PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN
2026

GOBERNACIÓN DE ANTIOQUIA
República de Colombia

Maria Cristina Giraldo Ospina
Directora de Tecnología e Información

Dirección de Tecnología e Información

2026

GOBERNACIÓN DE ANTIOQUIA
República de Colombia

TABLA DE CONTENIDO

1. INTRODUCCIÓN

La Gobernación de Antioquia, establece el Plan de Tratamiento de Riesgos de Seguridad de la información con el propósito de mitigar las amenazas que puedan afectar la Confidencialidad, Integridad, Disponibilidad y Privacidad de los activos de información de la Entidad.

Este plan contempla la implementación de acciones orientadas a reducir el impacto que podría generar la materialización de un riesgo, así como el desarrollo de estrategias para la identificación, análisis, tratamiento, evaluación y monitoreo continuo de dichos riesgos. Con ello se busca prevenir situaciones que comprometan el cumplimiento de los objetivos misionales de la Entidad.

Asimismo, el Plan se formula para definir y evaluar las medidas necesarias que permitan mitigar los riesgos existentes y aquellos que puedan surgir en el futuro, garantizando el cumplimiento de la normatividad vigente y de los requisitos establecidos por las partes interesadas en la gestión de la información.

2. DEFINICIONES[1]

Activos de Información:	En el contexto de seguridad digital son elementos tales como aplicaciones de la organización, servicios web, redes, Hardware, información física o digital, recurso humano, entre otros, que utiliza la organización para funcionar en el entorno digital.
Amenaza:	Causa potencial de un incidente no deseado, que puede resultar en daño a un sistema u organización.
Causa Inmediata:	Circunstancias bajo las cuales se presenta el riesgo, pero no constituyen la causa principal o base para que se presente el riesgo.
Causa Raíz:	Causa principal o básica, corresponde a las razones por la cuales se puede presentar el riesgo.
Confidencialidad:	Propiedad de la información que la hace no disponible o sea divulgada a individuos, entidades o procesos no autorizados.
Control:	Medida que mantiene y/o modifica un riesgo.
Consecuencia:	los efectos o situaciones resultantes de la materialización del riesgo que impactan en el proceso, la entidad, sus grupos de valor y demás partes interesadas. Resultado de un evento que afecta a los objetivos.
Disponibilidad:	Propiedad de ser accesible y utilizable a demanda por una entidad.
Evento de Seguridad de la Información:	Ocurrencia o cambio de un conjunto particular de circunstancias.
Incidente de seguridad de la Información:	Evento único o serie de eventos de seguridad de la información no deseados o inesperados que tienen una probabilidad significativa de comprometer las operaciones comerciales y amenazar la seguridad de la información.

[1] **Fuente de consulta:** https://www.normaiso27001.es/golsario-de-terminos-y-definiciones-iso-27000/
https://www.iso27000.es/glosario.html

Integridad:	Propiedad de exactitud y completitud.
Impacto:	El impacto en seguridad de la información es la consecuencia o efecto que tiene un incidente sobre los activos, procesos o servicios de una organización
Probabilidad:	Posibilidad de que algo suceda. Se entiende la posibilidad de ocurrencia del riesgo. Estará asociada a la exposición al riesgo del proceso o actividad que se esté analizando.
Riesgo:	Efecto que se causa sobre los objetivos de las entidades, debido a eventos potenciales.
Riesgo Inherente:	Nivel de riesgo propio de la actividad. El resultado de combinar la probabilidad con el impacto nos permite determinar el nivel del riesgo inherente, dentro de unas escalas de severidad.
Riesgo Residual:	El resultado de aplicar la efectividad de los controles al riesgo inherente.
Riesgo de Seguridad de la Información:	Posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información. Suele considerarse como una combinación de la probabilidad de un evento y sus consecuencias. (ISO/IEC 27000).
Vulnerabilidad:	Representan la debilidad de un activo o de un control que puede ser explotada por una o más amenazas.

3. OBJETIVO

Establecer y desarrollar un Plan de Tratamiento con el fin de gestionar los riesgos de Seguridad de la Información tomando como marco de referencia la metodología de riesgos de la Gobernación de Antioquia, con la finalidad de preservar la Confidencialidad, Integridad, Disponibilidad y Privacidad de los activos de información de la Entidad.

4. ALCANCE

Este plan se enfocará en la identificación, análisis, evaluación, tratamiento y seguimiento de riesgos asociados a los activos de información de la Gobernación de Antioquia.

5. MARCO DE REFERENCIA

Los procesos estratégicos, misionales, apoyo y evaluación de la Gobernación de Antioquia debe realizar seguimiento y gestión a los riesgos de Ciberseguridad.

El Plan de Tratamiento de Riesgos de Seguridad de la Información de la Gobernación de Antioquia tiene como objetivo mitigar los riesgos identificados sobre los activos de información mediante la implementación de las siguientes actividades:

ACTIVIDAD	TAREA	RESPONSABLE DE LA TAREA	RECURSOS	FECHAS PROGRAMADAS	
				FECHA INICIO	FECHA FIN
Identificación y valoración de riesgos de seguridad de la información con cada proceso de la Entidad.	Realizar mesas de trabajo para la identificación, análisis y evaluación de riesgos de Seguridad de la Información.	Dirección de Desarrollo Organizacional. Todos los Procesos de la Gobernación de Antioquia.	Recurso Humano Recurso Técnico Recursos Logísticos	2026	2026
	Aceptación y aprobación de la Matriz de Riesgos de Seguridad de la Información y su Plan de Tratamiento de Riesgos.	Dirección de Desarrollo Organizacional. Todos los Procesos de la Gobernación de Antioquia.	Recurso Humano Recursos Logísticos Recurso Financiero	2026	2026
	Publicación del Plan de Tratamiento de Riesgos de Seguridad de la Información.	Dirección de Desarrollo Organizacional.	Recurso Humano Recurso Tecnológico	2026	2026
Seguimiento al plan de tratamiento de riesgos de seguridad de la información.	Seguimiento al estado del Plan de tratamiento de Riesgos de Seguridad de la Información identificados y se deberá verificar las evidencias.	Dirección de Desarrollo Organizacional.	Recurso Humano Recurso Técnico Recursos Logísticos Recurso Financiero Recurso Tecnológico	2026	2026
	Evaluación de los Riesgos Residuales.	Dirección de Desarrollo Organizacional.	Recurso Humano Recurso Financiero	2026	2026

Tabla No.1 – Actividades del Plan de Tratamiento.

5.1. DESARROLLO DEL PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

Como primera medida, se debe tener en cuenta que la **"Política de Seguridad Digital"** vincula al **Modelo de Seguridad y Privacidad de la Información (MSPI)**[2], el cual se encuentra alineado con le Marco de Referencia de Arquitectura TI y soporta los habilitadores de la **"Política de Gobierno Digital"**.

El proceso de gestión de riesgos implica la aplicación sistemática de políticas, procedimientos y prácticas a las actividades de:

- Comunicación y consulta.
- Alcance, contexto, criterios.
- Evaluación de Riesgo.
- Tratamiento de riesgo.
- Seguimiento y revisión.

Como se ilustra en la siguiente **imagen No.1**.

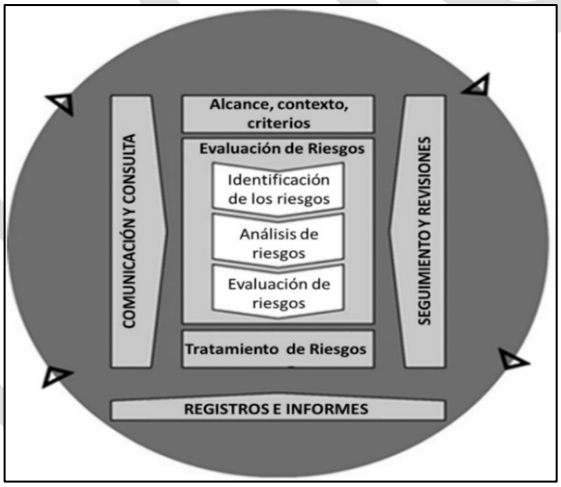

Imagen No.1 – Proceso de Administración y/o Gestión de Riesgo.

Este proceso de gestión de riesgos es una parte integral en la toma de decisiones la cual se debe integrar en la estructura de la operación y de los procesos de la Gobernación de Antioquia.

Razón por la cual la Entidad desarrolla una metodología de riesgos propia la cual sigue las directrices establecidas por el Departamento Administrativo de la Función Pública (DAFP)[3] y el Ministerio de Tecnología y las Comunicaciones (MinTIC) en materia de gestión de riesgos con el fin de promover la mejora continua de los procesos y los servicios prestados a la ciudadanía.

[2] **Fuente de información:** https://gobiernodigital.mintic.gov.co/seguridadyprivacidad/portal/Estrategias/MSPI/
[3] **Fuente de consulta:** https://www.funcionpublica.gov.co/documents/d/guest/2025-09-11_guia_gestion_integral_riesgo_v7?download=true

5.1.1. RIESGOS DE SEGURIDAD DE LA INFORMACIÓN

La **Gestión de Riesgos de Seguridad de la Información** constituye un pilar fundamental para garantizar la confianza de las partes interesadas en el uso seguro del entorno digital y en la protección de los activos de información de la Entidad. su propósito es identificar, evaluar y mitigar las amenazas que puedan comprometer la Confidencialidad, Integridad, Disponibilidad y Privacidad de la información.

Es este contexto, el **Modelo de Seguridad y Privacidad de la Información (MSPI)**, desarrollado por el Ministerio de Tecnologías de la Información y las Comunicaciones, se presenta como una herramienta estratégica que orienta a las organizaciones en el diseño, implementación, mantenimiento y mejora continua de un **Sistema de Gestión de Seguridad de la Información (SGSI)**. Dicho sistema se fundamenta en normas internacionales y en estándares de mejores prácticas, asegurando un enfoque sólido, actualizado y alineado con las exigencias del entorno digital contemporáneo.

A continuación, se desarrollan los pasos necesarios para la identificación y tratamiento de los riesgos asociados a la Disponibilidad, Integridad, Confidencialidad y Privacidad de los activos de información que permiten cumplir con la misión y alcanzar la Visión en las diferentes entidades.

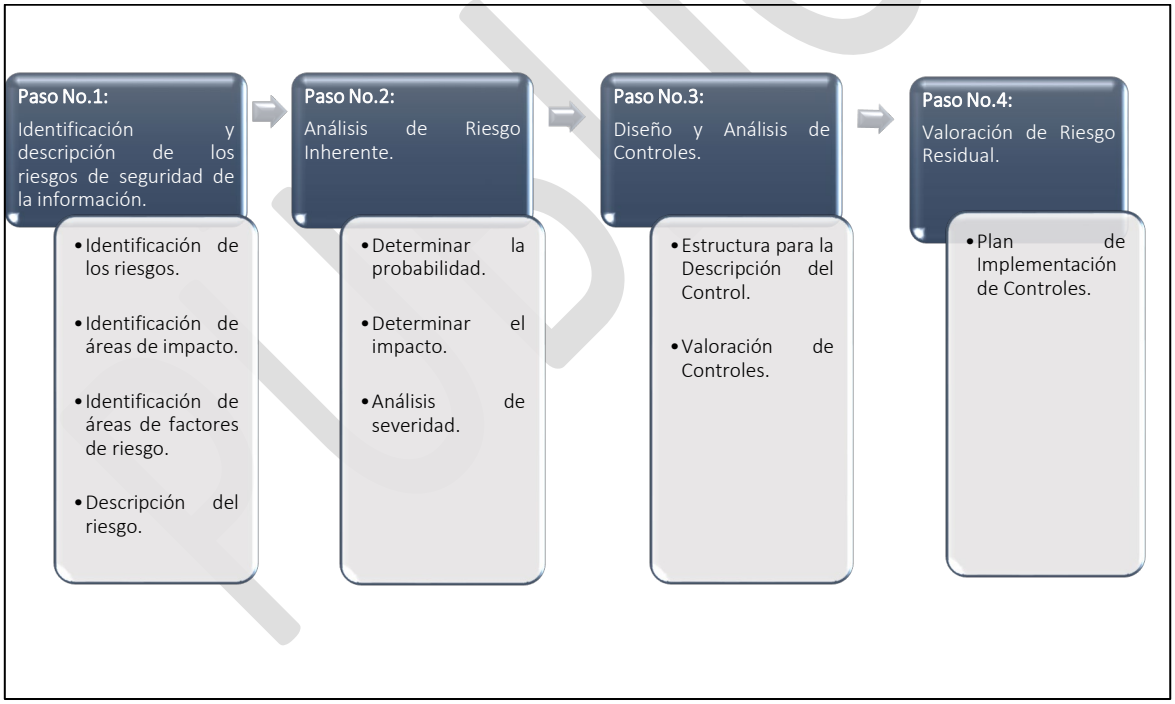

Imagen No.2 - Pasos para la identificación y tratamiento de los riesgos de los Activos de Información.

5.1.1.1. IDENTIFICACIÓN Y DESCRIPCIÓN DE LOS RIESGOS DE SEGURIDAD DE LA INFORMACIÓN.

a. Identificación de los Riesgos.

Como requisito previo, es indispensable contar con la **identificación de los Activos de Información** asociados a cada uno de los procesos de la Gobernación de Antioquia. Para ello, se debe aplicar el **Procedimiento de Inventario de Activos de Información** definido por la Entidad, el cual establece las directrices para su adecuada clasificación, registro y control.

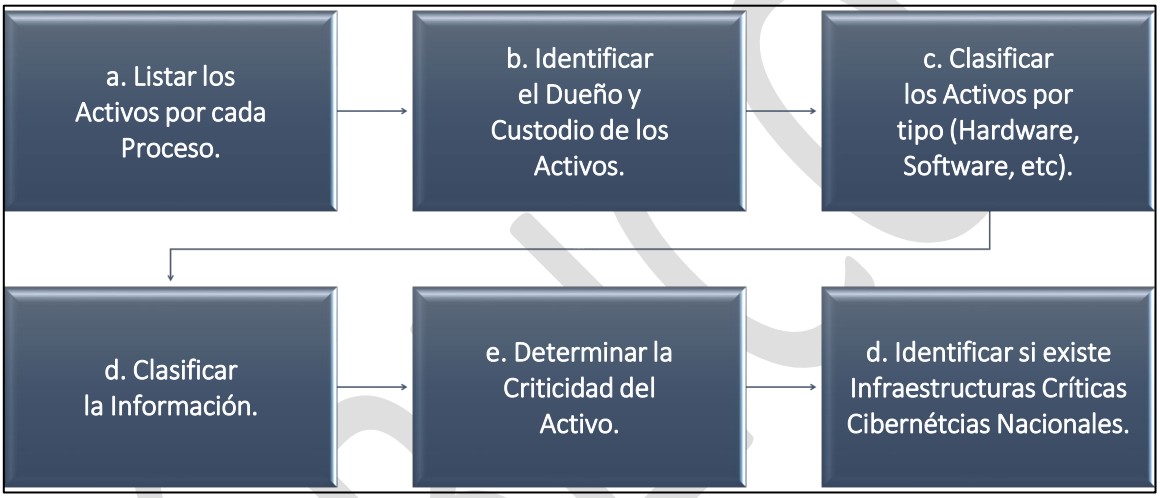

Imagen No.3 – Identificación y Valoración de los Activos de Información.

b. Identificación de Áreas de Impacto.

El **área de impacto** corresponde a las consecuencias negativas que puede sufrir la Gobernación de Antioquia si un riesgo llega a materializarse. También incluye los efectos que puedan generar los incidentes de seguridad de la información sobre el cumplimiento de los objetivos institucionales y sobre la gestión operativa de la Entidad.

c. Identificación de Áreas de Factores de Riesgo.

Corresponde a las fuentes que pueden generar riesgos dentro de la Entidad. para su adecuada gestión, es necesario identificar y definir las **amenazas** y las **vulnerabilidades** asociadas a cada activo de información del Proceso.

- **Amenaza:** Causa potencial de un incidente no deseado, que puede provocar daños a un sistema o a la Entidad, conforme a la definición establecida en la NTC-ISO/IEC 27001:2022. Estas amenazas pueden clasificarse por su origen en Deliberadas (D), Fortuitas (F) o Ambientales (A) así:

Deliberadas (D):	Acciones intencionales realizadas con el propósito de causar daño o afectar los activos de información.
Fortuitas (F):	Eventos no intencionales derivados de errores humanos, fallas técnicas o situaciones imprevistas.
Ambientales (A):	Situaciones externas relacionadas con el entorno físico o natural que pueden impactar la operación de la Entidad.

Tabla No.2 – Origen de Amenazas.

A continuación, se detallan las amenazas más comunes y su clasificación según su origen:

Tipo	*Amenaza*	*Origen*
Daño físico	Fuego	F, D, A
	Agua	F, D, A
	Contaminación	F, D, A
	Accidente Importante	F, D, A
	Destrucción del equipo o medios	F, D, A
	Polvo, corrosión, congelamiento	F, D, A
Eventos naturales	Fenómenos climáticos	A
	Fenómenos sísmicos	A
	Fenómenos volcánicos	A
	Fenómenos meteorológicos	A
	Inundación	A
Perdida de los servicios esenciales	Fallas en el sistema de suministro de agua o aire acondicionado	A
	Perdida de suministro de energía	A
	Falla en equipo de telecomunicaciones	D, F
Perturbación debida a la radiación	Radiación electromagnética	D, F
	Radiación térmica	D, F
	Impulsos electromagnéticos	D, F
Compromiso de la información	Interceptación de señales de interferencia comprometida	D
	Espionaje remoto	D
	Escucha encubierta	D
	Hurto de medios o documentos	D
	Hurto de equipo	D
	Recuperación de medios reciclados o desechados	D
	Divulgación	D, F
	Datos provenientes de fuentes no confiables	D, F
	Manipulación con hardware	D
	Manipulación con software	D
	Detección de la posición	D, F
Fallas técnicas	Fallas del equipo	F
	Mal funcionamiento del equipo	F
	Saturación del sistema de información	F
	Mal funcionamiento del software	F
	Incumplimiento en el mantenimiento del sistema de información.	F
Acciones no autorizadas	Uso no autorizado del equipo	D
	Copia fraudulenta del software	D
	Uso de software falso o copiado	D
	Corrupción de los datos	D
	Procesamiento ilegal de datos	D
Compromiso de las funciones	Error en el uso	D, F
	Abuso de derechos	D
	Falsificación de derechos	D
	Negación de acciones	D
	Incumplimiento en la disponibilidad del personal	D

Tabla No.3 - Amenazas Comunes.

- **Vulnerabilidad:** Debilidad de un activo o control que puede ser explotada por una o más amenazas, conforme a la definición establecida en la NTC-ISO/IEC 27001:2022.

Tipo	Vulnerabilidades
Hardware	Mantenimiento insuficiente
	Ausencia de esquemas de reemplazo periódico
	Sensibilidad a la radiación electromagnética
	Susceptibilidad a las variaciones de temperatura (o al polvo y suciedad)
	Almacenamiento sin protección
	Falta de cuidado en la disposición final
	Copia no controlada
Software	Ausencia o insuficiencia de pruebas de software
	Ausencia de terminación de sesión
	Ausencia de registros de auditoría
	Asignación errada de los derechos de acceso
	Interfaz de usuario compleja
	Ausencia de documentación
	Fechas incorrectas
	Ausencia de mecanismos de identificación y autenticación de usuarios
	Contraseñas sin protección
	Software nuevo o inmaduro
Red	Ausencia de pruebas de envío o recepción de mensajes
	Líneas de comunicación sin protección
	Conexión deficiente de cableado
	Tráfico sensible sin protección
	Punto único de falla
Personal	Ausencia del personal
	Entrenamiento insuficiente
	Falta de conciencia en seguridad
	Ausencia de políticas de uso aceptable
	Trabajo no supervisado de personal externo o de limpieza
Lugar	Uso inadecuado de los controles de acceso al edificio
	Areas susceptibles a inundación
	Red eléctrica inestable
	Ausencia de protección en puertas o ventanas
Organización	Ausencia de procedimiento de registro/retiro de usuarios
	Ausencia de proceso para supervisión de derechos de acceso
	Ausencia de control de los activos que se encuentran fuera de las instalaciones
	Ausencia de acuerdos de nivel de servicio (ANS o SLA)
	Ausencia de mecanismos de monitoreo para brechas en la seguridad
	Ausencia de procedimientos y/o de políticas en general (esto aplica para muchas actividades que la entidad no tenga documentadas y formalizadas como uso aceptable de activos, control de cambios, valoración de riesgos, escritorio y pantalla limpia entre otros)

Tabla No.4 - Vulnerabilidades Comunes.

a. Descripción del Riesgo.

Se identifican lo siguiente:

- **Tipo de Riesgo:** solo se admite uno de los tres (3) valores.

Imagen No.4 – Tipo de riesgos.

- **Descripción del Riesgo:** En este campo se expone la situación específica o el escenario que da origen al riesgo, indicando de manera clara cómo se manifiesta y por qué podría generar impactos negativos en la Entidad.

- **Clasificación del Riesgo:** Este campo corresponde al nombre que identifica la situación potencial que podría presentarse, es decir, el posible incidente de seguridad asociado al riesgo.

Tipo de Riesgo:	Descripción del Riesgo:	Clasificación del Riesgo:
Riesgo de la Pérdida de la Confidencialidad.	Existe la posibilidad de que personal no autorizado acceda a información sensible debido a controles de acceso insuficientes o configuraciones incorrectas, lo que podría comprometer datos institucionales.	Acceso no autorizado a información.

Tabla No.5 – Ejemplo de Descripción del Riesgo.

5.1.1.2. ANÁLISIS DEL RIESGO INHERENTE:

En esta etapa metodológica se aplican las tablas y matrices definidas por la Entidad, las cuales permiten evaluar los riesgos generales de la gestión antes de considerar cualquier control existente. Este análisis facilita comprender el nivel real de exposición al riesgo y establecer prioridades para su tratamiento.

a. Determinar la Probabilidad.

En esta actividad se analiza la **posibilidad de que el riesgo se materialice**, evaluando la frecuencia o recurrencia con la que podría ocurrir el evento no deseado según las condiciones actuales de la Entidad.

- **Frecuencia:** Corresponde al número de horas al año durante las cuales se ejecuta la actividad asociada al riesgo. Este valor permite estimar la exposición temporal al evento riesgoso.

- **% de Probabilidad Inherente (Cuantitativo):** Indica el porcentaje anual que representa la realización de la actividad que genera el riesgo, medido mediante una escala cuantitativa.

- **Probabilidad Inherente (Cualitativo):** Hace referencia al número de veces al año en que se lleva a cabo la actividad que puede originar el riesgo, evaluado mediante una escala cualitativa.

Probabilidad	Frecuencia de la Actividad
Muy Baja – 20%	La actividad que conlleva el riesgo se ejecuta como máximos 2 veces por año
Baja – 40%	La actividad que conlleva el riesgo se ejecuta de 3 a 24 veces por año
Media – 60%	La actividad que conlleva el riesgo se ejecuta de 25 a 500 veces por año
Alta .80%	La actividad que conlleva el riesgo se ejecuta más de 500 veces al año y máximo 5000 veces por año
Muy Alta – 100%	La actividad que conlleva el riesgo se ejecuta más de 5000 veces por año

Imagen No.5 - Tabla de Probabilidad.

b. Determinar el impacto.

En esta actividad se evalúan las **consecuencias que tendría la materialización del riesgo**, analizando el grado de afectación que podría generar sobre los procesos, los activos de información y los objetivos institucionales de la Entidad.

- **% de Impacto Inherente (Cuantitativo):** Corresponde a la medida porcentual del impacto económico o reputacional que podría generar la materialización del riesgo sobre la Entidad, evaluado mediante una escala cuantitativa.

- **Impacto Inherente (Cualitativo):** Hace referencia a la valoración cualitativa del impacto económico o reputacional que el riesgo podría ocasionar en la Entidad, utilizando una escala descriptiva para determinar su nivel.

Nivel de Impacto	Afectación Económica	Afectación Reputacional
Leve-20%	Afectación menor a 10 SMLMV	El riesgo afecta la imagen de algún área de la entidad.
Menor-40%	Mayor a 10 SMLMV y Menor a 50 SMLMV	El riesgo afecta la imagen de la entidad a nivel interno, de conocimiento general, de junta directiva y accionistas y/o de proveedores.
Moderado-60%	Mayor a 50 SMLMV y Menor a 100 SMLMV	El riesgo afecta la imagen de la entidad con algunos usuarios de relevancia frente al logro de los objetivos.
Mayor-80%	Mayor a 100 SMLMV y Menor a 500 SMLMV	El riesgo afecta la imagen de la entidad con efecto publicitario sostenido a nivel de sector administrativo, nivel departamental o municipal.
Catastrófico-100%	Mayor a 500 SMLMV	El riesgo afecta la imagen de la entidad a nivel nacional, con efecto publicitario sostenido a nivel país

Imagen No.6 - Tabla de Impacto.

c. Análisis de Severidad.

Zona de Riesgo Inherente: En este campo se identifica la zona de severidad dentro de la matriz de calor en la que se ubica el riesgo, de acuerdo con la combinación de su **probabilidad** y su **impacto**. Esta clasificación permite visualizar el nivel de exposición antes de aplicar controles.

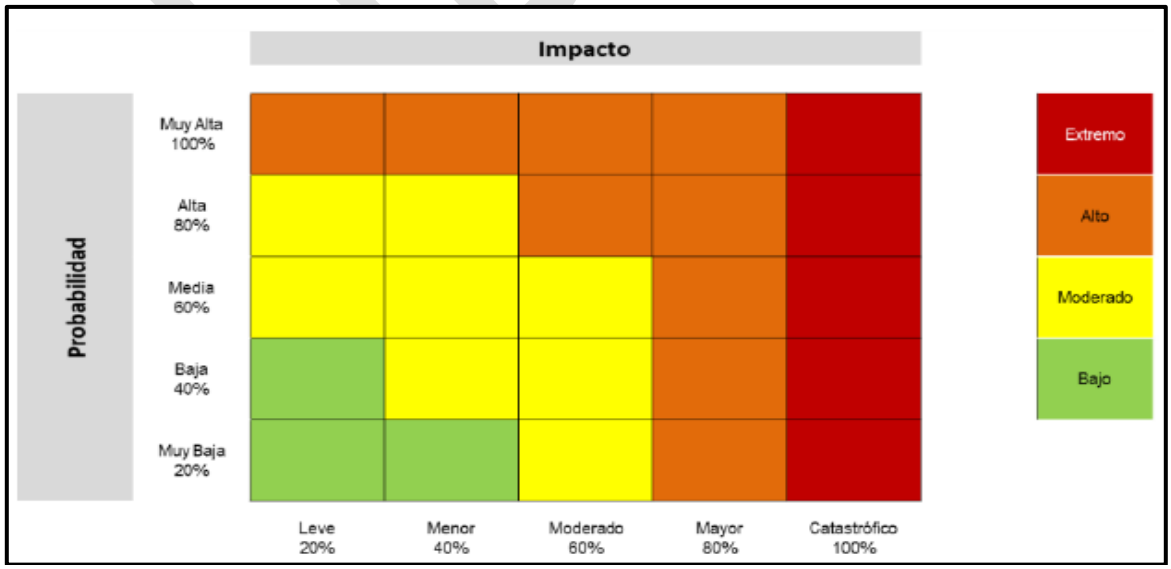

Imagen No.7 – Nivel del Riesgo (Zona de Severidad.

5.1.1.3. DISEÑO Y ANÁLISIS DE CONTROLES

En esta fase se definen, seleccionan y analizan los **controles necesarios para mitigar los riesgos identificados**, asegurando su alineación con los requisitos del Sistema de Gestión de Seguridad de la Información y con los lineamientos establecidos en la ISO/IEC 27001:2022.

El proceso incluye evaluar la pertinencia, efectividad y alcance de cada control, así como su capacidad para reducir la probabilidad o el impacto del riesgo. De esta manera, se garantiza que los controles propuestos sean adecuados, proporcionales y coherentes con las necesidades de la Entidad y con el nivel de protección requerido para los activos de información.

a. Estructura para la Descripción del Control.

En esta actividad se seleccionan los controles que se implementaran para mitigar los riesgos identificados. La selección se realiza con base a los lineamientos y controles definidos **NTC-ISO/IEC 27001:2022**, garantizando su alineación con los requisitos del Sistema de Gestión de Seguridad de la Información (SGSI).

No. Control	Control Anexo A	Descripción del Control
Consecutivo de los controles a establecer.	Seleccionar uno o varios de los 93 controles del Anexo A que le apliquen al riesgo identificado: **Dominio Organizacionales.** A.5.1 al A.5.37 **Dominio de Personas.** A.6.1 al A.6.8 **Dominio Físico.** A.7.1 al A.7.14 **Dominio Tecnológico.** A.8.1 al A.8.34	La descripción de cada control debe evidenciar de manera clara cómo contribuye a disminuir la probabilidad o el impacto del riesgo, así como su pertinencia frente a las necesidades de protección de los activos de información de la Entidad.

Tabla No.6 – Selección de Controles para Mitigar Riesgo.

b. Valoración del Control.

La implementación del control modifica la Probabilidad o el Impacto del riesgo, evaluando el grado en que dicho control contribuye a disminuir la exposición de la Entidad frente al riesgo identificado.

- **Afectación:** En esta actividad se establece la afectación que tendrá la implementación del control sobre la Probabilidad o el Impacto del riesgo.

- **Probabilidad:** En este campo se especifica si el control pretende modificar la probabilidad de ocurrencia de riesgo.

- **Impacto:** En este campo se especifica si el control pretende modificar el impacto de ocurrencia de riesgo.

- **Atributos:** En esta actividad se establecen los Atributos de la implementación del control, donde se consideran atributos de eficiencia y los de formalización del control.

Características de Eficiencia		Peso
Tipo	Preventivo	25%
	Detectivo	15%
	Correctivo	10%
*Implementación *Nota: En implementación no se tienen controles semiautomáticos.	Automático	25%
	Manual	15%

Características de Eficiencia		Descripción
Documentación	Procedimientos	Basados en la estructura del Modelo de Operación por procesos, despliegue desde cada proceso, sus procedimientos y esquemas asociados, que se encuentren documentados.
	Sistemas de información	Sistemas de información de apoyo a la ejecución del control (si existen).
	Otros Esquemas	Políticas de operación, manuales o guías específicas.
Frecuencia	Siempre que se ejecuta la actividad	La oportunidad en que se ejecuta el control debe ayudar a prevenir la mitigación del riesgo o a detectar la materialización del riesgo de manera oportuna.
	Periódicamente (diario, mensual, bimestral, trimestral, semestral).	
Evidencia (Trazabilidad de la ejecución)	Con registro manual	Se deja evidencia o rastro de la ejecución del control.
	Con registro electrónico	
Ejecución (Fuentes de información internas o externas)	Interna	Formatos o registros internos formales.
	Externa	Registros externos confiables (extractos bancarios, confirmaciones de autenticidad de documentos, SECOP, SIIF, SIGEP, bases de datos).
	Mixta	Combinación de datos de fuentes internas y externas formales.

ATRIBUTOS							
Tipo	%	Implementación	%	Calificación del control	Documentación	Frecuencia	Evidencia

Tabla No.7 – Valoración de los Atributos.

5.1.1.4. VALORACIÓN DEL RIESGO RESIDUAL

En esta etapa se evalúa la **efectividad de los controles aplicados**, con el propósito de determinar el **riesgo residual**. Este análisis permite identificar el nivel de exposición que persiste después de implementar los controles y establecer si es necesario fortalecer las medidas existentes o adoptar nuevas acciones de mitigación.

a. Plan de Implementación de Controles.

En esta actividad se define el plan para la puesta en marcha de los controles seleccionados, estableciendo las acciones necesarias, los responsables, los plazos y los recursos requeridos. Este plan permite organizar la ejecución de los controles y facilita su seguimiento y verificación, asegurando que contribuyan efectivamente a la mitigación de los riesgos identificados.

- **Tratamiento:** En este campo se especifica el tipo de tratamiento que se realizará entre cuatro (4) opciones disponibles:

Reducir:	Implementar controles para reducir la probabilidad o el impacto.
Compartir:	Compartir las consecuencias de la materialización del riesgo, por ejemplo, a través de la adquisición de una ciberpoliza.
Aceptar:	Cuando el nivel del riesgo está por debajo del apetito establecido por la alta dirección.
Evitar:	Cuando se decide eliminar el activo que es fuente del riesgo: por ejemplo, dar de baja un servidor.

Tabla No.8 – Tipo de Tratamiento.

- **Plan de Acción:** En este campo se especifica la identificación del Plan de acción con el cual se realizará la implementación de dicho control.
- **Responsable:** En este campo se especifica el cargo de quien implementa el control.
- **Fecha de Implementación:** En este campo se especifica la Fecha máxima de implementación del control.
- **Seguimiento:** En este campo se especifica la periodicidad del seguimiento a la implementación del control.
- **Estado:** En este campo se especifica el estado de la implementación del control.

5.1.2. SEGUIMIENTO Y REVISIÓN

La Gobernación de Antioquia, debe asegurar el cumplimiento de sus objetivos institucionales anticipándose a los eventos que puedan afectar su gestión.

En este propósito, el Modelo Integrado de Planeación y Gestión (MIPG), a través de sus componentes de Seguimiento, Monitoreo y Revisión, y en articulación con el Esquema de Líneas del Modelo Estándar de Control Interno (MECI), constituye un marco fundamental para la gestión del riesgo de la Entidad.

De acuerdo con lo señalado en el Capítulo II, donde se desarrolla la alineación estratégica entre la gestión del riesgo y el MIPG, la **Dimensión 7** despliega los componentes de evaluación del riesgo y las actividades de control, integrándolos con el esquema de líneas.

Este enfoque permite atender de manera integral la gestión del riesgo dentro de la Entidad, involucrando a todos los niveles organizacionales y definiendo con claridad los niveles de autoridad y responsabilidad en la aplicación de controles. Dichos controles se convierten en el eje para materializar el seguimiento y monitoreo de los riesgos que enfrenta la Gobernación de Antioquia.

En este contexto, resulta indispensable establecer **mecanismos adecuados para la medición del riesgo**, que permitan determinar la efectividad de los controles implementados y fortalecer la capacidad institucional para prevenir, mitigar y responder a los eventos adversos.

5.1.3. RECURSOS

En el marco de la gestión de riesgos de seguridad y privacidad de la información se debe establecer los siguientes recursos para abordar la gestión:

Definición	Recursos
Humanos	La Dirección de Desarrollo Organizacional serán los responsables de: • Coordinar, implementar, modificar y realizar seguimiento a las políticas, estrategias y procedimientos para la identificación de los riesgos de la Entidad.
Técnicos	Se basa en los instrumentos definidos como: • Guía para la administración de riesgos. • Instrumento para la gestión de riesgos (Matriz de riesgos SGSI). • Guía para la administración del riesgo y el diseño de controles en Entidades públicas. • Manual Operativo del Modelo Integrado de Planeación y Gestión – Política de Seguridad Digital y Política de Gobierno Digital.
Logísticos	Gestión de recursos para realizar socializaciones, transferencia de conocimientos y seguimiento a la gestión de riesgos.
Financieros	Para las actividades de logística, recursos humanos, técnicos, tecnológicos, entre otros.
Tecnológicos	Se basa en contar con las herramientas tanto de hardware como software para la aplicación de controles tecnológicos que se requieran para mitigar los riesgos.

Tabla No.9 – Recursos.

TABLAS

IMÁGENES