2025

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

ALCALDÍA DE BUCARAMANGA

Caja de Previsión Social Municipal

CPSM

Versión 0

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

CAJA DE PREVISIÓN SOCIAL MUNICIPAL DE BUCARAMANGA

Dirección General	Gestión de Tecnologías de Información
Alejandra Serrano R.	Jhonatan Tique Marín
	Gestión de Calidad
	Liliana M. Delgado Castellanos

TABLA DE CONTENIDO

1. OBJETIVO

Este plan proporciona una guía estratégica para identificar, controlar y minimizar los riesgos asociados a la seguridad de la información, garantizando la protección de la privacidad de la información y los datos relacionados con los procesos institucionales y las personas vinculadas a la entidad.

1.1 OBJETIVOS ESPECÍFICOS

Lograr un diagnóstico real de la situación actual de la CPSM en materia de riesgos de seguridad y privacidad de la información.

Aplicar las metodologías, mejores prácticas y recomendaciones dadas por la función pública y el MinTIC para el Tratamiento de Riesgos de Seguridad y Privacidad de la Información.

Optimización de los recursos de la CPSM en la aplicación del Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información.

2. ALCANCE

El plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información se extiende a todos los procesos de la institución que gestionen, procesen, almacenen o interactúen con información institucional, abarcando tanto sistemas tecnológicos como prácticas operativas, para garantizar la protección integral de los datos y recursos asociados.

3. GLOSARIO

Activo: Cualquier recurso que tenga valor para la organización y esté relacionado con el tratamiento de información, incluyendo datos, sistemas, hardware, software, edificios, personal, entre otros. (ISO/IEC 27000).

Amenaza: Causa potencial de un incidente no deseado que puede generar daño a los activos, procesos o la organización. Ejemplo: ataques cibernéticos, desastres naturales o errores humanos. (ISO/IEC 27000).

Análisis de Riesgo: Proceso estructurado para identificar, evaluar y entender los riesgos relacionados con la seguridad de la información, determinando su nivel y potencial impacto.

Auditoría: Proceso sistemático, independiente y documentado que verifica el cumplimiento de criterios establecidos y detecta desviaciones en la implementación de controles. (ISO/IEC 27000).

Ciberseguridad: Conjunto de medidas, tecnologías y políticas diseñadas para proteger sistemas, redes y datos frente a amenazas o incidentes cibernéticos, minimizando riesgos.

Ciberespacio: Entorno virtual donde interactúan sistemas interconectados a través de redes electrónicas, incluyendo internet y otras tecnologías de comunicación.

Control: Medida administrativa, técnica, física o legal implementada para gestionar riesgos y garantizar la seguridad de la información. También conocido como salvaguarda o contramedida.

Confidencialidad: Propiedad que garantiza que la información sea accesible solo para personas autorizadas.

Declaración de Aplicabilidad: Documento oficial que especifica los controles implementados en el SGSI de acuerdo con los riesgos identificados, justificando su aplicación o exclusión. (ISO/IEC 27000).

Gestión de Incidentes de Seguridad de la Información: Conjunto de procesos para identificar, reportar, mitigar, analizar y aprender de incidentes relacionados con la seguridad de la información. (ISO/IEC 27000).

Integridad: Propiedad que asegura que la información se mantenga completa, precisa y sin modificaciones no autorizadas.

Plan de Continuidad del Negocio (BCP): Estrategia para garantizar la operación de funciones esenciales durante y después de eventos que interrumpan las actividades normales.

Plan de Tratamiento de Riesgos: Documento que detalla las acciones necesarias para gestionar riesgos de seguridad inaceptables e implementar controles adecuados para mitigarlos.

Riesgo: Posibilidad de que una amenaza aproveche una vulnerabilidad, causando daño a un activo de información. Es una combinación de la probabilidad de ocurrencia y la gravedad de las consecuencias. (ISO/IEC 27000).

Seguridad de la Información: Protección de la información para garantizar su confidencialidad, integridad y disponibilidad. (ISO/IEC 27000).

Sistema de Gestión de Seguridad de la Información (SGSI): Marco organizacional que define políticas, procedimientos y recursos para gestionar y mejorar la seguridad de la información de manera continua. (ISO/IEC 27000).

Trazabilidad: Capacidad de rastrear todas las acciones realizadas sobre un sistema o información, identificando de manera inequívoca a los responsables. (ISO/IEC 27000).

Vulnerabilidad: Punto débil o falla en un activo o control que puede ser explotado por una amenaza. (ISO/IEC 27000).

Parte Interesada: Individuo u organización que puede influir, ser influido o percibirse como afectado por las actividades o decisiones relacionadas con la seguridad de la información.

Disponibilidad: Garantía de que los sistemas, servicios y datos estén accesibles y funcionales cuando se requieran por los usuarios autorizados.

Impacto: Consecuencias que un incidente puede generar sobre los activos, los procesos o la organización, considerando aspectos operativos, financieros y reputacionales.

Resiliencia: Capacidad de una organización para resistir y recuperarse de eventos que afecten la seguridad de la información o la continuidad del negocio.

Matriz de Riesgos: Herramienta que organiza y evalúa riesgos en función de su probabilidad e impacto, permitiendo priorizar las acciones de mitigación.

Mitigación: Acciones destinadas a reducir la probabilidad o el impacto de un riesgo identificado.

Política de Seguridad de la Información: Declaración formal que define las directrices, responsabilidades y prácticas relacionadas con la protección de la información.

4. RESPONSABLE

La estructura organizacional definida para la ejecución del Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información está diseñada para garantizar

una gestión eficiente, efectiva y alineada con los objetivos estratégicos de la organización. A continuación, se detallan los roles y funciones principales:

RESPONSABILIDADES FRENTE A LOS RIESGOS	
LINEA DE DEFENSA: ESTRATEGICA	
El Director / Alta Dirección	○ Identificar aquellos riesgos que impidan el logro de la misión, objetivos y metas institucionales. ○ El equipo diectivo determinara el apetito, tolerancia y capacidad de los riesgos. ○ Definir los lineamientos para la administración del riesgo, el control y la supervision de su cumplimiento.
Comité Institucional de Gestión y Desemepño	○ Analizar la gestion del riesgo y aplicar mejoras ○ Asegurar la impl ementación y desarrollo de la politica de gestión de riesgo y las directrices en materia de seguridad digital y de la información. ○ Aprobar el mapa de riesgos de corrupción que hace parte del PAAC y sus actualizaciones. ○ Aprobar Mapa de Riesgo Fiscal que hace parte de la Política de Administración de Riesgo. ○ Aprobar mapas de riesgos de gestion ○ Aprobar mapa de seguridad de la información
Comité Institucional de Coordinacion de Control Interno	○ Recomendar mejoras y hacer seguimiento a la Politica de Administración del riesgo. ○ Retroalimentar a la alta dirección sobre la efectividad de los controles para la gestión del riesgo ○ Analizar eventos y riesgos criticos ○ Realizar seguimiento a los riesgos consolidados en el Mapa de Riesgos de Gestión, Mapa Riesgos Fiscales (dos veces al año), Mapa de Riesgos de Corrupción (tres veces al año según la norma) y Mapa de Riesgos

	de Seguridad de la Información (dos veces al año), de conformidad con el Plan Anual de Auditoría
LINEA DE DEFENSA: PRIMERA LINEA	
Lideres de Procesos/ Equipo de trabajo	○ Identificar y valorar los riesgos que puedan afectar los procesos a su cargo y actualizar cuando se requiera. ○ Hacer monitoreo a los controles para mitigar los riesgos identificados, alinearlos con las metas y objetivos de la entidad y proponer mejoras a la gestión del riesgo. ○ Desarrollar ejercicios de autoevaluación para establecer la eficiencia, eficacia y efectividad de los controles. ○ Informar a la Subdirección administrativa (segunda línea) sobre los riesgos materializados en los programas, proyectos, planes y/o procesos a su cargo
LINEA DE DEFENSA: SEGUNDA LINEA	
Subdirección Administrativa	○ Monitorear la gestión del riesgo y control ejecutado por la primera linea de defensa. ○ Consolidar los mapas de riesgo (fiscales, corrupción, y presentarlo ante el comité institucional de gestión y desempeño.(informe), una vez aprobado publicar en pag web como componente del PAAC a mas tardar el 31 Enero. ○ Solicitar publicación de los mapas de riesgos en la pagina web. ○ Aprobar a traves del proceso de calidad(Sistema integrado de Gestión), las acciones de mejora a que haya lugar propuestas por los lideres de proceso. ○ Diseñar mecanismos para que los servidores publicos y contratistas, formulen sus apreciaciones y/o

	propuestas para el diseño del mapa de riesgos de corrupción del PAAC.
Sistemas	○ Publicar mapas de riesgos en pagina web institucional ○ Asesorar a los lideres de proceso en la identificación de los riesgos de seguridad de la información e implementación de los controles definidos. ○ Presentar el mapa de riesgo de seguridad de la información y presentarlo ante el Comité de Gestión y Desempeño Institucional (informe)
LINEA DE DEFENSA: TERCERA LINEA	
Oficina de Control interno	○ Asesorar y acompañar de forma coordinada con la primera linea de defensa en la identificación de los riesgos institucionales. ○ Realizar los seguimientos a los mapas de riesgos de conformidad con el plan anual de auditorias y reportar al comité de Coordinacion y control interno. ○ Alertar a la linea estrategica sobre la probabilidad de riesgos de corrupción en las areas auditadas (seguimientos) ○ Realizar seguimientos al PAAC, verificar la publicación de los mapas de riesgos en pagina web dentro de los primeros 10 dias habiles del mes de Mayo (corte 30 abril); septiembre (corte agosto); enero (corte a diciembre) ○ Analizar el diseño e idoneidad de los controles establecidos en los procesos.

5. MARCO NORMATIVO

Decreto Nacional 767 de 2022, "Por el cual se establecen los lineamientos generales de la Política de Gobierno Digital y se subroga el Capítulo 1 del Título 9 de la Parte 2 del Libro 2 del Decreto 1078 de 2015, Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones".

Resolución 746 de 2022 expedida por el Ministerio de TIC, ""Por la cual se fortalece el Modelo de Seguridad y Privacidad de la Información y se definen lineamientos adicionales a los establecidos en la Resolución No. 500 de 2021".

Guía DAFP Guía para la Administración del Riesgo, "Guía para la Administración del Riesgo y el diseño de controles en entidades públicas (Versión 6)".

Decreto Nacional 612 de 2018, "Por el cual se fijan directrices para la integración de los planes institucionales y estratégicos al Plan de Acción por parte de las entidades del Estado", donde se encuentra el presente Plan Estratégico de Seguridad de la Información (PESI) como uno de los requisitos a desarrollar para cumplir con esta normativa.

Resolución 500 de 2021 expedida por el Ministerio de TIC, "Por la cual se establecen los lineamientos y estándares para la estrategia de seguridad y privacidad de la información y se adopta el modelo de seguridad y privacidad como habilitador de la política de Gobierno Digital".

CONPES 3995 de 2020, "Política Nacional de Confianza y Seguridad digital". - Manual de Gobierno Digital – MINTIC. - Modelo de Seguridad y Privacidad de la Información – MINTIC.

Ley Estatutaria 1581 de 2012. Ley de Protección de Datos Personales

6. DESCRIPCIÓN Y/O DESARROLLO

La Caja de Previsión Social Municipal de Bucaramanga (CPSM), comprometida con la mejora continua, ha implementado un método lógico y sistemático diseñado para identificar, analizar, evaluar, tratar, monitorear y comunicar los riesgos relacionados con el manejo de la información institucional. Este enfoque tiene como objetivo mitigar cualquier impacto significativo que dichos riesgos puedan generar en la organización.

En sus operaciones diarias, la CPSM utiliza Tecnologías de la Información y las Comunicaciones (TIC) para la captura, procesamiento y reporte de información, tanto a nivel interno como en su interacción con diferentes entidades descentralizadas.

Este contexto tecnológico expone a la institución a posibles ataques malintencionados, errores humanos o manipulaciones indebidas de la información, lo cual puede derivar en problemas económicos, legales y administrativos.

Por lo anterior, este documento establece una línea de acción clara que permite a la CPSM gestionar eficazmente los riesgos inherentes a su entorno, asegurando la confidencialidad, integridad y disponibilidad de la información, y garantizando que esta esté protegida frente a cualquier amenaza.

6.1 CATEGORÍAS DE RIESGOS

1.Operativos: Provenientes del funcionamiento y operatividad de los procesos, sistemas de información, estructura de la entidad y articulación entre dependencias.
2. Recurso Humano: Se asocia a la cualificación, competencia y disponibilidad de personal requerido para realizar un proyecto o función.
3.Financieros: Relacionados con el manejo de recursos que incluyen la ejecución presupuestal, la elaboración de los estados financieros, los pagos, manejos de excedentes de tesorería y el manejo de los bienes.
4.Cumplimiento y conformidad: Se asocian con la capacidad de la entidad para cumplir con los requisitos legales, contractuales, de ética pública y en general con su compromiso ante la comunidad.
5.Tecnológicos: Relacionados con la capacidad tecnológica para satisfacer sus necesidades actuales y futuras y el cumplimiento de la misión.
6.De Seguridad de la Información: Se asocia a la disponibilidad, confiabilidad e integridad de la información institucional.
7.De comunicación: Relacionadas con los canales, medios y oportunidades para informar durante las diferentes etapas de un proyecto.
8.Contractual: Relacionados con los atrasos o incumplimiento de las etapas contractuales en cada vigencia.

6.2 IDENTIFICACIÓN DEL RIESGO

Se han identificado tres riesgos principales asociados a la seguridad de la información, cuya ocurrencia podría comprometer la protección y gestión de los datos institucionales:

Pérdida de la confidencialidad: Acceso no autorizado a la información que compromete su naturaleza privada.

Pérdida de la integridad: Alteración no autorizada de los datos que afecta su exactitud, consistencia o validez.

Pérdida de la disponibilidad: Incapacidad de acceder a la información cuando sea requerida, lo que puede interrumpir las operaciones institucionales.

Para cada uno de estos riesgos, es necesario asociar los activos específicos o grupos de activos relevantes de los procesos, y analizar conjuntamente las posibles amenazas y vulnerabilidades que podrían propiciar su materialización.

6.3 DESCRIPCIÓN DE CAUSAS

Se detallan las posibles causas vinculadas al riesgo identificado, las cuales pueden clasificarse en dos categorías:

Causas intrínsecas: Estas están relacionadas directamente con los elementos internos del proceso, como personas, métodos, materiales, equipos o instalaciones involucradas en su ejecución.

Causas externas: Aquellas que surgen del entorno en el cual se lleva a cabo el proceso, incluyendo factores ambientales, sociales, económicos o regulatorios ajenos a la institución pero que impactan su desarrollo.

Este enfoque permite una comprensión integral de las causas del riesgo, facilitando su análisis y la implementación de medidas efectivas para su control.

6.4 CONSECUENCIAS

Se identifican los posibles efectos derivados de la materialización del riesgo, los cuales pueden impactar tanto los objetivos del proceso como a la entidad en su conjunto. Estos efectos se pueden clasificar en:

- Daños a afiliados o colaboradores.

- Pérdidas económicas que afecten la sostenibilidad financiera.
- Deterioro de la reputación e imagen institucional.
- Sanciones legales o regulatorias.
- Incremento de reprocesos operativos.
- Retrasos significativos en las actividades o proyectos.
- Generación de insatisfacción entre usuarios o partes interesadas.

Esta clasificación facilita la evaluación del impacto del riesgo y la priorización de acciones para su mitigación.

6.5 BARRERAS DE SEGURIDAD EXISTENTES

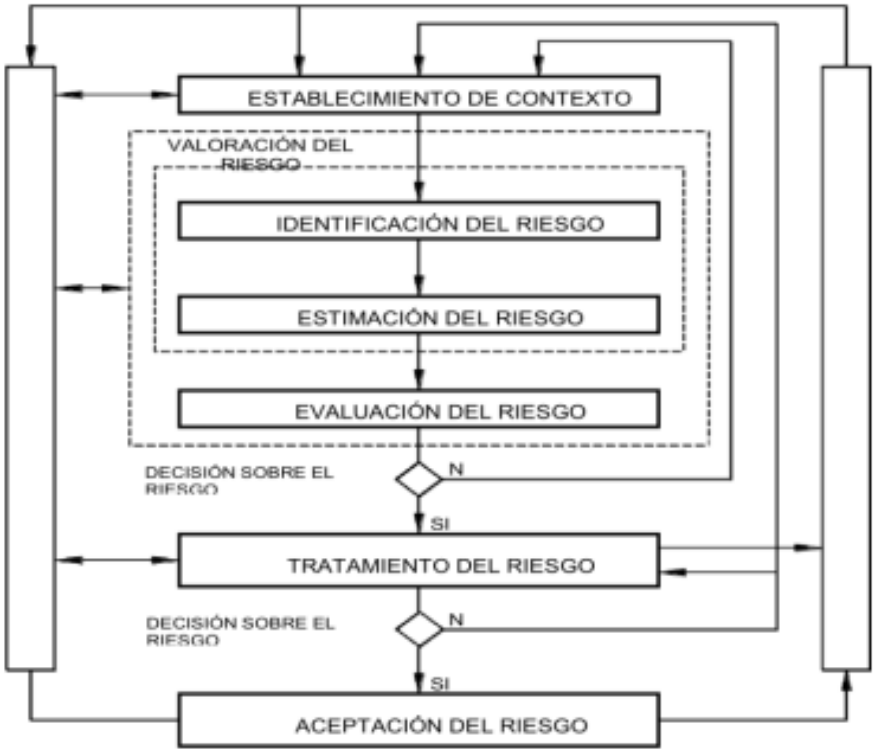
Se describen los controles existentes y las medidas implementadas para prevenir la materialización del riesgo. Estos controles pueden encontrarse en protocolos o procedimientos documentados, guías de respuesta inmediata, o en la aplicación de buenas prácticas en seguridad, tales como las enfocadas en la protección del afiliado.

Además, es relevante destacar que este apartado también incluye acciones y prácticas recomendadas en este documento, las cuales complementan y fortalecen los controles, actividades, y planes de mitigación previamente establecidos y documentados.

6.6 VISIÓN PROCESO DE GESTIÓN DE RIESGO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

A continuación, se presenta el modelo de gestión de riesgos de seguridad y privacidad de la información, diseñado con base en las normas ISO/IEC 31000 e ISO/IEC 27005. Este modelo se estructura en una serie de elementos clave que garantizan un enfoque integral y efectivo en la gestión de riesgos.

El proceso de gestión de riesgos de seguridad de la privacidad de la información debe ser iterativo, asegurando que las actividades de valoración y tratamiento de riesgos se realicen de manera continua y cíclica, adaptándose a los cambios y necesidades del entorno. Los elementos que lo componen son:



6.6.1 ESTABLECIMIENTO DEL CONTEXTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

El contexto para la gestión de riesgos de seguridad y privacidad de la información establece los criterios fundamentales necesarios para guiar el ejercicio por parte de la CPSM y alcanzar los resultados esperados. Este contexto se basa en la identificación de las fuentes que pueden originar riesgos y oportunidades dentro de los procesos de la CPSM, en el análisis de debilidades y amenazas asociadas, así como en la valoración de los riesgos considerando tanto sus posibles consecuencias para la Entidad como la probabilidad de que ocurran.

Además, se enfoca en la formulación de acciones de mitigación orientadas a alcanzar y mantener niveles de riesgo aceptables para la institución.

Como principios fundamentales para la gestión de riesgos de seguridad de la información, se definen los siguientes criterios:

6.6.1.1 CRITERIOS DE EVALUACIÓN DEL RIESGO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

La evaluación de los riesgos de seguridad de la información se centrará en los siguientes aspectos clave:

Valor estratégico del proceso de información: Reconociendo su importancia para los objetivos misionales y estratégicos de la CPSM.

Criticidad de los activos de información involucrados: Identificando su relevancia y el impacto potencial ante cualquier vulneración.

Cumplimiento normativo: Considerando los requisitos legales, reglamentarios y las obligaciones contractuales relacionadas con la seguridad de la información.

Preservación de la confidencialidad, integridad y disponibilidad: Priorizando estos pilares fundamentales para asegurar la continuidad y eficacia de las operaciones de la CPSM.

Expectativas y percepciones de las partes interesadas: Evaluando las posibles consecuencias negativas sobre la confianza, reputación y buen nombre de la CPSM en caso de incidentes de seguridad.

6.6.1.2 CRITERIOS DE IMPACTO

Los criterios de impacto se definirán considerando el alcance, los daños o los costos que un evento de seguridad de la información pueda generar para la CPSM. Estos criterios abarcarán los siguientes aspectos clave:

Clasificación de los activos de información afectados: Evaluando el nivel de sensibilidad y criticidad de los activos comprometidos.

Brechas en la seguridad de la información: Analizando la pérdida de confidencialidad, integridad o disponibilidad de la información.

Impacto financiero: Cuantificando las pérdidas económicas y la afectación al valor estratégico de la CPSM.

Alteraciones en los planes o plazos establecidos: Identificando retrasos o cambios en los cronogramas que comprometan los objetivos institucionales.

Daños a la reputación: Considerando la afectación a la imagen y confianza en la CPSM por parte de las partes interesadas.

Incumplimientos legales, reglamentarios o contractuales: Evaluando las sanciones o consecuencias derivadas de la falta de conformidad.

Deterioro de operaciones: Midiendo la afectación en las actividades internas y en las relaciones con terceros.

6.1.1.3 CRITERIOS DE ACEPTACIÓN

Los criterios de aceptación estarán directamente relacionados con las políticas, metas y objetivos establecidos por la CPSM, así como con las expectativas y requerimientos de las partes interesadas. Estos criterios definirán los niveles de riesgo que la entidad está dispuesta a asumir y serán fundamentales para guiar la toma de decisiones y priorización de acciones en la gestión de riesgos.

6.7 VALORACIÓN DE LOS RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

Antes de proceder con la valoración de los riesgos de seguridad de la información, es esencial contar con un inventario detallado de los activos de información asociados a los procesos. Este inventario servirá como base para enfocar la evaluación de los riesgos y garantizar que todos los elementos relevantes sean considerados.

Es necesario identificar y describir los activos de manera cualitativa o cuantitativa, priorizándolos de acuerdo con los criterios de evaluación del riesgo y los objetivos estratégicos de la CPSM. Este enfoque permitirá alinear la gestión de riesgos con las metas institucionales.

El proceso de valoración de riesgos de seguridad de la información se estructura en las siguientes etapas clave:

Análisis del riesgo

Identificación de los riesgos: Determinar posibles eventos o situaciones que puedan afectar la seguridad de los activos de información.

Estimación del riesgo: Evaluar la probabilidad de ocurrencia y el impacto de los riesgos identificados.

Evaluación del riesgo
Comparar los resultados del análisis con los criterios establecidos para determinar cuáles riesgos requieren tratamiento y priorizar las acciones necesarias.

6.7.1 IDENTIFICACIÓN DEL RIESGO

Para la evaluación de riesgos de seguridad y privacidad de la información, el primer paso es identificar los activos de información asociados a cada proceso evaluado. Los activos de información se dividen en dos categorías principales:

ACTIVOS PRIMARIOS

1. **Procesos o subprocesos y actividades del negocio:**
   - Aquellos cuya pérdida o degradación imposibilitaría cumplir la misión de la organización.
   - Procesos que contienen información confidencial o tecnología propietaria crítica.
   - Procesos que, si se alteran, afectan significativamente el cumplimiento de los objetivos estratégicos.
   - Procesos necesarios para satisfacer requisitos legales, reglamentarios o contractuales.

2. **Información:**
   - Información esencial para la misión o el negocio de la organización.
   - Datos personales definidos según las normativas de privacidad.
   - Información estratégica necesaria para alcanzar los objetivos organizacionales.
   - Datos costosos de recolectar, almacenar, procesar o transmitir, cuya pérdida tendría alto impacto económico.

3. **Actividades y procesos de negocio:**
   - Procesos relacionados con la propiedad intelectual cuya degradación impediría la ejecución de tareas clave.
   - Procesos indispensables para cumplir con obligaciones legales o contractuales.

ACTIVOS DE SOPORTE

1. **Hardware:**
   - Componentes físicos que sustentan los procesos, como computadoras, servidores, impresoras, discos duros y documentos en papel.

2. **Software:**
   - Programas esenciales para el procesamiento de datos, incluidos sistemas operativos, aplicaciones estándar y herramientas de administración.

3. **Redes:**
   - Infraestructura de telecomunicaciones que conecta sistemas y dispositivos, como conmutadores, cableado y puntos de acceso.

4. **Personal:**
   - Grupos humanos involucrados en el sistema de información, como usuarios, desarrolladores y responsables de su operación.

5. **Sitio:**
   - Ubicaciones físicas donde se implementan medidas de seguridad, como edificios, salas de servidores y áreas críticas.

6. **Estructura organizativa:**
   - Responsables, áreas específicas y contratistas relacionados con la operación y seguridad de la información.

6.7.2 IDENTIFICACIÓN DE AMENAZAS Y VULNERABILIDADES

Una vez identificados los activos, se debe reconocer las posibles amenazas que podrían causar daños a la información, procesos y elementos de soporte. Este análisis incluye:

- **Identificación de amenazas:** Realizada mediante entrevistas con propietarios de activos, usuarios y expertos.

- **Evaluación de vulnerabilidades:** Se identifican debilidades que podrían ser explotadas por las amenazas.

MÉTODOS PARA IDENTIFICAR AMENAZAS:

- Entrevistas con líderes de procesos y usuarios.
- Inspección física de instalaciones y equipos.
- Uso de herramientas automatizadas para escaneo de vulnerabilidades.

Análisis de consecuencias

Por cada amenaza identificada, se evaluarán las vulnerabilidades asociadas y las consecuencias potenciales. Estas consecuencias reflejan cómo podrían impactar la confidencialidad, integridad y disponibilidad de los activos de información.

Este enfoque asegura una evaluación integral y efectiva, alineada con las mejores prácticas para proteger los activos de información y mitigar los riesgos de seguridad y privacidad de la información.

Estimación del riesgo

La estimación del riesgo tiene como objetivo determinar la probabilidad de ocurrencia de los riesgos identificados y el impacto de sus consecuencias. Este proceso permite calificarlos, evaluarlos y priorizarlos para establecer su nivel de criticidad y definir estrategias efectivas de tratamiento. La finalidad principal de esta etapa es proporcionar una valoración estructurada que facilite la priorización y tratamiento de los riesgos de manera eficiente.

Aspectos clave para la estimación del riesgo:

Probabilidad:

Representa la posibilidad de que un riesgo ocurra, considerando la frecuencia con la que este se ha presentado en el pasado o podría presentarse en el futuro.

Se evalúa la probabilidad de que una amenaza aproveche una vulnerabilidad específica del activo de información.

Esta evaluación puede ser cuantitativa o cualitativa, basándose en datos históricos, experiencias previas y análisis de expertos.

La siguiente tabla o escala establecerá los niveles de probabilidad, facilitando la clasificación de los riesgos según su posible ocurrencia.

	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%	

Al estimar los riesgos, es crucial considerar no solo la frecuencia histórica, sino también las tendencias actuales y futuras que puedan influir en la probabilidad y el impacto de los riesgos, asegurando así un enfoque integral y preventivo en su gestión.

Impacto: Se refiere a las consecuencias derivadas de la materialización de un riesgo, evaluando la magnitud y gravedad de sus efectos sobre la CPSMB. Este concepto abarca los posibles daños económicos, operativos, legales, reputacionales y sociales que puedan comprometer los objetivos y el funcionamiento de la organización.

	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	

Se recomienda realizar este análisis en colaboración con todas las personas o con aquellos que posean un conocimiento profundo del proceso, quienes, gracias a su experiencia y expertise, puedan evaluar tanto el impacto como la probabilidad de ocurrencia del riesgo, siguiendo los rangos establecidos en las tablas que se presentan posteriormente.

6.7.3 DETERMINACIÓN DEL RIESGO INHERENTE Y RESIDUAL

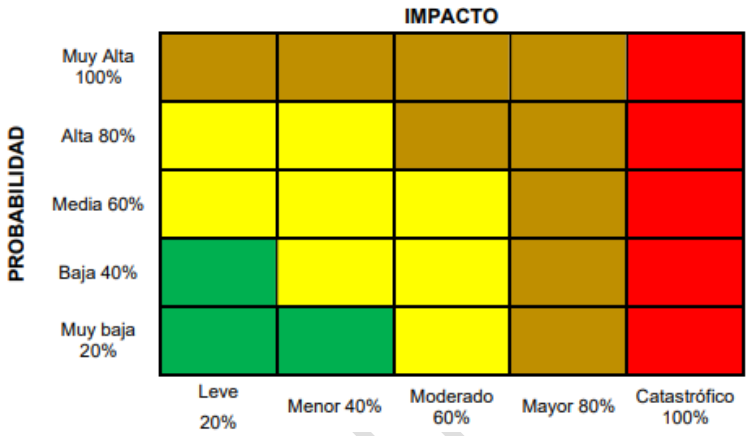
El análisis del riesgo, determinado por su probabilidad e impacto, permite realizar una primera evaluación del riesgo inherente (escenario sin controles) y comprender el grado de exposición al riesgo al que está sujeta la entidad. La exposición al riesgo se calcula como la ponderación entre probabilidad e impacto, y se representa gráficamente en una matriz de riesgos, una herramienta que identifica las zonas de riesgo y facilita su análisis visual.

Esta matriz permite clasificar los riesgos según su nivel de severidad (bajo, moderado, alto o extremo), proporcionando un enfoque estructurado para priorizar aquellos que requieren atención inmediata y definir estrategias adecuadas de tratamiento y planes de acción.

Según el plan de tratamiento de riesgos de seguridad digital, la exposición al riesgo se calcula mediante la fórmula:

Riesgo = Probabilidad × Impacto

A continuación, se presenta la matriz de riesgos, que ilustra gráficamente las diferentes zonas de riesgo, facilitando el análisis y la toma de decisiones informadas respecto a las medidas necesarias para mitigar o gestionar los riesgos identificados.



Esta herramienta proporciona una visión integral de los riesgos, permitiendo identificar y priorizar aquellos que requieren atención según la zona en la que se ubiquen (BAJO, MODERADO, ALTO o EXTREMO). Este enfoque facilita la organización efectiva de prioridades, apoyando la toma de decisiones sobre el tratamiento de los riesgos y la implementación de planes de acción estratégicos para su gestión.

6.7.4 EVALUACIÓN DE LOS RIESGOS

Después de evaluar los impactos, la probabilidad y las posibles consecuencias de los escenarios de incidentes que afectan los activos de información, se determinarán los niveles de riesgo. Estos niveles deberán contrastarse con los criterios establecidos en el contexto, con el objetivo de facilitar una toma de decisiones informada y fundamentada en la gestión de riesgos de seguridad de la información, buscando minimizar su impacto y proteger los intereses estratégicos de la Alta Entidad.

7. MAPA DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN

Como componente esencial de este plan, se incluyen los riesgos identificados en el mapa de riesgos de seguridad de la información. Este documento define las acciones

y actividades requeridas para asegurar su adecuada implementación. A continuación, se presentan de manera general los riesgos definidos para el año 2024, complementados por el Mapa Integrado de Riesgos de Gestión, Corrupción y Seguridad de la Información, que se adjunta como anexo, el cual contiene el detalle de cada una de las acciones.

Consultar Mapa Integrado de Riesgos de Gestión, corrupción y seguridad de la información CPSM

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

De manera periódica, se realizará una revisión del valor de los activos, los impactos, las amenazas, las vulnerabilidades y las probabilidades, con el objetivo de identificar posibles cambios que requieran una reevaluación iterativa de los riesgos de seguridad de la información.

Dado que los riesgos son dinámicos y están en constante evolución, al igual que la propia Entidad, estos pueden transformarse de manera significativa e inesperada.

Por ello, es fundamental contar con una supervisión continua que permita identificar:

- Nuevos activos o modificaciones en el valor de los existentes.
- Aparición de nuevas amenazas.
- Cambios o detección de nuevas vulnerabilidades.
- Incrementos en las consecuencias o impactos asociados.
- Incidentes relacionados con la seguridad de la información.

Con el fin de garantizar el cumplimiento de los objetivos establecidos en la gestión de los riesgos de seguridad de la información, será necesario definir esquemas de seguimiento y medición que permitan evaluar el sistema de gestión de riesgos. Esto facilitará una toma de decisiones oportuna y contextualizada.

CONTROL DE CAMBIOS DEL DOCUMENTO					
VERSIÓN	**FECHA**	**DESCRIPCIÓN DE AJUSTES**	**ELABORÓ**	**REVISÓ**	**APROBÓ**
0	30/01/2025	Emisión Inicial	Jhonatan Tique Marín Profesional Universitario Sistemas	Liliana M. Delgado C. Profesional de Calidad	APROBADO EN COMITÉ MIPG ACTA N° 005 de 2025 del 30/01/2025