Plan de Tratamiento de Riesgos Seguridad y Privacidad de la Información

2026

Instituto de Valorización de Manizales

INVAMA

Manizales, enero 2026

Versión 5.0

CONTENIDO

INDICE DE FIGURAS

1. INTRODUCCIÓN

El plan de tratamiento de riesgos de Seguridad y Privacidad de la Información - PTR, se basa en una orientación estratégica que requiere el desarrollo de una cultura de carácter preventivo, de manera que, al comprender el concepto de riesgo, así como el contexto, se planean acciones que reduzcan la afectación a la entidad en caso de materialización, adicional se busca desarrollar estrategias para la identificación, análisis, tratamiento, evaluación y monitoreo de dichos riesgos con mayor objetividad, dando a conocer aquellas situaciones que pueden comprometer la disponibilidad, integridad y confiabilidad de la información.

El Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información (PTR) se formula en cumplimiento del Decreto 612 de 2018, la Resolución MinTIC 500 de 2021, la Resolución 746 de 2022 y la Resolución 0227 de 2025, como instrumento complementario al Plan de Seguridad y Privacidad de la Información (PSPI). El PTR establece las acciones necesarias para tratar los riesgos identificados que puedan afectar la confidencialidad, integridad, disponibilidad y privacidad de la información de la Entidad, de conformidad con el Modelo de Seguridad y Privacidad de la Información (MSPI).

El PTR se articula directamente con el Plan de Seguridad y Privacidad de la Información (PSPI), el Modelo de Seguridad y Privacidad de la Información (MSPI) y el Modelo Integrado de Planeación y Gestión (MIPG), constituyéndose en un insumo clave para el diligenciamiento del FURAG.

2. OBJETIVOS

2.1 **Objetivo General**

Definir el enfoque, criterios y acciones para identificar, analizar, evaluar, tratar, aprobar, comunicar y hacer seguimiento a los riesgos de seguridad y privacidad de la información en la Entidad, con el fin de reducir su impacto y probabilidad, fortaleciendo la confianza digital y el cumplimiento normativo de la Entidad.

2.2 **Objetivos Específicos**

- 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 de los servicios a los que el Instituto de Valorización de Manizales pueda estar expuesto, y de esta manera alcanzar los objetivos, la misión y la visión institucional, protegiendo y preservando la integridad, confidencialidad, disponibilidad, privacidad y autenticidad de la información.

- Cumplir con los requisitos legales, reglamentarios, regulatorios y de las Normas Técnicas Colombianas.

- Gestionar los riesgos de Seguridad y Privacidad de la información, Seguridad Digital y Continuidad de la Operación de los servicios, de acuerdo con los contextos establecidos en la Entidad.

- Fortalecer y apropiar conocimiento referente a la gestión de riesgos de Seguridad y Privacidad de la información, Seguridad Digital y Continuidad de la Operación de los servicios del INVAMA.

3. ALCANCE

Aplica a todos los procesos, sistemas de información, activos de información, servicios digitales, funcionarios, contratistas y terceros que gestionen o tengan acceso a información institucional.

El Plan de Tratamiento de Riesgo tendrá en cuenta todos los riesgos en especial los que se encuentren en los niveles Moderado, Mayor y Catastrófico acorde con los lineamientos definidos por la Entidad, teniendo en cuenta que los riesgos que se encuentren en niveles inferiores serán aceptados por la Institución.

4. TÉRMINOS Y DEFINICIONES

Con el propósito de facilitar la comprensión de este documento se describen las siguientes definiciones:

- **Activo de Información:** Todo lo que tiene valor para el INVAMA y que contiene, genera, procesa, almacena y le da un tratamiento a la información o se relaciona con la misma. Existen diferentes tipos de activos como: Información (bases de datos, bases de conocimiento), tecnológicos o digitales (hardware y software), infraestructura física (instalaciones, oficinas), organizacionales (procesos, metodologías, servicios) y el recurso humano (Empleados de Planta, Contratistas, proveedores, Terceros).

- **Ciberseguridad**: Conjunto de actividades dirigidas a proteger el ciberespacio contra el uso indebido del mismo, defendiendo su infraestructura tecnológica, los servicios que prestan y la información que manejan.

- **Confidencialidad:** Atributo de la información que determina quién está autorizado a acceder a ella y previene su divulgación no autorizada dentro del INVAMA.

- **Contraseña Fuerte:** Contraseña que consta mínimo de nueve caracteres, mayúsculas, minúsculas, números y caracteres especiales.

- **Control:** las políticas, los procedimientos, las prácticas y las estructuras organizativas concebidas para mantener los riesgos de seguridad de la información por debajo del nivel de riesgo asumido. Control también es utilizado como sinónimo de salvaguarda o contramedida, es una medida que modifica el riesgo.

- **Copias de Seguridad:** Es el proceso mediante el cual se realiza la copia de la información existente, con el fin de poder recuperarla en caso de que ocurra un fallo que afecte a esta y pueda estar disponible.

- **Custodio de activo de información**: Parte designada de la organización, un cargo, proceso, o grupo de trabajo encargado de administrar, modificar, leer, procesar y hacer efectivos los controles de seguridad definidos, tales como copias de seguridad.

- **Disponibilidad:** Atributo de la información que determina para quién está disponible y los permisos de su uso dentro de las gestiones que adelante en el INVAMA.

- **Gestión de claves:** son controles que se realizan mediante la gestión de claves criptográficas.

- **Gestión de incidentes de seguridad de la información:** Son las acciones de control para garantizar la seguridad de los activos de información y su apropiada gestión, implementando las acciones para detectar, reportar, evaluar, responder, tratar y aprender de los incidentes de seguridad de la información en el INVAMA.

- **Gestión de riesgos:** Son las acciones que realiza el INVAMA para la identificación, análisis, evaluación, tratamiento, seguimiento y revisión del riesgo.

- **Impacto**: El costo para la organización de un incidente -de la escala que sea-, que puede o no ser medido en términos estrictamente financieros - p.ej., pérdida de reputación, implicaciones legales, etc. Consecuencia que sobre un activo tiene la materialización de una amenaza.

- **Incidente de seguridad de la información:** Evento único o serie de eventos de seguridad de la información inesperados o no deseados que compromete al INVAMA.

- **Información:** Es un activo de valor que hace parte de la Agencia Nacional Digital, por la cual asume funciones como responsable o encargada de la misma en cumplimiento de los requisitos legales, normativos e institucionales. La información corresponde a todo dato de la Entidad (tecnológico, administrativo, financiero, contable, entre otros), propio o de Terceros con las cuales dispone de un acuerdo o convenio; y datos personales de las cuales asume un rol como responsable o encargado.

- **Integridad:** Atributo de la información que protege los activos de información sobre posibles alteraciones, modificaciones no autorizadas formalmente por el INVAMA.

- **Inventario de activos:** lista de todos aquellos recursos (físicos, de información, software, documentos, servicios, intangibles, etc.) dentro del alcance del SGSI, que tengan valor para el INVAMA y necesiten por tanto ser protegidos de potenciales riesgos.

- **Plan de continuidad del negocio:** plan orientado a permitir la continuidad de las principales funciones misionales o del negocio en el caso de un evento imprevisto que las ponga en peligro.

- **Principios de Seguridad de la Información**: son características propias de la protección de la información: la Confidencialidad, Integridad y Disponibilidad.

- **Proceso:** conjunto de actividades interrelacionadas o interactuantes que transforman unas entradas en salidas.

- **Responsable de activo de información:** identifica a un individuo, un cargo, proceso o grupo de trabajo designado por la entidad, que tiene la responsabilidad de definir los controles, el desarrollo, el mantenimiento, el uso y la seguridad de los activos de información asignados.

- **Riesgo:** Es la probabilidad de que una amenaza o vulnerabilidad pueda ocasionar la pérdida y/o alteración de la información del INVAMA

- **Seguridad de la información:** preservación de la confidencialidad, integridad y disponibilidad de la información.

- **Sistema de Gestión de Seguridad de la Información (SGSI):** Es un conjunto de políticas de seguridad de la información que siguen la norma ISO/IEC 27001. Un SGSI es para una organización el diseño, implantación, mantenimiento de un conjunto de procesos para gestionar eficientemente la Accesibilidad de la información, buscando asegurar la confidencialidad, integridad y disponibilidad de los activos de información, minimizando a la vez los riesgos de seguridad de la información

- **Vulnerabilidad:** Es la debilidad o fallo del sistema que pone en riesgo la confidencialidad, integridad y disponibilidad de la información del INVAMA

- **Norma:** Principio que se dispone de carácter general, donde se establecen las obligaciones, restricciones y orientaciones para el acceso y uso de los activos de información.

- **Política:** Declaración de alto nivel que describe la posición del INVAMA sobre un tema específico.

- **Procedimiento:** Documento que define los pasos a seguir y que deben ser implementados en una situación dada.

5. MARCO NORMATIVO

- **ISO 27001.** Tecnologías de la Información. Técnicas de Seguridad. Sistemas de Gestión de Seguridad de la Información. Requisitos.

- **ISO 27002.** Tecnología de la Información. Técnicas de seguridad. Código de prácticas para los controles de seguridad de la información.

- **ISO 27005.** Gestión de Riesgos de Seguridad de la Información.

- **ISO 27017.** Código de buenas prácticas de seguridad servicios en la nube.

- **ISO 27018.** Código de práctica protección de información personal en nubes públicas.

- **ISO 27035.** Buenas prácticas de gestión de incidentes de seguridad de información.

- **ISO 22301.** Requisitos Sistema de Gestión de la Continuidad del Negocio.

- **ISO 31000.** Gestión del Riesgo – Directrices

- **Guía para la Administración del Riesgo y el Diseño de Controles en Entidades Públicas**. Guía de gestión de riesgos del DAFP.

- **Modelo de Gestión de Riesgos de Seguridad Digital (MGRSD)**

- **NIST framework Ciberseguridad**, es el marco que permite a las organizaciones comprender, gestionar y reducir los riesgos cibernéticos y proteger sus redes y datos, proporciona un lenguaje común y un resumen de las mejores prácticas en ciberseguridad.

- **Ley 1581 de 2012.** Protección datos personales. Circular 005 de 2017 SIC (Países Autorizados).

- **Ley 1712 de 2014.** Transparencia y del Derecho de Acceso a la Información Pública.

- **Ley 1273 de 2009.** Delitos informáticos

- **Ley 527 de 1999.** Acceso y uso mensajes de datos, comercio electrónico y firmas digitales.

- **Ley 23 de 1982**. Derechos de autor.

- **Ley 594 de 2000**. Ley general de archivo.

- **Decreto 2578 de 2012.** Reglamenta el Sistema Nacional de Archivos.

- **CONPES 3854 de 2016** – Política de Seguridad Digital del Estado Colombiano.

- **Decreto 612 de 2018.** Integración de los planes institucionales y estratégicos al Plan de Acción por parte de las entidades del Estado.

- **Decreto 620 de 2020**. Lineamientos generales en el uso y operación de los Servicios Ciudadanos Digitales.

- **Resolución 1519 de 2020.** Por la cual se definen los estándares y directrices para publicar la información señalada en la Ley 1712 del 2014 y se definen los requisitos materia de acceso a la información pública, accesibilidad web, seguridad digital, y datos abiertos.

- **CONPES 3995 de 2020.** Política Nacional de Confianza y Seguridad Digital

- **Resolución 500 de 2021.** Lineamientos y estándares para la estrategia de seguridad digital y se adopta el modelo de seguridad y privacidad como habilitador de la política de Gobierno Digital.

- **Decreto 338 de 2022.** Lineamientos generales para fortalecer la gobernanza de la seguridad digital

- **Resolución 746 de 2022.** Por la cual se fortalece el Modelo de Seguridad y Privacidad de la Información y se definen lineamientos adicionales a los establecidos en la Resolución número 500 de 2021.

- **Resolución MinTIC 0227 de 2025**. Por la cual se actualiza el Anexo 1 de la Resolución 500 de 2021 y se derogan otras disposiciones relacionadas con la materia

6. METODOLOGÍA DE GESTIÓN Y TRATAMIENTO DE RIESGOS

La metodología de gestión de identificación, evaluación y gestión de riesgos de seguridad y privacidad de la información del INVAMA, se basa en la NTC-ISO 27005 la NTC-ISO 31000, la Guía de Gestión del Riesgo del Departamento Administrativo de la Función Pública - DAFP. Su propósito es la identificación, estimación y evaluación de los riesgos de la Entidad para definir un plan de tratamiento que se ajuste a los objetivos de cada uno de los procesos.

El Modelo de Seguridad y Privacidad de la Información integra en cada una de sus fases tareas asociadas a la gestión de riesgos de seguridad de la información, ya que esta práctica constituye su base fundamental. La guía para la gestión del riesgo de función pública, llevarán a cumplir dichas tareas de gestión de riesgo de seguridad de la información requeridas en el MSPI.

En esencia, la interacción entre ambos modelos puede resumirse de la siguiente manera:

1. Las actividades de identificación de activos, identificación, análisis, evaluación y tratamiento de los riesgos se alinean con la fase de PLANIFICACIÓN del MSPI.
2. Las actividades de implementación de los planes de tratamiento de riesgos se alinean con la fase de IMPLEMENTACIÓN del MSPI.
3. Las actividades de monitoreo y revisión, revisión de los riesgos residuales, efectividad de los planes de tratamiento o los controles implementados y auditorías se alinean con la fase de EVALUACIÓN DEL DESEMPEÑO del MSPI.
4. Las actividades de MEJORAMIENTO CONTINUO en ambos modelos son similares y trabajan simultáneamente, ya que dependerán de las fases de Medición del Desempeño para identificar aspectos a mejorar en la aplicación de ambos Modelos.

A continuación, se ilustra en que acciones del MPSI se tendrá interacción directa con el Modelo de Gestión de Riesgos de Seguridad de la información.

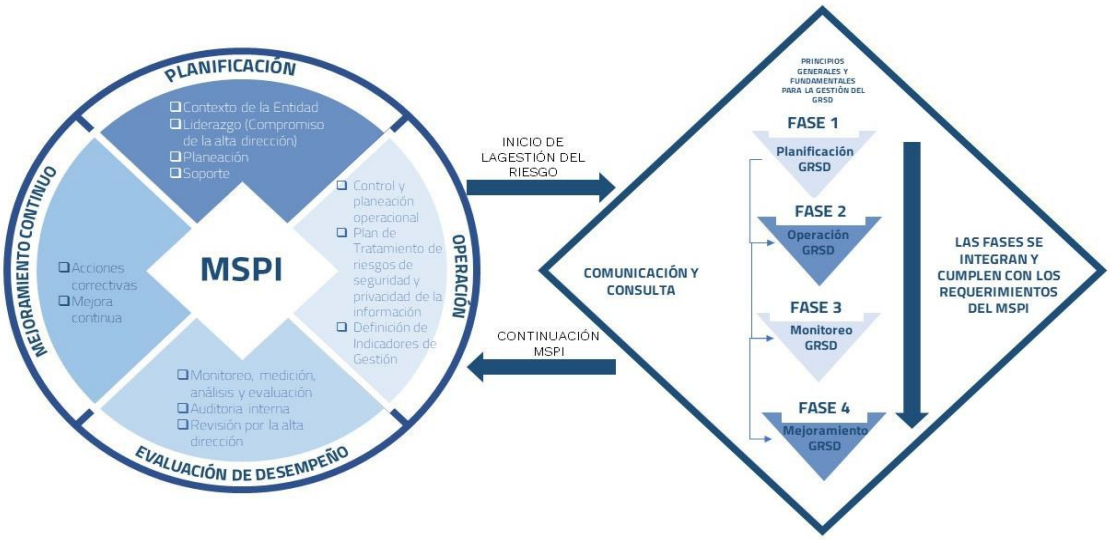

Figura 1. Interacción entre el MSPI y el MGRSD
Fuente: MINISTERIO DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES

Esta metodología se desarrolla en 8 pasos como se indica en la *figura 2.*

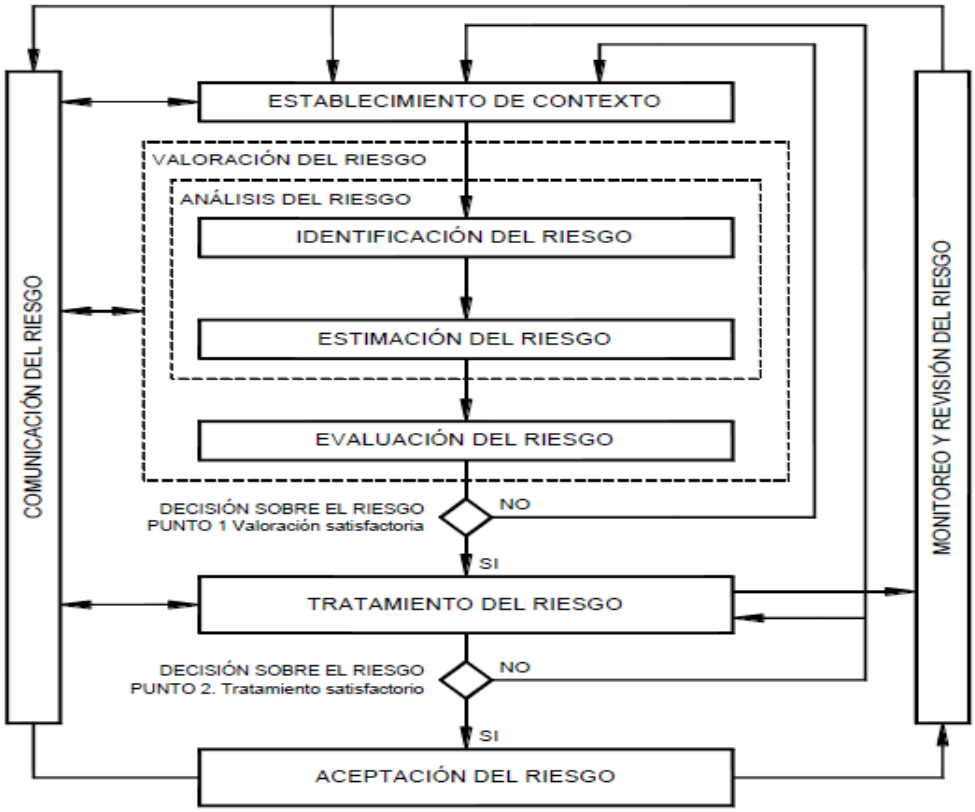

Figura 2. Proceso de Gestión de Riesgos de Seguridad de la Información
Fuente: MinTIC, "Guía de gestión de riesgos." 2016.

Los riesgos se analizan considerando el impacto y la probabilidad, y se clasifican según el nivel de riesgo residual aceptable definido por la Entidad y de acuerdo al ***MANUAL - LINEAMIENTOS DE ADMINISTRACIÓN DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN GT-SP-MA-02***

6.1 **Establecer Contexto**

El objetivo de esta etapa es determinar qué factores internos y externos pueden impactar a la institución, qué requiere protección y de acuerdo con los recursos actuales cómo podría darse esa protección, determinando los alcances y limitaciones existentes.

6.1.1 **Contexto Organizacional**

La identificación correcta del contexto organizacional es la base para identificar los riesgos y facilitar el análisis y la gestión de estos.

Se consideran los objetivos estratégicos, el Plan de Acción Institucional, el MIPG, la Política de Gobierno Digital y los procesos institucionales.

6.1.2 **Contexto Tecnológico**

Incluye la infraestructura tecnológica, sistemas de información, servicios en la nube, redes, plataformas digitales y activos tecnológicos.

6.1.3 **Contexto Normativo**

Incluye las obligaciones legales, regulatorias y contractuales relacionadas con seguridad de la información, privacidad y protección de datos personales.

6.1.4 **Apetito y Tolerancia del Riesgo**

El apetito del riesgo se define en esta etapa, dado que establece los criterios para evaluar y aceptar o no los riesgos.

La Entidad define cinco (5) niveles de riesgo: Leve, Menor, Moderado, Mayor y Catastrófico.

- **Leve y Menor:** Riesgos aceptados por la Entidad.
- **Moderado:** Riesgos tolerables con tratamiento.
- **Mayor y Catastrófico:** Riesgos no tolerables.

La Alta Dirección aprueba formalmente el apetito y la tolerancia al riesgo, los cuales sirven como marco para la evaluación y el tratamiento de los riesgos.

🔴 Riesgo Catastrófico

Corresponde a riesgos que pueden generar un impacto crítico sobre la continuidad del servicio, el cumplimiento de la misión institucional, la legalidad, la reputación de la Entidad o los derechos fundamentales de los titulares de la información.

Tolerancia:
🚫 NO TOLERABLE

Lineamientos de gestión:

- No se aceptará ningún riesgo clasificado en este nivel.
- Requiere atención inmediata y prioritaria.
- Debe ser reportado de forma inmediata a la Alta Dirección.
- Se debe definir e implementar un plan de tratamiento del riesgo en un plazo máximo de dos (2) meses.
- Cualquier excepción deberá ser aprobada expresamente por la Alta Dirección.

🟠 Riesgo Mayor

Riesgos que pueden afectar significativamente los objetivos estratégicos, la operación institucional o la seguridad y privacidad de la información, generando consecuencias relevantes a nivel operativo, legal o reputacional.

Tolerancia:
🚫 NO TOLERABLE

Lineamientos de gestión:

- Requiere la ejecución de acciones de tratamiento prioritarias a corto plazo.
- Debe ser informado a la Alta Dirección.
- El plan de tratamiento no deberá superar un plazo de seis (6) meses.
- Cualquier excepción deberá ser aprobada por la Alta Dirección.

🟡 Riesgo Moderado

Riesgos con impacto controlable que pueden afectar de manera parcial los procesos, servicios o activos de información, sin comprometer gravemente los objetivos institucionales.

Tolerancia:
⚠️ **TOLERABLE CON TRATAMIENTO**

Lineamientos de gestión:

- No se acepta de forma automática.
- Se deben administrar mediante procedimientos rutinarios.
- Se deberán fortalecer, mejorar o documentar controles existentes para reducir el nivel de riesgo.
- Su tratamiento será planificado y ejecutado conforme a la disponibilidad de recursos y prioridades institucionales.

🟢 Riesgo Menor

Riesgos con bajo impacto y baja probabilidad, cuyos efectos son limitados y fácilmente gestionables dentro de la operación normal de la Entidad.

Tolerancia:
✅ **TOLERABLE / ACEPTABLE**

Lineamientos de gestión:

- El riesgo es aceptado por la Entidad.
- Se gestiona mediante controles existentes y procedimientos rutinarios.
- No requiere acciones adicionales de tratamiento, salvo monitoreo periódico.

🔵 Riesgo Leve

Riesgos residuales mínimos, sin impacto significativo sobre los procesos, activos de información o el cumplimiento de los objetivos institucionales.

Tolerancia:
✅ **TOLERABLE / ACEPTABLE**

Lineamientos de gestión:

- El riesgo es aceptado formalmente por la Entidad.
- Se mantiene bajo observación y seguimiento.
- No requiere definición de planes de tratamiento específicos.

La Entidad declara que **acepta los riesgos clasificados en los niveles Leve y Menor**, en tanto se mantengan dentro de los parámetros establecidos y bajo monitoreo continuo.

Los riesgos clasificados como **Moderados** serán gestionados mediante controles y acciones de mejora, mientras que los riesgos **Mayores y Catastróficos** no serán aceptados y deberán ser tratados de manera prioritaria, con participación directa de la Alta Dirección.

6.2 **Identificación del Riesgo**

Se identifican los riesgos asociados a los activos de información, considerando amenazas, vulnerabilidades y consecuencias sobre la confidencialidad, integridad, disponibilidad y privacidad de la información.

Las fuentes de identificación incluyen:

- Inventario de activos de información ***GT-SP-FO-02 Inventario de activos de información***
- Resultados del autodiagnóstico MSPI ***MinTIC GT-SP-FO-01 Autodiagnóstico MSPI 27001_2022***
- Auditorías internas y externas
- Incidentes de seguridad ***GT-SP-FO-04 Reporte de Eventos Incidentes de Seguridad***
- Cambios tecnológicos u organizacionales

Las posibles vulnerabilidades de los activos de información y amenazas de seguridad se encuentran definidos en el ***MANUAL - LINEAMIENTOS DE ADMINISTRACIÓN DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN GT-SP-MA-02***.

Los riesgos se establecen en la ***MATRIZ DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN GT-SP-FO-03***.

6.3 **Análisis y Evaluación de Riesgos**

Se determina la probabilidad e impacto de cada riesgo identificado, considerando controles existentes.

Para la valoración de los riesgos se definieron criterios institucionales de impacto y probabilidad, considerando factores legales, operativos, reputacionales, financieros

y de continuidad del servicio; de acuerdo al ***MANUAL - LINEAMIENTOS DE ADMINISTRACIÓN DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN GT-SP-MA-02***.

6.4 **Tratamiento de Riesgos**

Para cada riesgo identificado se definen las acciones de tratamiento, responsables, plazos y controles asociados, priorizando aquellos riesgos con nivel **Mayor o Catastrófico.**

Para los riesgos no aceptables, la Entidad define una o más de las siguientes opciones:

- **Mitigar:** Esta estrategia busca, reducir la probabilidad de ocurrencia de un riesgo, reducir sus consecuencias, o lograr ambos objetivos a la vez. Un riesgo puede mitigarse a través de controles de gestión y procedimientos encaminados a reducir la frecuencia o el impacto generado. Se requiere plan de tratamiento.

- **Transferir:** Hace referencia a buscar respaldo y compartir con otro parte del riesgo. Se trasladan las posibles pérdidas por eventos de riesgo a otras empresas a través de arreglos contractuales, tercerización de procesos y seguros, con el fin de compartir el riesgo. Al transferir un riesgo no se transfiere las responsabilidades por lo que deberán ser constantemente monitoreadas para asegurarnos de su correcto tratamiento. Se requiere plan de tratamiento.

- **Evitar:** Determinación de la Entidad de finalizar o dar por terminada la actividad o procedimiento que exponía a la entidad a cierto riesgo que ya no se está dispuesto a tener. Normalmente se utiliza cuando la evaluación del riesgo es muy alta, o los costos para implementar los controles exceden los beneficios de su implementación. Se requiere plan de tratamiento.

- **Aceptar** (solo cuando aplique): Cuando se acepta un riesgo se asumen las consecuencias en el momento que se presenten. Toda aceptación del riesgo debe ser documentada y firmada por el Comité de Gestión y Desempeño Institucional indicando los criterios de esta decisión. Por último, deberán ser constantemente monitoreados en caso evolucionen y se conviertan en riesgos más graves. **Nota:** No puede haber aceptación de riesgos sobre situaciones que conlleven a incumplimientos normativos.

Cada riesgo tratado contará con:

- Acción de tratamiento
- Responsable
- Recursos
- Plazo
- Control asociado (ISO 27001 / MSPI)

El tratamiento de riesgos se articula directamente con la Declaración de Aplicabilidad (SOA), garantizando que los controles seleccionados respondan a los riesgos identificados.

6.5 **Declaración de Aplicabilidad (SOA)**

La Declaración de Aplicabilidad (Statement of Applicability – SOA) es el documento que consolida los controles de seguridad y privacidad de la información seleccionados por la Entidad, de acuerdo con los riesgos identificados y tratados.

La SOA:

- Identifica los controles del Anexo A de la ISO/IEC 27001:2022 y los controles del MSPI aplicables a la Entidad.
- Justifica la inclusión o exclusión de cada control.
- Evidencia la relación directa entre riesgos, planes de tratamiento y controles implementados.
- Constituye un insumo obligatorio para auditorías internas, externas y ejercicios de evaluación de madurez.

La SOA se mantiene como un documento controlado y actualizado, y forma parte integral del PTR, sin perjuicio de que se gestione como anexo independiente.

6.6 **Aprobación y Comunicación**

Los riesgos clasificados como **Moderados, Mayores y Catastróficos**, así como los planes de tratamiento, deben ser:

- Revisados por el Comité de Gestión y Desempeño Institucional
- Aprobados por la Alta Dirección cuando aplique.

El PTR será comunicado a los líderes de proceso y responsables de los activos de información.

6.7 **Seguimiento y Monitoreo**

La Entidad realizará seguimiento y monitoreo permanente al ciclo de gestión del riesgo, incluyendo:

- Cambios en el contexto organizacional, tecnológico y normativo.
- Evolución de los riesgos identificados.
- Cumplimiento y efectividad de los planes de tratamiento.
- Materialización de incidentes de seguridad y privacidad.

El monitoreo se realizará de manera continua y el seguimiento como mínimo de forma semestral, con reporte a la Alta Dirección y a las instancias de gobernanza de seguridad digital.

7. MAPA DE RUTA

El Plan de Tratamiento de Riesgos – PTR, contempla la definición de las actividades a desarrollar en aras de mitigar los riesgos sobre los activos

ACCIONES	RESPONSABLE	FECHA INICIO	FECHA FIN	RESULTADO
Socialización de la guía y herramienta de gestión de riesgos de seguridad y privacidad de la información, seguridad digital y continuidad de la operación.	-Responsable de Seguridad y Privacidad de la Información -Comunicaciones	01-Feb-2026	28-Feb-2026	Socialización
Identificación, análisis y evaluación de riesgos de seguridad y privacidad de la información, seguridad digital y continuidad de la operación.	-Responsable de Seguridad y Privacidad de la Información -Líderes de procesos	01-Feb-2026	30-Abr-2026	Matriz de Riesgos
Aceptación, aprobación riesgos identificados y planes de tratamiento	-Responsable de Seguridad y Privacidad de la Información -Comité MIPG	01-May-2026	30-May-2026	Actas de Reunión Matriz de Riesgos
Publicación y socialización matriz de riesgos	-Responsable de Seguridad y Privacidad de la Información -Comunicaciones	01-Jun-2026	30-Jun-2026	Link de Transparencia
Ejecución de controles y tratamientos	Responsables designados	01-Jun-2026	31-Dic-2026	Matriz de Riesgos
Seguimiento y monitoreo de riesgos	-Responsable de Seguridad y Privacidad de la Información	01-Jun-2026	31-Dic-2026	Matriz de Riesgos
Revisión por la Dirección	-Responsable de Seguridad y Privacidad de la Información -Alta Dirección -Comité MIPG	01-Ene-2027	31-Ene-2027	Actas de Reunión