Alcaldía de Medellín
ISVIMED
Instituto Social de Vivienda y Hábitat de Medellín

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

VIGENCIA AÑO: 2023

Enero de 2023

PL-GT-04

ELABORADO POR	REVISADO POR	APROBADO POR
Carlos Gómez Valencia Profesional Especializado **Madeleyn Palacios Zapata** Contratista	**Lucas Fernando Areiza Rúa** Subdirección Administrativa y Financiera **Carolina Martínez Cano** Líder del MIPG y Sistemas de Gestión	**René Hoyos Hoyos** Director

TABLA DE CONTENIDO

1. Introducción

La gestión de riesgos de Seguridad y Privacidad de la Información, Seguridad Digital y Continuidad de la Operación Tecnológica, le permite al ISVIMED realizar la identificación, análisis y tratamiento a los riesgos que pueden comprometer el cumplimiento de los objetivos trazados en torno a la Plataforma Estratégica de la entidad en cumplimiento de su misión, contribuyendo en la toma de decisiones con el fin de prevenir la materialización de estos.

La gestión de riesgos de seguridad y privacidad de la información son los procesos por medio de los cuales se busca eliminar las pérdidas de información, facilitando el conocer las fortalezas y debilidades a los que está expuesto el servicio durante todo su ciclo de vida.

Por esto es muy importante para las organizaciones contar con un Plan de tratamiento de riesgos de seguridad y privacidad de la información, para generar confianza ante todos los actores (grupos de interés y grupos de valor). Por esta razón el Instituto de Vivienda y Hábitat de Medellín, basado en un mapa de riesgos desarrolla este plan, buscando dar respuesta a las necesidades actuales y proteger la confianza depositada en ella con los datos almacenados por sus diferentes procesos.

De acuerdo con lo mencionado, el ISVIMED ha tomado como referencia la normativa establecida por el estado colombiano, CONPES 3854 de 2016 y 3995 de 2020 Modelo de Seguridad y Privacidad de MinTic y lo establecido en el decreto 1008 de 14 de junio 2018, adoptando las buenas prácticas y los lineamientos establecidos en los estándares ISO 27001:2013 y la Política de administración del riesgo de la Entidad.

2. Objetivos

2.1. Objetivo estratégico al cual le apunta el plan

El presente plan se articula con la plataforma estratégica de la entidad a través del aporte que éste hace al cumplimiento del siguiente objetivo estratégico:

- Implementar los lineamientos establecidos en materia de la seguridad y privacidad de la Información.
- Administrar los riesgos que afectan los resultados de la gestión institucional

2.2. Objetivo del Plan

Definir y aplicar los lineamientos para tratar de manera integral los riesgos de Seguridad y Privacidad de la Información, Seguridad Digital y Continuidad de la Operación Tecnológica que el Instituto social de Vivienda de Medellin ISVIMED pueda estar expuesto, y de esta manera alcanzar los objetivos, la misión y la visión institucional, protegiendo y preservando la integridad, confidencialidad, disponibilidad y autenticidad de la información.

3. Alcance

El alcance inicia con la identificación de los riesgos relacionados con la seguridad de la información hasta su posterior control.

4. Definiciones

- **Confidencialidad:** es la propiedad de prevenir que se divulgue la información a personas o sistemas no autorizados.

- **Integridad:** es la propiedad que busca proteger que se modifiquen los datos libres de forma no autorizada.

- **Disponibilidad:** es una característica, cualidad o condición de la información que se encuentra a disposición de quien tiene que acceder a esta, bien sean personas, procesos o aplicaciones.

- **Seguridad** de la Información: consiste en asegurar que los recursos del Sistema de Información de una empresa se utilicen de la forma que ha sido decidido y el acceso de información se encuentra contenida, así como controlar que la modificación solo sea posible por parte de las personas autorizadas para tal fin y por supuesto, siempre dentro de los límites de la autorización.

- **Activos de información** son los elementos que la Seguridad de la Información debe proteger. Por lo que son tres elementos lo que forman los activos:
    - **Información:** es el objeto de mayor valor para la empresa.
    - **Equipos**: suelen ser software, hardware y la propia organización.
    - **Usuarios:** son las personas que usan la tecnología de la organización.

- **Administración/gestión del riesgo:** actividades coordinadas para dirigir y controlar la organización con relación al riesgo.

- **Evento:** ocurrencia o cambio de un conjunto particular de circunstancias.

- **Política de administración del riesgo:** declaración de la dirección y las intenciones generales de una organización con respecto a la gestión del riesgo. La gestión o administración del riesgo establece lineamientos precisos y acerca del tratamiento, manejo y seguimiento a los riesgos.

- **Control:** medida que mantiene y/o modifica un riesgo.

- **Consecuencia/impacto:** resultado de un evento que afecta a los objetivos.

- **Fuente de riesgo:** elemento que, por si solo o en combinación con otros, tiene el potencial de generar riesgo.

- **Riesgo inherente:** es aquel al que se enfrenta una entidad en ausencia de acciones de la dirección para modificar su probabilidad o impacto.

- **Riesgo residual:** nivel de riesgo que permanece luego de tomar sus correspondientes medidas de tratamiento.

- **Probabilidad:** se entiende como la posibilidad de ocurrencia del riesgo. Esta puede ser medida con criterios de frecuencia o factibilidad.

- **Matriz de riesgos:** documento con la información resultante de la gestión del riesgo.

5. Marco legal

- **Decreto 103 de 2015** “por el cual se reglamenta parcialmente la Ley 1712 de 2014 y se dictan otras disposiciones”

- **Ley 1712 de 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”.

- **Decreto 1377 de 2013** “Por el cual se reglamenta parcialmente la Ley 1581 de 2012, Derogado Parcialmente por el Decreto 1081 de 2015.

- **ISO 27001 de 2013**. Tecnología de la información. Técnicas de seguridad. Sistemas de gestión de la seguridad de la Información (SGSI). Requisitos.

- **ISO/IEC 27002:2013**. Describe los objetivos de control y controles recomendables en cuanto a seguridad de la información.

- **Ley 1581 de 2012** “Por la cual se dictan disposiciones generales para la protección de datos personales.”

- **LEY 1273 de 2009**. Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado "de la protección de la información y de los datos"- y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones.

- Guía de administración del riesgo establecida por la Función Pública año 2021.

6. Desarrollo

6.1. Política de administración del riesgo y responsabilidades.

La gestión de riesgo es una actividad que está inmersa en las actividades del modelo de operación por procesos de la Entidad y hacen parte de las responsabilidades de la alta dirección y de las 3 líneas de defensa que establece el MECI.

Para el desarrollo del plan de tratamiento de riesgos, el ISVIMED ha establecido el procedimiento P-GM-06 Procedimiento para la administración del riesgo el cual establece los lineamientos para poder identificar, analizar, tratar, valorar, evaluar y monitorear los riesgos de Seguridad y Privacidad de la Información, Seguridad Digital y Continuidad de la Operación Tecnológica en las instalaciones y sedes del Instituto Social de Vivienda de Medellín ISVIMED.

Para la ejecución del plan de tratamiento de riesgos de Seguridad y Privacidad de la Información, Seguridad Digital y Continuidad de la Operación Tecnológica, se realizarán las actividades acordes a lo establecido en el Plan de Sostenibilidad del Modelo de Seguridad y Privacidad de la Información.

6.2. Identificar los riesgos.

Tiempo establecido para la actividad (ANS): 2 semanas

El líder de proceso, en coordinación con su equipo de trabajo, desarrollará el ejercicio de identificación de los riesgos que le apliquen, teniendo como base el objetivo y los procedimientos asociados al mismo, así como la demás información consignada en la caracterización de su proceso. Para desarrollar el proceso de identificación de riesgos se recomienda tener en cuenta la siguiente información asociada al proceso: informes de auditorías internas y externas, resultados de PQRS, cambios en los procedimientos y leyes que rigen los mismos, evaluación de indicadores, sugerencias de los comités existentes en el Instituto, etc. La identificación comprende los siguientes pasos:

6.2.1. Establecimiento del contexto

Los integrantes de cada proceso deberán analizar los factores internos (tanto de la organización como del proceso) y externos que afecten o puedan afectar su operación, dentro de los cuales pueden estar los siguientes:

Factores externos: se podrán considerar factores relacionados con el entorno político, económico, social, cultural, tecnológico, legal, ambiental, entre otros.

Factores internos (a nivel organizacional): dentro de este grupo se podrán considerar variables relacionadas con: disponibilidad de personal, asignación presupuestal, competencias del personal, seguridad y salud en el trabajo, articulación de procesos, estructura organizacional, cultura organizacional, gestión del conocimiento, disponibilidad de datos y sistemas de información, direccionamiento estratégico, aspectos tecnológicos, entre otros.

Factores internos (a nivel de proceso): se podrán analizar variables tales como: diseño del proceso, articulación, procedimientos asociados, liderazgo al interior, activos de TI del proceso, etc.

Dentro del análisis del contexto interno y de proceso se deberán identificar: las aplicaciones, servicios web, redes, información física o digital, tecnologías de la información, que se utilizan en el Instituto con las cuales tenga interacción el proceso o aquellas que sean propias del mismo.

Para la determinación y análisis de los factores internos y externos antes señalados es importante contar con la participación de los integrantes del proceso y su consolidación se realizará utilizando la plantilla que se relaciona a continuación (Disponible en el formato ***Matriz de Riesgos de proceso, pestaña 1, establecimiento contexto***):

Factor: Externo/Interno/Proceso	Variable	¿Cómo me puede afectar?	
		CARÁCTER: Positivo/negativo	Breve análisis

En el establecimiento del contexto para el proceso, es importante considerar los ejercicios similares que se hayan realizado a nivel estratégico (corporativo), dado que los mismos serán la base para el análisis a nivel de proceso. De igual forma, se deberán identificar y analizar el estado de los activos de TI con los que cuente el proceso, siguiendo la estructura que se señala en el formato ***Matriz de Riesgos de Proceso, pestaña 2, identificación activos TI***, tal como se muestra a continuación:

Activo	Responsable	Observaciones

Si de manera posterior al análisis de identificación de los activos de TI, se determina que el proceso no cuenta con los mismos, se deberá continuar el análisis con los factores internos y externos. Por último, la actualización del contexto estratégico se realizará como mínimo una vez al año y se dejará evidencia documentada del ejercicio.

6.2.2. Identificación de los riesgos

La identificación de los eventos que serán categorizados como riesgos se realiza teniendo en cuenta las variables analizadas en el establecimiento del contexto. De igual forma, es indispensable tener presente el objetivo del proceso. Una condición previa a la evaluación de riesgos es el establecimiento de objetivos asociados a los diferentes niveles de la entidad (COSO, 2013).

En ocasiones es posible recurrir a información externa de entidades con objetos sociales similares, para mapear posibles eventos que puedan ser tenidos en cuenta dentro de la identificación de los riesgos. Para la identificación de los riesgos se seguirán los siguientes pasos: lluvia de ideas sobre posibles riesgos y definición de los riesgos, las cuales se desarrollan a continuación.

a) Lluvia de ideas sobre posibles riesgos

Los integrantes del proceso iniciarán la identificación de los riesgos realizando una lluvia de ideas con opciones que podrán ser consideradas de manera posterior como riesgos. La lluvia de ideas se debe apoyar en el resultado del establecimiento del contexto realizado en la etapa anterior. Dentro del ejercicio es importante desarrollar las siguientes preguntas:

¿Qué puede suceder?

¿Cómo puede suceder?
¿Cuándo puede suceder?
¿Qué consecuencias tendría su materialización?

La lluvia de ideas permite conocer múltiples eventos y a su vez identificar los de mayor relevancia para analizarlos en las etapas siguientes de la metodología de administración del riesgo.

Como apoyo a la lluvia de ideas es importante tener en cuenta los riesgos de los procesos de versiones anteriores, los cuales pueden ser ratificados sin agregar cambios, ratificados con cambios o eliminados dentro de la fase de identificación. También una fuente de consulta para la identificación de los riesgos son los informes de auditoría interna y externa, que se hayan realizado a cada proceso.

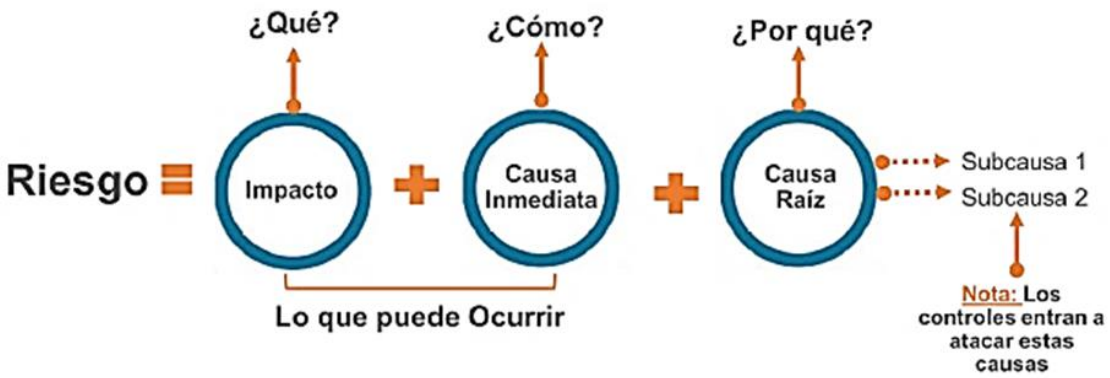
b) Definición de los riesgos

Teniendo como insumo los resultados del paso anterior, se procederá a la definición específica de cada uno de los riesgos desarrollando los siguientes elementos:

(1) Descripción del Riesgo	(2) Subcausas	(3) Clasificación del riesgo

(1) Descripción del Riesgo

La descripción del riesgo debe contener todos los detalles que sean necesarios y que sea fácil de entender tanto para el líder del proceso como para personas ajenas al mismo. Se debe utilizar la siguiente estructura que facilita su redacción y proporciona claridad, la cual inicia con la frase POSIBILIDAD DE y se analizan los siguientes aspectos:



La anterior estructura evita la subjetividad en la redacción y permite entender la forma como se puede manifestar el riesgo, así como sus causas inmediatas y causas principales o raíz, esta es información esencial para la definición de controles en la etapa de valoración del riesgo.

Desglosando la estructura propuesta tenemos:

Impacto: las consecuencias que puede ocasionar a la organización la materialización del riesgo. En las entidades públicas se pueden clasificar de dos maneras: afectación económica y/o afectación reputacional.

Causa inmediata: circunstancias o situaciones más evidentes sobre las cuales se presenta el riesgo, las mismas no constituyen la causa principal o base para que se presente el riesgo.

Causa raíz: es la causa principal o básica, corresponden a las razones por la cuales se puede presentar el riesgo, son la base para la definición de controles en la etapa de valoración del riesgo. Se debe tener en cuenta que para un mismo riesgo pueden existir más de una causa o subcausas que pueden ser analizadas.

A continuación, se expone el siguiente ejemplo:

Redacción inicia con:	QUE?	COMO SE REFLEJA?	POR QUE?
Posibilidad de	afectación económica del Instituto	* por la indebida asignación de recursos publicos (detrimento patrimonial).	debido a la asignación / destinación del subsidio Municipal de Vivienda sin el cumplimiento de los requisitos legales.
	afectación reputacional del Instituto	* por hallazgos disciplinarios y penales por parte de los entes de control. * Por el costo social asociado a la perdida de la oportunidad para la asignación del subsidio Municipal de Vivienda a hogares que cumplen con los requisitos legales.	
	Impacto	Causa Inmediata	Causa Raíz

La descripción del riesgo consolida o resume los análisis sobre impacto + causa inmediata + causa raíz, permitiendo contar con una redacción clara y concreta del riesgo identificado, tal como se establece en la Guía para la administración del Riesgo y diseño de controles de la Función Pública, versión 5.

La descripción del riesgo debe quedar de la siguiente forma:

POSIBILIDAD DE + Impacto para la entidad (Qué) + Causa Inmediata (Cómo) + Causa Raíz (Por qué)

En los ejercicios de actualización, los integrantes del proceso revisarán los riesgos identificados en ejercicios anteriores, teniendo en cuenta el análisis de contexto actual y podrán ratificarlos, modificarlos o eliminarlos.

Para la identificación y redacción de los riesgos de corrupción se debe utilizar la misma estructura arriba descrita, teniendo en cuenta que se enmarquen en su definición:

Posibilidad de que, por acción u omisión, se haga uso del poder para desviar la gestión de lo público para el beneficio particular (tomado de la Guía para la gestión del riesgo de corrupción de la Presidencia de la República del año 2015).

(2) Subcausas: consignar las razones por las cuales se podría materializar el riesgo. En la definición de las subcausas es posible utilizar palabras tales como: “ausencia de”, “falta de”, “poco o escaso”, “insuficiente”, “debilidades en”, “no aplicación de”, entre otros.

(3) Clasificación del riesgo: basándose en la descripción de las tipologías de riesgo, abajo desarrolladas, se debe escoger la que se considere se ajusta a la naturaleza del evento que se está analizando. Dentro de las tipologías se tienen:

Riesgos estratégicos: posibilidad de ocurrencia de eventos que afecten los objetivos estratégicos del Instituto y por tanto impactan toda la entidad. Este tipo de riesgos están asociados a los objetivos o proyectos estratégicos del Instituto.

Riesgos operativos: posibilidad de ocurrencia de eventos que afecten los procesos de la entidad. Este tipo de riesgos se relacionan con los procesos y las fallas humanas que puedan llevar a la interferencia de los mismos. También se deben considerar los riesgos asociados directamente a la integridad de los colaboradores del Instituto.

Riesgos financieros: posibilidad de ocurrencia de eventos que afecten los estados financieros y todas aquellas áreas involucradas con el proceso financiero como presupuesto, tesorería, contabilidad, cartera, costos, etc.

Riesgos tecnológicos: posibilidad de ocurrencia de eventos que afecten total o parcialmente la infraestructura tecnológica (hardware, software, redes, etc.) del Instituto. Son generados por el uso de tecnología, como virus informáticos, vandalismo puro o de ocio en las redes informáticas, fraudes, intrusiones de hackers, colapso de las telecomunicaciones que puede generar daño de información o interrupción del servicio.

Riesgos de cumplimiento: posibilidad de ocurrencia de eventos que afecten la situación jurídica o contractual de la organización debido a su incumplimiento o desacato a la normatividad legal y las obligaciones contractuales.

Riesgo reputacional: posibilidad de ocurrencia de un evento que afecte la imagen, buen nombre o reputación del Instituto ante sus partes interesadas.

Riesgos de corrupción: posibilidad de que, por acción u omisión, se use el poder para desviar la gestión del Instituto hacia un beneficio particular.

La información resultante de la identificación del riesgo se deberá consignar en el formato ***Matriz de Riesgos de Proceso, pestaña 3, matriz de riesgos***, tal como se señala a continuación:

4.2. IDENTIFICACION DEL RIESGO						
Temática / Linea de Acción	QUE? Impacto	COMO SE REFLEJA? Causa Inmediata	POR QUE? Causa Raiz	Descripción del Riesgo	Subcausas	Clasificación del Riesgo

6.3. Evaluar los riesgos

Tiempo establecido para la actividad (ANS): 2 días

Dentro de esta fase de desarrollan los siguientes pasos: 6.3.1 Análisis de riesgos y 6.3.2 Evaluación de Riesgos, tal como se desarrollan a continuación:

6.3.1 Análisis de riesgos (riesgo inherente): en esta etapa se determinará la probabilidad y el impacto de los riesgos identificados sin tener en cuenta el efecto de los controles que se estén implementando o se puedan implementar para su tratamiento.

Por **probabilidad** se entiende la posibilidad de ocurrencia del riesgo, la cual se mide teniendo como base la frecuencia del evento en un término de tiempo

determinado. Para el cálculo de la probabilidad inherente se utilizará la siguiente tabla:

	Frecuencia de la Actividad	Probabilidad
Muy Baja	La actividad que conlleva el riesgo se ejecuta como máximos 2 veces por año	20%
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%
Alta	La actividad que conlleva el riesgo se ejecuta mínimo 500 veces al año y máximo 5000 veces por año	80%
Muy Alta	La actividad que conlleva el riesgo se ejecuta más de 5000 veces por año	100%

La anterior tabla pretende hacer un cálculo de la probabilidad más preciso ya que mientras más se ejecute una actividad aumenta la probabilidad de que el riesgo se materialice, es decir, hay más exposición al riesgo.

De otro lado, por impacto se entienden como las consecuencias que pueden ocasionar al proceso/Instituto la materialización del riesgo. Para determinar el impacto se deberá escoger dentro de la “Tabla de Calificación de Impacto” los descriptores que aplican al nivel de impacto del riesgo que se esté analizando, de la siguiente manera:

Tabla de Calificación de Impacto Inherente

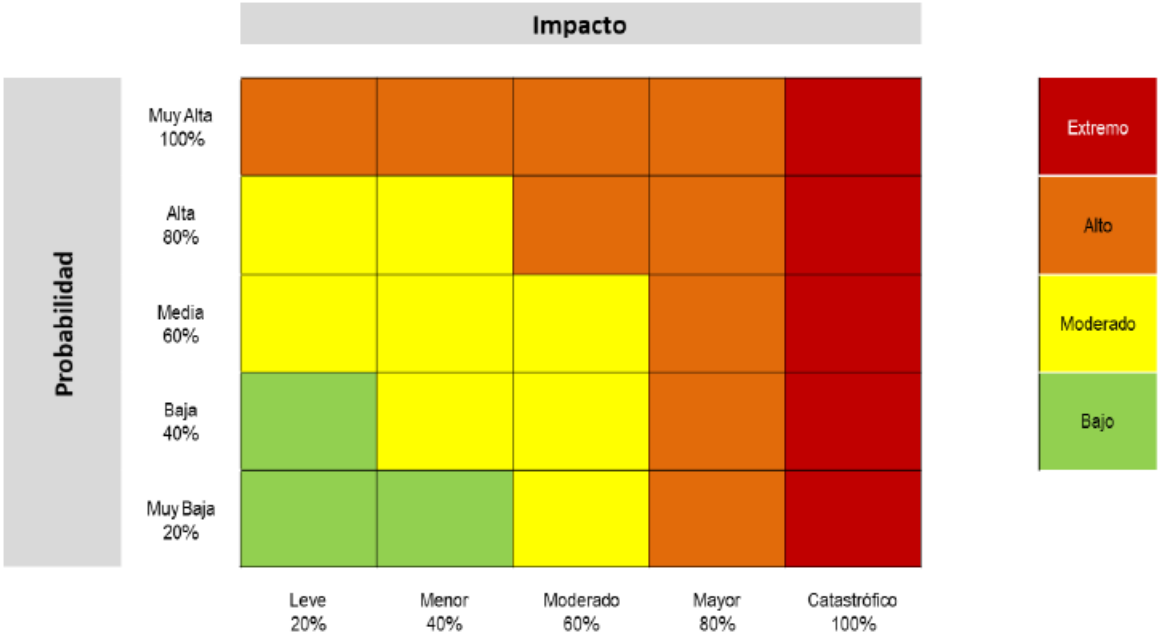
Descriptor	Nivel	Descripción
LEVE	20%	1. No tiene impactos en la prestación del servicio ni en la operación de los procesos internos. 2. No afecta el cumplimiento de la misión ni de los objetivos estratégicos del Plan de Desarrollo. 3. No representa impactos financieros para la organización. 4. No genera multas ni sanciones. 5. Genera consecuencias negativas en la imagen (opinión) ante sus grupos de interés (internos) de baja intensidad (puntuales) y mitigable o reversible de manera inmediata. 6. No genera fallas en el funcionamiento del software o hardware, ni perdida/daño de

Descriptor	Nivel	Descripción
		información o mal uso de esta.
BAJA	40%	1. Interrupción mínima en la prestación de los servicios o en la operación de los procesos. Reversibles de manera inmediata. 2. Retrasa algunas actividades de proyectos, pero no afectan la ejecución global de los mismos. No afecta el cumplimiento los objetivos estratégicos del Plan de Desarrollo. 3. Puede llevar traslados de rubros, ajustes en el presupuesto, pero no representa impactos financieros para la organización. 4. Genera llamados de atención, pero no multas ni sanciones. 5. Genera consecuencias negativas en la imagen (opinión) ante sus grupos de interés de intensidad media y mitigable o reversible en el corto plazo (6 meses). La imagen del Instituto se podría ver afectada a nivel regional y local. 6. Genera fallas de funcionamiento en el software o hardware que dificultad el acceso a información afectando funciones específicas, cargos específicos. Reversible en un término no mayor a 2 horas.
MODERADA	60%	1. Genera interrupción y demora en la prestación del servicio y/o en el desarrollo de las actividades de los procesos. Reversibles en un término de máximo 1 día. 2. Retrasa actividades, llevando a extender plazos para la ejecución de las mismas, pero no afectan la ejecución global de los proyectos. No afecta el cumplimiento de los objetivos estratégicos del Plan de Desarrollo. 3. Puede llevar traslados de rubros, ajustes en el presupuesto, pero no representa impactos financieros para la organización. Puede desencadenar en retrasos del plan de inversiones. 4. Genera algunas multas y sanciones por incumplimiento. Puede generar procesos disciplinarios al personal interno. 5. Genera consecuencias negativas en la imagen (opinión) ante sus grupos de interés (comunidad, de intensidad alta y mitigable o reversible en el mediano plazo (1 año). La imagen del Instituto se podría ver afectada a nivel regional y local. 6. Genera fallas de funcionamiento en el software o hardware que dificultad el acceso a información afectando funciones específicas, cargos específicos. Reversible en un término no mayor a 5 horas.

Descriptor	Nivel	Descripción
ALTA	80%	1. Genera interrupción y demora en la prestación del servicio y/o en el desarrollo de las actividades de los procesos. Reversibles en un término de 1 a 2 días. 2. Retrasa proyectos, llevando a extender plazos, aumentar presupuesto, para la ejecución de estos, pero no afectan la ejecución global. No afecta el cumplimiento de los objetivos estratégicos del Plan de Desarrollo. 3. Puede llevar traslados de rubros, ajustes en el presupuesto y retrasos en su ejecución. Representa impactos financieros para la organización (perdida, no desembolso) que llevan al incumplimiento de proyectos del plan desarrollo. 4. Genera multas y sanciones por incumplimiento. Puede generar procesos disciplinarios al personal interno, remoción de personal de sus cargos. 5. Genera consecuencias negativas en la imagen (opinión) ante sus grupos de interés de intensidad grave y mitigable o reversible en el largo plazo (Cuatro años o menos). La imagen del Instituto se podría ver afectada a nivel regional y nacional. 6. Genera fallas de funcionamiento en el software o hardware que dificultad el acceso a información afectando módulos completos (SIFI), afectación de servidores (Correo, Directorio Activo). Reversible en un término no mayor a 8 horas.
MUY ALTA	100%	1. Genera interrupción y demora significativa en la prestación del servicio y/o en el desarrollo de las actividades de los procesos. Reversibles en un término de 3 a 5 días. 2. Genera incumplimiento de los proyectos. Genera sobrecostos y afecta el cumplimiento de los objetivos estratégicos de Plan de Desarrollo. 3. Representa impactos financieros para la organización (perdida, no desembolso) que llevan al incumplimiento de objetivos del plan desarrollo. 4. Genera multas y sanciones por incumplimiento. Puede generar procesos disciplinarios al personal interno, remoción de personal de sus cargos. Pago de indemnizaciones por incumplimiento que puede llevar a afectar el presupuesto del Instituto. 5. Genera consecuencias negativas en la imagen (opinión) ante sus grupos de interés (comunidad, empleados, clientes, gobierno, etc.) con una intensidad muy alta y reversible en el largo plazo (más de 5 años para revertir la afectación). La imagen del Instituto se podría ver afectada a nivel regional y nacional. 6. Genera fallas de funcionamiento en el software o hardware que dificultad el acceso a información afectando módulos completos (SIFI), afectación de servidores (Correo, Directorio Activo). Reversible en un tiempo superior a un día.

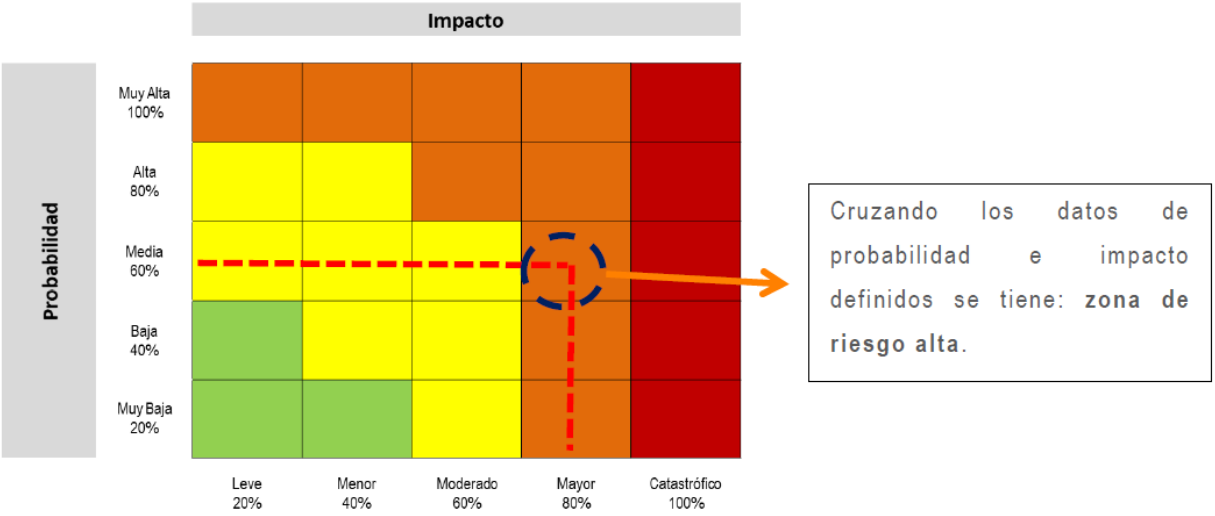
Nota 1: en caso de que un riesgo tenga más de un impacto dentro del análisis, se deberá considerar aquel (impacto) de mayor relevancia, es decir aquel que en caso de materializarse el riesgo genere situaciones de mayor afectación para el proceso/entidad.

A partir del análisis de la probabilidad de ocurrencia del riesgo y sus consecuencias o impactos, se busca determinar la zona de riesgo inicial (RIESGO INHERENTE). Se definen 4 zonas de severidad en la matriz de calor que se muestra a continuación:



Fuente: Adaptado del Curso Riesgo Operativo Universidad del Rosario por la Dirección de Gestión y Desempeño Institucional de Función Pública, 2020.

Ejemplo: Para un riesgo con probabilidad inherente media (60%) e impacto inherente mayor (80%), su ubicación en la zona de riesgo inherente será la siguiente:



La información de PROBABILIDAD e IMPACTO se ingresa en el formato ***Matriz de Riesgos de Proceso, pestaña 3, matriz de riesgos***, automáticamente hará el cálculo para la zona de riesgo inherente (Columna N)

J	K	L	M	N
EVALUACION DE RIESGO INHERENTE				
Probabilidad Inherente	%	Impacto Inherente	%	Zona de Riesgo Inherente
Media	60%	Mayor	80%	Alto

6.3.2. Valoración de los riesgos (Riesgo Residual):

En esta etapa se determinará la probabilidad y el impacto de los riesgos identificados teniendo en cuenta el efecto de los controles que se estén implementando para mitigar la materialización del riesgo. En este sentido, se determinará el riesgo residual, el cual resulta de determinar la probabilidad y el impacto del riesgo una vez se haya realizado la identificación y la valoración de los controles existentes. Se realiza en dos momentos: (1) identificación y valoración de controles para cada riesgo, y (2) evaluación del riesgo residual en cuanto a probabilidad e impacto teniendo en cuenta el efecto ejercido por los controles identificados.

6.3.2.1. Identificación y valoración de controles

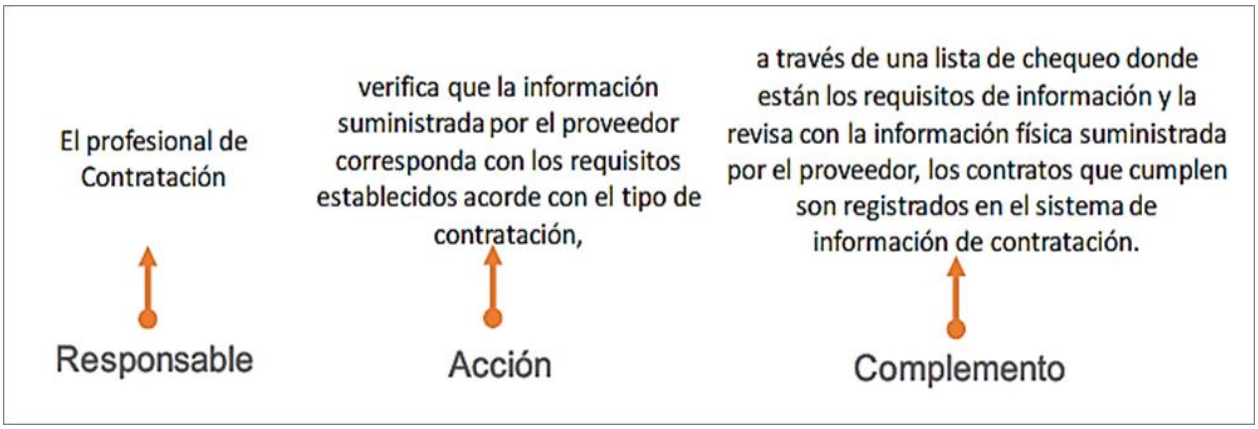
Conceptualmente un control se define como la medida que permite reducir o mitigar el riesgo. Para la valoración de controles se debe tener en cuenta:

- La identificación de controles se debe realizar a cada riesgo a través de las entrevistas con los líderes de procesos o servidores expertos en su labor. En este caso sí aplica el criterio experto.
- Los responsables de implementar y monitorear los controles son los líderes de proceso con el apoyo de su equipo de trabajo.
- En lo posible cada subcausa debe tener un control asociado.

Se propone la siguiente estructura para la adecuada redacción de controles:

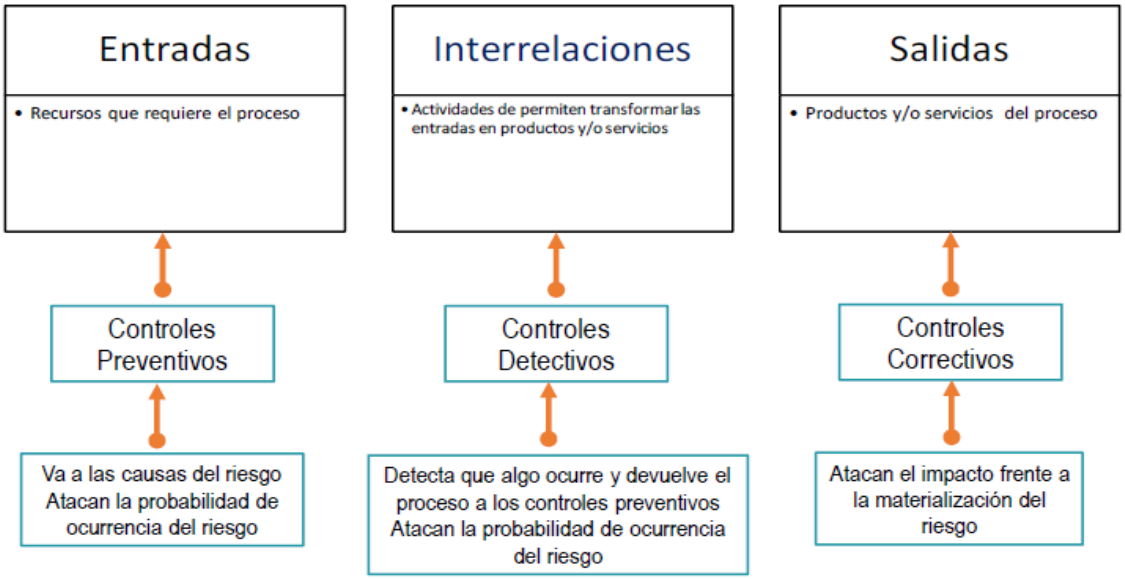
- **Responsable de ejecutar el control:** identifica el cargo del servidor que ejecuta el control, en caso de que sean controles automáticos se identificará el sistema que realiza la actividad.
- **Acción:** se determina mediante verbos que indican la acción que deben realizar como parte del control.
- **Complemento:** corresponde a los detalles que permiten identificar claramente el objeto del control.

A continuación, se relaciona ejemplo de la Guía para la administración del riesgo de la Función Pública, versión 5:



Tipologías de controles:

A través del ciclo de los procesos es posible establecer cuándo se activa un control y, por lo tanto, establecer su tipología con mayor precisión. Para comprender esta estructura conceptual, en la siguiente figura se consideran 3 fases globales del ciclo de un proceso así:



Fuente: Adaptado del Curso Riesgo Operativo Universidad del Rosario por la Dirección de Gestión y Desempeño Institucional de Función Pública, 2020.

Control preventivo: control accionado en la entrada del proceso y antes de que se realice la actividad originadora del riesgo, se busca establecer las condiciones que aseguren el resultado final esperado.

Control detectivo: control accionado durante la ejecución del proceso. Estos controles detectan el riesgo, pero generan reprocesos.

Control correctivo: control accionado en la salida del proceso y después de que se materializa el riesgo. Estos controles tienen costos implícitos.

Valoración de controles:

A continuación, se analizan los atributos para el diseño del control, teniendo en cuenta características relacionadas con la eficiencia y la formalización.

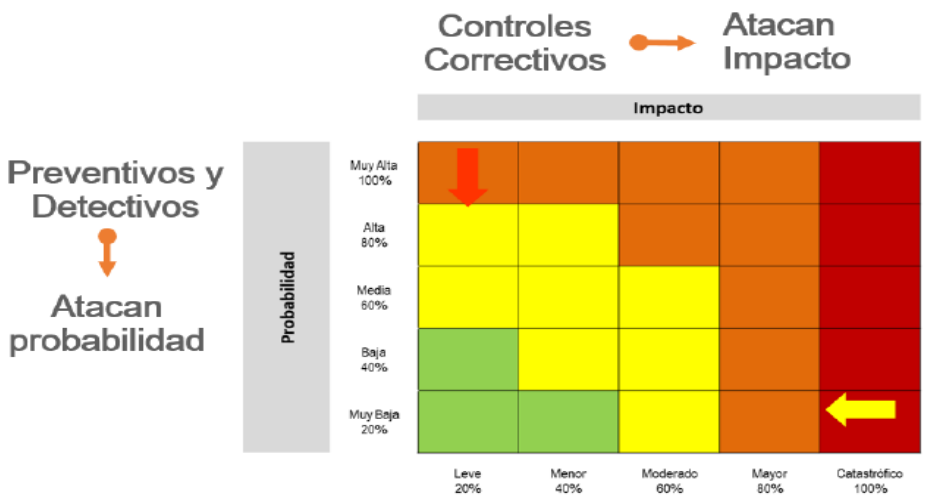
Tabla de Atributos para el diseño del control:

Características			Descripción	Peso
Atributos de Eficiencia	**Tipo**	**Preventivo**	Va hacia las causas del riesgo, aseguran el resultado final esperado.	**25%**
		Detectivo	Detecta que algo ocurre y devuelve el proceso a los controles preventivos. Se pueden generar reprocesos.	**15%**
		Correctivo	Dado que permiten reducir el impacto de la materialización del riesgo, tienen un costo en su implementación.	**10%**
	Implementación	**Automático**	Son actividades de procesamiento o validación de información que se ejecutan por un sistema y/o aplicativo de manera automática sin la intervención de personas para su realización.	**25%**
		Manual	Controles que son ejecutados por una persona., tiene implícito el error humano.	**15%**
***Atributos de Formalización**	**Documentación**	**Documentado**	Controles que están documentados en el proceso, ya sea en manuales, procedimientos, flujogramas o cualquier otro documento propio del proceso.	-
		Sin Documentar	Identifica a los controles que pese a que se ejecutan en el proceso no se encuentran documentados en ningún documento propio del proceso	-
	Frecuencia	**Continua**	Este atributo identifica a los controles que se ejecutan siempre que se realiza la actividad originadora del riesgo.	-
		Aleatoria	Este atributo identifica a los controles que no siempre se ejecutan cuando se realiza la actividad originadora del riesgo	-
	Evidencia	**Con Registro**	El control deja un registro que permite evidenciar la ejecución del control	-

		Sin Registro	El control no deja registro de la ejecución del control	-

*****Nota: Los atributos de formalización se recogerán de manera informativa, con el fin de conocer el entorno del control y complementar el análisis con elementos cualitativos; éstos no tienen una incidencia directa en su efectividad.

Se debe tener en cuenta que es a partir de los controles que se dará el movimiento en la matriz de calor.
La figura que se muestra a continuación muestra el movimiento en el eje de probabilidad y en el eje de impacto de acuerdo con los tipos de controles.



Fuente: Adaptado del Curso Riesgo Operativo Universidad del Rosario por la Dirección de Gestión y Desempeño Institucional de Función Pública, 2020.

La ***Matriz de Riesgos de Proceso, pestaña 3*** automáticamente hará el cálculo, acorde con el control o controles definidos y con sus atributos analizados, lo que permitirá establecer el nivel de riesgo residual, como se muestra a continuación:

O	P	Q	R	S	T	U	V	W	X	Y	Z	AA	AB	AC	AD	AE	AF	AG
4.3. EVALUACIÓN DEL RIESGO																		
VALORACION DE CONTROLES										EVALUACION DEL RIESGO RESIDUAL								
			Atributos															
No. Control	Descripción del Control	Afectación	Tipo	Implementació	Calificación	Documentació	Frecuencia	Evidencia	Nombre de la evidencia	Probabilidad Residual	Probabilidad Residual	%	Impacto Residual	%	Probabilidad Residual Final	%	Impacto Residual Final	%	Zona de Riesgo Residual Final
1	Control 1 ejemplo	Probabilidad	Preventivo	Manual	40%	Documentado	Aleatoria	Con Registro	Evidencia 1	36.0%	Baja	36%	Mayor	80%	Baja	36.0%	Moderado	60.0%	Moderado
2	Control 2 ejemplo	Impacto	Correctivo	Manual	25%	Sin Documentar	Aleatoria	Con Registro	Evidencia 2	36.0%	Baja	36%	Moderado	60%					

Se debe asegurar que los controles que han sido identificados para atacar las causas del riesgo se encuentren descritos en los procedimientos, guía, instructivo, manual, según aplique, que el proceso utiliza para desarrollar la actividad donde se genera el riesgo. De igual forma, cuando se esté identificando los controles se podrá recurrir a los tipos documentales antes descritos (propios del proceso) para efectos de identificar los controles que se tienen implementados y de esta manera asociarlos a las causas identificadas para cada riesgo. Puede pasar que los controles se encuentren consignados en los procedimientos, pero los mismos pueden necesitar ajustes por lo cual desde el responsable del proceso deberá emprender el trabajo de actualización.

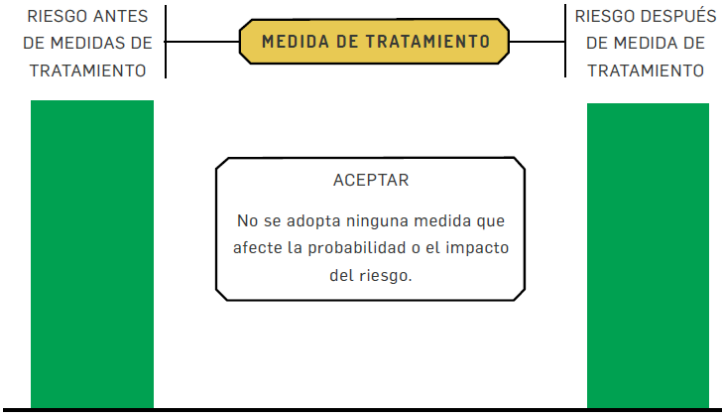
6.4. Realizar el tratamiento de los riesgos

Tiempo establecido para la actividad (ANS): 2 días

El tratamiento de los riesgos implica dos pasos: 6.4.1 Determinar la acción de tratamiento y 6.4.2 Formular acciones específicas, las cuales se implementarán para disminuir la probabilidad y/o atenuar el impacto del riesgo.

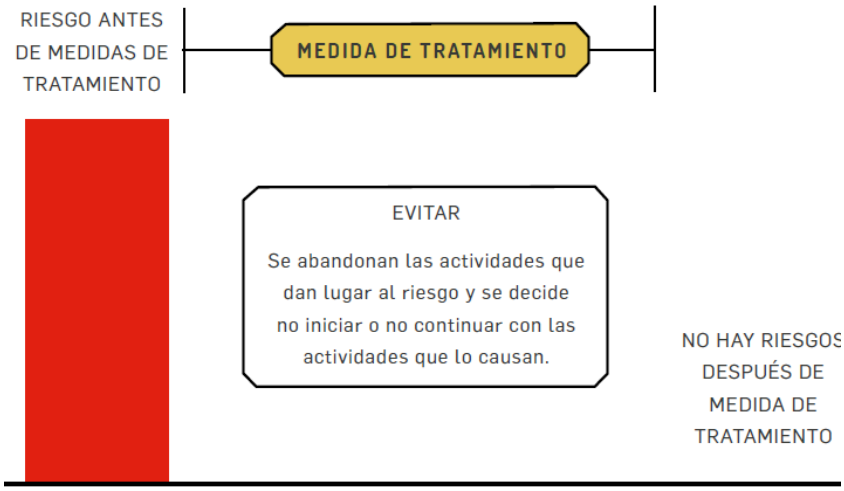
6.4.1. Determinar la acción de tratamiento: en este paso se debe escoger una o la combinación de las acciones de tratamiento que aplique para el riesgo. Entre las acciones que son posibles escoger se tienen:

(i) Aceptar: No se adopta ninguna medida que afecte la probabilidad o el impacto del riesgo.

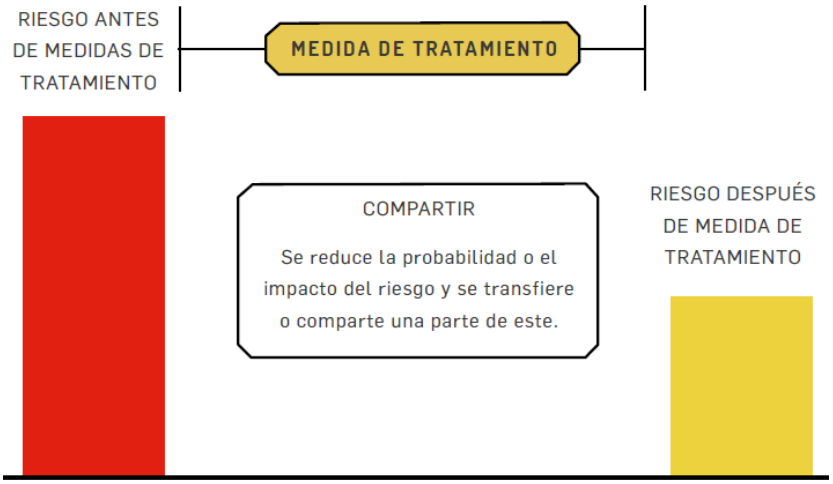


Si bien la aceptación de un riesgo implica convivir con el mismo sin poder desarrollar mayores acciones al respecto, es importante que el proceso tenga pleno conocimiento del mismo para efectos de planificar el desarrollo de las actividades.

(ii) Evitar: Se abandonan las actividades que dan lugar al riesgo y se decide no iniciar o no continuar con las actividades que lo causan.



(ii) Reducir - Compartir: Se reduce la probabilidad o el impacto del riesgo y se transfiere o comparte una parte de éste.

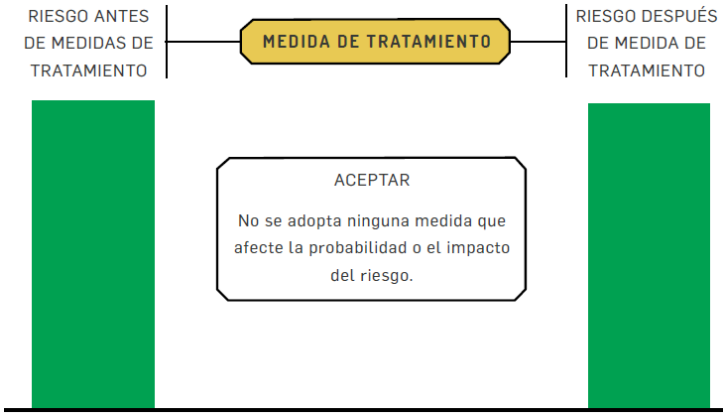


(iv) Reducir - Mitigar: Se adoptan medidas para reducir la probabilidad o el impacto del riesgo o ambos, esto conlleva a la implementación de controles.

El tratamiento de los riesgos implica dos pasos: Determinar la acción de tratamiento y Formular acciones específicas, las cuales se implementarán para disminuir la probabilidad y/o atenuar el impacto del riesgo.

Determinar la acción de tratamiento: en este paso se debe escoger una o la combinación de las acciones de tratamiento que aplique para el riesgo. Entre las acciones que son posible escoger se tienen:

- **Aceptar:** No se adopta ninguna medida que afecte la probabilidad o el impacto del riesgo.



Lo ideal sería que los riesgos se puedan llevar hasta una zona baja, pero se debe tener en cuenta que existen causas que pueda que se deriven de agentes generadores externos, por lo cual no se podrían desarrollar acciones al respecto. En este sentido, es posible que un riesgo se deba aceptar y no se puedan desarrollar acciones adicionales, aunque el mismo este una zona moderada.

6.4.2 Formular acciones específicas: una vez se hayan escogido las acciones de tratamiento desarrolladas en el paso anterior, se debe proceder a formular las actividades que de manera específica ayudarán a desplegar las mismas. Para la formulación de las acciones de tratamiento se deben seguir los lineamientos establecidos en el procedimiento “Procedimiento para la aplicación de acciones correctivas, preventivas, mejora y planificación de cambios”.

Para los riesgos ubicados en zona extrema y alta se debe registrar una acción preventiva de forma prioritaria. Para las zonas moderada y baja se deben plantear acciones para mejorar los controles existentes o crear los que hagan falta, lo cual permita que el riesgo disminuya en su probabilidad o impacto.

Se debe monitorear el comportamiento de los riesgos con el fin de lograr que aquellos ubicados en las zonas extremas y altas, bajen de cuadrante y se ubiquen en zona moderada o baja y se mantengan en esta última.

En la formulación de acciones se debe tener en cuenta que el control para una causa identificada para un riesgo en el proceso “X” puede depender de otro proceso, por lo cual se deberá trabajar de manera articulada para que cada proceso, desde su competencia documente las acciones a que haya lugar.

6.5. Ejecutar el monitoreo y seguimiento

Tiempo establecido para la actividad (ANS): Seguimiento: 1 semana; Monitoreo: constante.

El monitoreo a los riesgos se debe realizar de manera permanente y está a cargo del líder de cada proceso y su equipo de colaboradores. El líder del proceso debe consolidar un seguimiento a la matriz de riesgos de manera trimestral y deberá ser enviado a la Subdirección de Planeación. El líder del proceso, en colaboración con los enlaces del proceso, podrá consignar la información resultante del monitoreo en la parte final de la matriz en la celda denominada “Seguimiento trimestre I, II, III o IV (según aplique), esto con el fin de consolidar la información que de manera posterior deberá ser enviada a la Subdirección de Planeación.

Por su parte la Subdirección de Planeación consolidará un informe sobre la administración del riesgo a nivel global, utilizando como insumo la información suministrada por cada proceso la resultante de las actividades de acompañamiento desarrolladas. Dicho informe será presentado al Comité Institucional Coordinador de Control Interno de manera trimestral, para que al respecto se revise, analice y se tomen las medidas a nivel estratégico a que haya lugar.

Para efectos del seguimiento a los riesgos clasificados como de corrupción, se consolidará una matriz propia para la temática, la cual resultará del trabajo de identificación de riesgos a nivel de proceso. El seguimiento a esta matriz aparte de contar con el monitoreo de cada subdirección y de la Subdirección de Planeación (en el marco del informe cuatrimestral para reportar dicho componente al PAAC), también será objeto de auditoría por parte de la Oficina de Control Interno con corte a las siguientes fechas: 30 de abril, 31 de agosto y 31 de diciembre de cada año.

Cuando un riesgo se materialice, el líder del proceso donde ocurrió deberá tomar las acciones de manera inmediata para corregir la situación e implementar una acción correctiva, donde se haga el respectivo análisis de causas. La materialización de los riesgos deberá ser reportada por el líder o un miembro del proceso, a través de correo electrónico, al área de planeación y de manera conjunta se deberá iniciar la actualización de la información pertinente en la matriz de riesgos. De igual forma, para efectos de mejorar el seguimiento a los riesgos materializados desde la Oficina de Control Interno se informará a la Sub. de Planeación cuando se identifique la materialización de algún riesgo en el marco del desarrollo de las auditorías internas.

Por último, desde la subdirección de Planeación se desarrollará un ejercicio de autoevaluación del sistema de administración del riesgo, con lo cual se calculará el índice de madurez del mismo. Esta autoevaluación se realizará a través del formato Índice de Madurez Administración del Riesgo, el cual se diseñó basados en los requerimientos de la ISO 31000:2018. De manera adicional se medirán el indicador Efectividad en el cierre de acciones derivadas de riesgos.

Nombre	Formula
Efectividad en el cierre de acciones derivadas de riesgos	# acciones cerradas de manera efectiva/#acciones totales derivadas de riesgo*100
Índice de madurez de la administración del riesgo	Promedio (Evaluación de los Principios requeridos para la administración del riesgo)

6.6. Efectuar la comunicación y consulta

Tiempo establecido para la actividad (ANS): - constante según aplique

La comunicación y consulta con las partes involucradas, tanto internas como externas, tendrá lugar durante todas las etapas del proceso para la administración del riesgo. Desde la Subdirección de Planeación se desarrollarán estrategias de comunicación encaminadas a sensibilizar sobre la importancia de la administración del riesgo y sobre la aplicación de la metodología dentro de los procesos del Instituto. De igual forma, es responsabilidad de los líderes de proceso velar porque el personal a su cargo conozca los riesgos que le apliquen y desarrollen los controles que se encuentren establecidos en los procedimientos a su cargo. En relación a la consulta, los líderes de los procesos, quienes conocen de primera mano el estado de riesgo, deberán comunicar los resultados de los ejercicios de monitoreo y seguimiento que apoyen la toma de decisiones. Desde la Oficina de Control Interno se deberán comunicar los resultados de los ejercicios de aseguramiento a las instancias pertinentes, así como los posibles cambios que identifique en alguna variable del contexto que permita administrar los eventos de manera oportuna.

Por último, la línea estratégica deberá analizar los cambios en el contexto, interno y externo, y comunicarlos de manera oportuna para que al respecto se desarrolle el proceso de administración del riesgo que permita evitar la materialización de los riesgos

7. Matriz de riesgos gestión TI

4.2 IDENTIFICACIÓN DEL RIESGO						4.3 EVALUACIÓN DE LOS RIESGOS						
						4.3.1 Análisis del Riesgo			4.3.2 Valoración de los riesgos			
No.	RIESGO	DESCRIPCIÓN	CAUSA (S)	EFECTO (S)	TIPO DE RIESGO	PROBABILIDAD	IMPACTO	EVALUACIÓN DEL RIESGO (RIESGO INHERENTE)	CONTROLES EXISTENTES	PROBABILIDAD	IMPACTO	EVALUACIÓN DEL RIESGO (RIESGO RESIDUAL)
1	Falta o vencimiento de licencias	Que el instituto no cuente con las licencias de uso de software necesarias para la ejecución de los procesos institucionales.	1. Falta de identificación de las necesidades de licenciamiento. 2. Falta de control a las vigencias de las licencias.	* Afecta la ejecución de los procesos. * Sanciones por parte del fabricante del software * Suspensión de la operación del software.	Riesgos operativos	4	4	16 - Zona Extrema	1. **Procedimiento (Cual es el control):** Solicitud de necesidades de licenciamiento a las áreas a través de memorandos. **Responsable:** Subdirector Administrativo y Financiera. **Frecuencia:** Anualmente. **Evidencia:** Memorando o Correo. **Objetivo:** Conocer las necesidades del instituto sobre temas de licenciamiento para generar una efectiva gestión de las adquisiciones. 2. **Procedimiento (Cual es el control):** Planilla de control de licencias. **Responsable:** Tecnólogo de Sistemas. **Frecuencia:** Trimestral **Evidencia:** Planilla de control de licencias. **Objetivo:** Garantizar que se cuenta con las respectivas licencias vigentes y con las herramientas necesarias para realizar las distintas funciones.	2	2	4 - Zona Baja
2	Perdida de información (Robo, alteración y/o perdida de información)	La información almacenada en los diferentes equipos y servidores puede ser vulnerada por virus o accesos no autorizados afectando la integridad y disponibilidad de la información.	1. Ausencia o debilidad en las políticas de seguridad de la información. 2. Incendio (propagación de fuego). 2.1 Corto circuito. 3. Extracción manual de la información por personal no autorizado. 4. Centralización de la información en un solo usuario. 5. Ataque informático.	* Afecta la ejecución de los procesos. * Manipulación indebida de información. * Uso de información confidencial. * Daño a la imagen institucional.	Riesgos operativos	5	4	20 - Zona Extrema	1. **Procedimiento:** No existe (Objetivo de las políticas de seguridad de la información con las cuales no se cuenta actualmente). 2. **Procedimiento:** Ubicación de extintores en los lugares asesorados por la ARL-Brigada de emergencia. **Objetivo:** Evitar daños por incendio. **Responsable:** Profesional Especializado, Profesional en Seguridad y Salud en el Trabajo. **Frecuencia:** Cada vez que pasa. **Evidencia:** Extintores. **2.1 No existe control.** (Red contra incendios) Se esta implementando. 3. **Procedimiento:** Solicitar la asignación de permisos a solicitud de Jefe Inmediato o Supervisor. **Responsable:** Equipo TIC. **Frecuencia:** Según requerimiento. **Evidencia:** Solicitud en SIFI o por medio de correo. **Objetivo:** Garantizar que los accesos a la información se asignen a personal autorizado. 4. **Procedimiento:** Almacenamiento de la información en los recursos compartidos (Recursos respaldados por medio de backup diario) **Responsable:** Equipo TIC y usuarios. **Frecuencia:** Constante (Backup diario). **Evidencia:** Copias de información en discos externos. **Objetivo:** Evitar perdida de información. 5.**Procedimiento:** Cortafuegos. (firewall). **Responsable:** TIC. **Frecuencia:** mensual. **Objetivo:** limitar los ataques que se puedan presentar contra las plataformas del instituto. **Evidencia:** Panelaro del sistema operando.	5	4	20 - Zona Extrema
3	Daño en recursos tecnológicos.	Afectación de software y hardware parcial o total que apoyan la operación de los procesos.	1. Fallas eléctrica (UPS). 2. Corto circuito. 3. Condiciones naturales (Incendio)	* Afecta la ejecución de los procesos. * Costos adicionales por mantenimiento. * Perdida económica atribuible al costo de los recursos tecnológicos.	Riesgos tecnológicos	5	3	15 - Zona Extrema	1. **procedimiento:** alimentación eléctrica de los equipos por medio de la UPS. **Responsable:** Gestión de Infraestructura. **Frecuencia:** diaria. **Objetivo:** poder controlar el apagado de los equipos ante una falla eléctrica. **Evidencia:** el funcionamiento de UPS, el mantenimiento de la UPS. **2. No existe control.** (Red contra incendios) **3. Procedimiento:** Ubicación de extintores en los lugares asesorados por la ARL-Brigada de emergencia. **Objetivo:** Evitar daños por incendio. **Responsable:** Profesional Especializado, Profesional en Seguridad y Salud en el Trabajo. **Frecuencia:** Cada vez que pasa. **Evidencia:** Extintores.	5	3	15 - Zona Extrema
4	Interrupción en el servicio para los usuarios internos o externos.	Falla en la prestación de los servicios que ofrece el instituto de cara a la comunicación con los ciudadanos PQRSD (página web, telefonía).	1. Falla en los servidores. 2. Falla en bases de datos de SIFI.	* No acceso al servicio por parte de la ciudadanía. * Sanciones de tipo legal.	Riesgos cumplimiento	5	3	15 - Zona Extrema	1. **Pprocedimiento:** alimentación eléctrica de los equipos por medio de la UPS. **Responsable:** Gestión de Infraestructura. **Frecuencia:** diaria. **Objetivo:** poder controlar el apagado de los equipos ante una falla eléctrica. **Evidencia:** el funcionamiento de UPS, el mantenimiento de la UPS. 2. **Procedimiento:** Se realiza Backup de la base de datos de SIFI diariamente. **Responsable:** Equipo TIC. **Frecuencia:** Diaria. **Evidencia:** Almacenamiento en NAS y discos externos. **Objetivo:** Garantizar que en momento de daño o perdida de información se logre poner en marcha nuevamente el servicio de SIFI.	3	1	3 - Zona baja

8. Indicadores

La medición y monitoreo de este plan se realiza mediante el siguiente indicador el cual se describe a continuación:

- **CUMPLIMIENTO DEL PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN - MIPG:**

Objetivo: Realizar seguimiento al avance del plan de tratamiento de riesgos de seguridad y privacidad de la información - MIPG.

Fórmula de Cálculo indicador compuesto:

$$= \frac{\text{No. De actividades realizadas en el periodo}}{\text{No. de actividades programadas para el periodo}} * 100$$

Interpretación: A más actividades realizadas mayor el resultado del indicador.

Medición: Mensual

9. Registros

- Formato Matriz de Riesgo de Proceso.