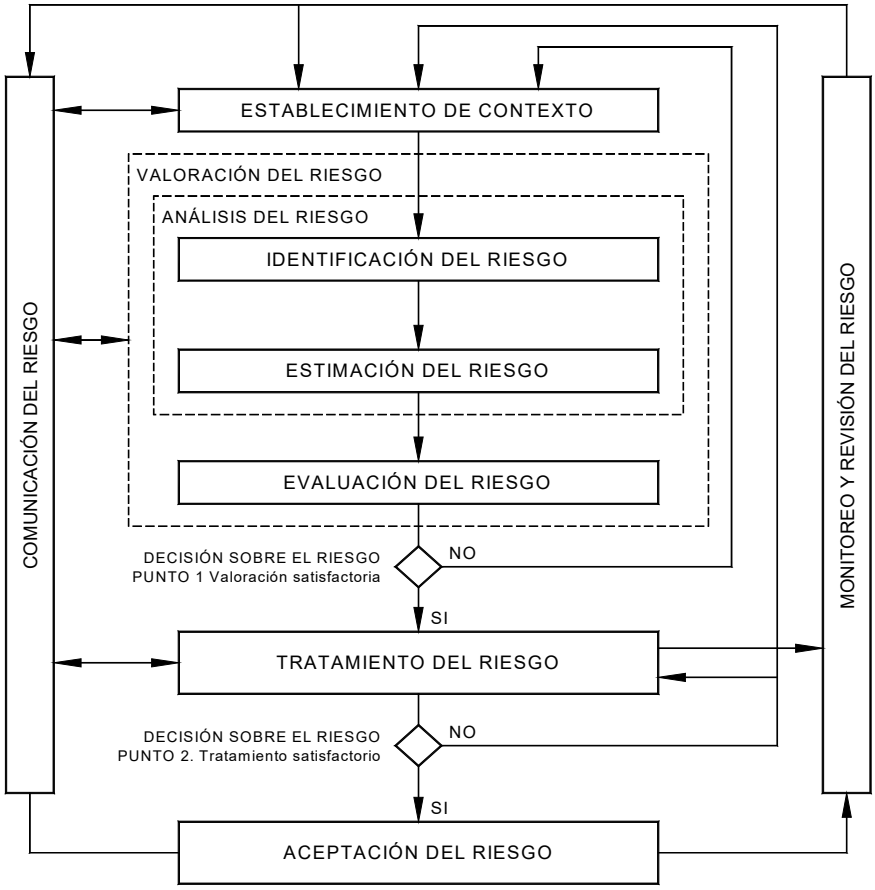
8. ETAPAS PARA LA ADMINISTRACIÓN DEL RIESGO

Se presenta cada una de las etapas a desarrollar durante la administración del riesgo; en la descripción de cada etapa se desplegaran los aspectos conceptuales y operativos que se deben tener en cuenta.

- **Contexto estratégico:** determinar los factores externos e internos del riesgo.
- **Identificación:** identificación de causas, riesgo, consecuencias y clasificación del riesgo.
- **Análisis:** Calificación y evaluación del riesgo inherente.
- **Valoración:** identificación y evaluación de controles; incluye la determinación del riesgo residual.
- **Manejo:** determinar, si es necesario, acciones para el fortalecimiento de los controles.
- **Seguimiento:** evaluación integral de los riesgos.

9. VISION GENERAL DEL PROCESO DE GESTION DE RIESGO EN LA SEGURIDAD DE LA INFORMACION

A continuación, se presenta el modelo de gestión de riesgos de seguridad de la información diseñado basado tanto en la norma ISO/IEC 31000 como en la ISO 27005 para la adecuada administración de riesgos en la seguridad de la información; los elementos que lo componen son:



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

10. ESTABLECIMIENTO DEL CONTEXTO DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN

El contexto de gestión de riesgos de seguridad de la información define los criterios básicos que serán necesarios para enfocar el ejercicio por parte de la entidad 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 administración central, 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:

10.1 Criterios de evaluación del riesgo de seguridad de la información:

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

- El valor estratégico del proceso de información en la alcaldía de Barrancabermeja.
- 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 administración central.
- Las expectativas y percepciones de las partes interesadas y las consecuencias negativas para el buen nombre y reputación de la administración central.

10.2 Criterios de Impacto

Los criterios de impacto se especificarán en términos, daño o de los costos , 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

11. VALORACIÓN DE LOS RIESGOS DE SEGURIDAD DE LA INFORMACIÓN

Los riesgos se deberán identificar, describir cuantitativamente o cualitativamente y priorizarse frente a los criterios de evaluación del riesgo y los objetivos relevantes para la Administración central Municipal, 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
    - Se mide el impacto del riesgo
    - Se realimentación del riesgo

11.1 Identificación del riesgo

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

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

11.1.1 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.

11.1.2 De Soporte

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

11.3 **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.)

11.4 **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.)

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

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

11.7 **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 administración central municipal. Existen distintos métodos para analizar amenazas, por ejemplo:

- Controles de seguridad
- 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.

11.2 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.

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

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, costos de reparación o sustitución, interrupción del servicio, disminución del rendimiento, infracciones legales, pérdida de ventaja competitiva, vulnerabilidad en los datos 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.

11.3 Formulario para el registro de la estimación de los riesgos de seguridad de la información:

MATRIZ DOFA PARA IDENTIFICACIÓN DE RIESGOS			
Responsable:			
Objetivo:			
Fecha:			
Qué servicio afecta:			
Proceso:			
Debilidades	**Fuente**	**Amenazas**	**Proceso Mitigación**

Para diligenciar la matriz anterior, y como parte introductoria se deberá informar a los asistentes: la dependencia a la cual corresponde el proceso y el objetivo (se debe presentar indicando que se hace, cual es el mediante y la finalidad). Con esta información, se identificarán las posibles debilidades como:

- La administración, la estructura organizacional, las funciones y las responsabilidades.
- Las políticas, los objetivos y las estrategias que existen para su realización.
- Las capacidades, entendidas en términos de recursos y de conocimiento (humanos, de capital, tiempo, personas, infraestructura, procesos, sistemas y tecnologías).
- Los sistemas de información y comunicación, flujos de información formales e informales y toma de decisiones.
- Las normas, directrices y modelos adoptados por la organización.

- La forma y el alcance de las relaciones contractuales.

PROBABILIDAD			
Concepto	**Valor**	**Descripción**	**Frecuencia**
Raro	1	El evento puede ocurrir sólo en circunstancias excepcionales.	No se ha presentado en los últimos 5 años
Improbable	2	Es muy poco factible que el evento se presente.	Al menos de 1 vez en Los últimos 5 años.
Posible	3	El evento podría ocurrir en algún momento.	Al menos de 1 vez en Los últimos 2 años.
Probable	4	El evento probablemente ocurrirá en la mayoría de las circunstancias,	Al menos de 1 vez en El último año.
Casi Certeza	5	Se espera que ocurra en la mayoría de las circunstancias	Más de 1 vez al año.

IMPACTO		
Concepto	**Valor**	**Descripción**
Insignificante	1	La materialización del riesgo **puede ser controlado** por los participantes del proceso, y **no afecta los objetivos del proceso**.
Menor	4	La materialización del riesgo ocasiona **pequeñas demoras** en el cumplimiento de las actividades del proceso, y **no afecta significativamente el cumplimiento de los objetivos** de la Administración Central Municipal. Tiene un impacto bajo en los procesos de otras áreas.
Moderado	6	La materialización del riesgo **demora el cumplimiento de los objetivos del proceso,** y tiene un **impacto moderado en los procesos de otras áreas** de la Administración Central Municipal. Puede además causar un deterioro en el desarrollo del proceso dificultando o retrasando el cumplimiento de sus objetivos, impidiendo que éste se desarrolle en forma normal.
Mayor	9	La materialización del riesgo **retrasa el cumplimiento de los objetivos de la Administración central Municipal** y tiene un **impacto significativo en la imagen pública** de los servicios que presta la Alcaldia. Puede además generar impactos a los entes descentralizados y las otras entidades que comparten información con la alcaldía Como la DIAN, pagos a Terceros, declaraciones de Rentas Municipal

Catastrófico	10	La materialización del riesgo **imposibilita el cumplimiento de los objetivos de la Alcaldia**, tiene un **impacto catastrófico en la imagen pública de la administración central Municipal**. Puede además generar impactos que afecten giros de la nación, perdida de información confidencial imposible, restablecer el servicio

11.4 Clasificación de los riesgos

Durante la etapa de identificación, se realiza una clasificación del riesgo, según sus características, con el fin de orientar la formulación de un tratamiento adecuado que posibilite la mitigación del riego mediante la definición de controles y planes de manejo:

Clases de riesgo	Definición
Estratégico	Son los riesgos relacionados con la misión y el cumplimiento de los objetivos estratégicos, la definición de políticas, diseño y conceptualización de la entidad por parte de la alta gerencia.
Operativo	Relacionados con el funcionamiento y operatividad de los sistemas de información de la entidad: definición de procesos, estructura de la entidad, articulación entre dependencias.
Financieros	Relacionados con el manejo de los recursos de la entidad: ejecución presupuestal, elaboración estados financieros, pagos, manejos de excedentes de tesorería y manejo de los bienes.
Cumplimiento	Capacidad de cumplir requisitos legales, contractuales, ética pública y compromiso con la comunidad.
Tecnología	Capacidad para que la tecnología disponible satisfaga las necesidades actuales y futuras y el cumplimiento de la misión.
Imagen	Tienen que ver con la credibilidad, confianza y percepción de los usuarios de la entidad.

11.5 Riesgos de Factores externos

Los factores externos pueden generar riesgos difíciles de mitigar, para ello deben ser identificadas las amenazas. Mediante lluvia de ideas se identifican los aspectos del entorno, para este caso puntual, no existe una regla específica, sin embargo tendrán el mismo tratamiento de las debilidades, es decir afinidad por agrupación, generando como resultado un listado como:

- Nueva tecnología disponible
- Nuevas leyes
- Demoras en la respuesta de comunicaciones enviadas por otras entidades
- Incremento en el número de solicitudes por alta demanda de usuarios
- Cambio de Gobierno
- Poco conocimiento por parte de la ciudadanía
- Adaptación a normatividad internacional

Con el listado de estas ideas, se debe identificar el factor externo al cual perteneces cada idea:

Idea	Factores Externos
Nueva tecnología disponible	Tecnológico
Nuevas leyes	Legal
Demoras en la respuesta de comunicaciones enviadas por otras entidades	Interinstitucional
Incremento en el número de solicitudes por alta	Social

demanda de usuarios	
Cambio de Gobierno	Político
Poco conocimiento por parte de la ciudadanía	Social
Adaptación a normatividad internacional	Legal

CONTEXTO ESTRATÉGICO			
PROCESO:			
OBJETIVO:			
FECHA:			
FACTORES INTERNOS	**CAUSAS**	**FACTORES EXTERNO**	**CAUSAS**
Tecnología y sistemas de información	• Equipos insuficientes • Equipos obsoletos	Tecnológico	• Nuevo tecnología disponible.
Modelo de operación	• Ausencia de políticas de operación • Proceso manual • Fallas en el seguimiento a los procedimientos del proceso	Legal	• Nuevas leyes • Adaptación a normatividad internacional
Talento Humano	• Desconocimiento de la normatividad aplicada • Desmotivación	Interinstitucional	Demoras en la respuesta de comunicaciones enviadas por otras entidades

CONTEXTO ESTRATÉGICO			
	• Resistencia al cambio		
Tecnología y sistemas de información	• Información desactualizada	Social	Incremento en el número de solicitudes para alta demanda de usuarios
Mecanismos de control	• Los indicadores no miden nada	Político	Cambio de gobierno

11.6 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.

12. TRATAMIENTO DE LOS RIESGOS DE SEGURIDAD DE LA INFORMACIÓN

Como resultado de la etapa de evaluación del riesgo tendremos una lista ordenada de los riesgos con la identificación, 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 relevante para la decisión.

COSTO - BENEFICIO	OPCION DE TRATAMIENTO
El nivel de riesgo está muy alejado del nivel de tolerancia, su costo y tiempo del tratamiento es muy superior a los beneficios	**Evitar** el riesgo, su propósito es no proceder con la actividad o la acción que da origen al riesgo (ejemplo, dejando de realizar una actividad, tomar otra alternativa, etc.)
El costo del tratamiento por parte de terceros (internos o externos) es más beneficioso que el tratamiento directo	**Transferir o compartir** el riesgo, entregando la gestión del riesgo a un tercero (ejemplo, contratando un seguro o subcontratando el servicio).
El costo y el tiempo del tratamiento es adecuado a los beneficios	**Reducir o Mitigar** el riesgo, seleccionando e implementando los controles o medidas adecuadas que logren que se reduzca la probabilidad o el impacto
La implementación de medidas de control adicionales no generará valor agregado para reducir niveles de ocurrencia o de impacto.	**Retener o acepta**r el riesgo, no se tomará la decisión de implementar medidas de control adicionales. Monitorizarlo para confirmar que no se incrementa

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.

13. 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 podrán 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.

14. CRONOGRAMA VALORACION DE RIESGOS DE SEGURIDAD DE LA INFORMACION

La Entidad definirá y mantendrá un cronograma de actividades para la realización de la valoración de los riesgos de seguridad de la información en los procesos de la organización, basado con su criticidad y su valor para el cumplimiento de la misión de la Administración Central.

15. DOCUMENTOS ASOCIADOS

- Políticas de seguridad de la información Municipio de Barrancabermeja
- Procedimiento de soporte Usuario final Municipio de Barrancabermeja

16. RESPONSABLES DEL DOCUMENTO

Elaboró:	Ingeniero: Marino Rodríguez Palacios
Cargo:	Profesional Universitario – Coordinador del Grupo Funcional Operaciones TI (Infraestructura Tecnológica, Sistemas de Información y Soporte Tecnológico)

Responsable:	Ingeniero: Marino Rodríguez Palacios
Cargo:	Profesional Universitario – Coordinador del Grupo Funcional Operaciones TI (Infraestructura Tecnológica, Sistemas de Información y Soporte Tecnológico)

Aprobó:	Ingeniero. Alberto Eloy Carrillo Vargas
Cargo:	Secretario TIC