# PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN EN LA INSTITUCIÓN UNIVERSITARIA COLEGIO MAYOR DE ANTIOQUIA.

**2026**

**TECNOLOGÍA Y MEDIOS AUDIOVISUALES.**

## 1. INTRODUCCIÓN

La Institución Universitaria Colegio Mayor de Antioquia adopta un enfoque metódico para optimizar la identificación, análisis, evaluación, tratamiento y monitoreo de los riesgos vinculados a la gestión de la información institucional. Esta estrategia busca prevenir y mitigar riesgos derivados del uso de Tecnologías de la Información y la Comunicación (TIC) en las actividades cotidianas, evitando vulneraciones que podrían acarrear problemas legales, económicos y administrativos. Este documento define el marco de trabajo para asegurar la protección de las bases de datos institucionales.

## 2. ÁMBITO DE APLICACIÓN

El presente plan tiene una vigencia para el periodo 2025-2027 y aplica de manera integral a todos los procesos definidos en el Mapa de Procesos Institucionales.

## 3. OBJETIVOS DEL PLAN

### *3.1 Objetivo General*

Desarrollar el marco estratégico y operativo para la gestión proactiva de los riesgos de seguridad y privacidad de la información, conforme a la guía metodológica del DAFP, la Ley 1581 de 2012 y los lineamientos vigentes de MINTIC.

### *3.2 Objetivos específicos*

- **Diagnóstico:** Realizar un diagnóstico certero sobre la situación actual de la Institución frente a los riesgos de seguridad y privacidad.
- **Metodología:** Aplicar las mejores prácticas definidas por el DAFP y MINTIC (Modelo de Seguridad y Privacidad - MSPI) para una gestión eficaz.
- **Integración Institucional:** Colaborar en la solidificación del modelo integral de planeación y gestión (MIPG) dentro de las políticas de Gobierno Digital y Seguridad Digital.
- **Cultura de Seguridad:** Ejecutar programas de sensibilización anuales dirigidos a toda la comunidad universitaria sobre la protección de datos y ciberseguridad.
- **Monitoreo:** Evaluar semestralmente la eficacia de los controles implementados y actualizar el mapa de riesgos institucional ante nuevas amenazas.

## 4. RECURSOS Y RESPONSABLES

### 4.1 Recursos

| Categoría de Recurso | Tipo | Descripción y Aplicación Específica | Responsable de Gestión |
|---|---|---|---|
| **Talento Humano** | Estratégico | **CISO / Oficial de Seguridad:** Líder encargado de la gobernanza y articulación del MSPI. | Rectoría / Planeación |
| **Talento Humano** | Técnico | **Equipo de TI:** Administradores de red y servidores encargados de los controles técnicos. | Oficina de TIC |
| **Talento Humano** | Control | **Auditores Internos:** Personal capacitado en ISO 27001 para la verificación de controles. | Control interno |

| | | | |
|---|---|---|---|
| **Tecnológicos** | Hardware | **Infraestructura de Red:** Firewalls, servidores de respaldo, sistemas de detección de intrusos (IDS). | Oficina de TIC |
| **Tecnológicos** | Software | **Herramientas de Seguridad:** Antivirus corporativo, software de cifrado, gestores de vulnerabilidades. | Oficina de TIC |
| **Tecnológicos** | Servicios | **Certificados SSL y Firmas Digitales:** Para garantizar la integridad y autenticidad de los datos. | Oficina de TIC |
| **Financieros** | Inversión | **Presupuesto para Ciberseguridad:** Rubros destinados a la actualización de licencias y renovación tecnológica. | Suboficial Administrativa |
| **Financieros** | Gastado | **Pólizas de Ciber riesgo:** Recursos para la transferencia del riesgo mediante seguros especializados. | Suboficial Administrativa |
| **Información** | Regulador | **Suscripción a bases legales:** Acceso a actualizaciones sobre Ley 1581, Decretos de MINTIC y estándares ISO. | Secretaría General |
| **Información** | Metodológico | **Guías del DAFP y MINTIC:** Documentación técnica para la evaluación de riesgos en entidades públicas. | Oficina de Planeación |

*4.2 Responsabilidades Clave*

**A. Alta Dirección (Rectoría y Consejo Directivo)**

Como máximos responsables de la gestión institucional, sus funciones en materia de seguridad son:

- **Aprobación Estratégica:** Sancionar la Política de Seguridad y Privacidad de la Información y el Plan de Tratamiento de Riesgos.
- **Asignación de Recursos:** Garantizar la suficiencia presupuestal, técnica y humana para la implementación de los controles definidos.
- **Liderazgo y Compromiso:** Promover una cultura organizacional donde la seguridad de la información sea una prioridad en todos los niveles académicos y administrativos.
- **Revisión por la Dirección:** Evaluar anualmente los resultados de la gestión de riesgos para tomar decisiones de mejora de alto nivel.

**B. Comité Institucional de Gestión y Desempeño**.
Actúa como el órgano de gobernanza de la seguridad de la información (según Res. 087 de 2018):

- **Priorización de Riesgos:** Validar la priorización de los riesgos detectados y aprobar las acciones de tratamiento propuestas.
- **Articulación Institucional:** Asegurar que los riesgos de seguridad se integren de manera coherente en el Mapa de Riesgos Institucional.
- **-Seguimiento:** Monitorear el avance del Plan de Tratamiento de Riesgos y los indicadores de eficacia de los controles.

**C. Líder de Seguridad y Privacidad de la Información (CISO)**
Es el articulador técnico y estratégico del modelo:

- **Gestión Metodológica:** Dirigir el proceso de identificación, análisis y valoración de riesgos bajo la metodología GT-MA-004.
- **Asesoría Técnica:** Brindar lineamientos a los líderes de proceso sobre cómo implementar controles de seguridad.
- **Gestión de Incidentes:** Coordinar la respuesta ante eventos que vulneren la seguridad o la privacidad de los datos.
- **Capacitación:** Diseñar y liderar el programa anual de sensibilización en seguridad digital y Habeas Data.

**D. Oficina de Tecnologías de la Información (OTI) / Soporte Técnico**
Responsables de la capa técnica de protección:

- **Implementación Tecnológica:** Desplegar y mantener firewalls, sistemas de respaldo (backups), cifrado de datos y software antivirus.
- **Monitoreo de Infraestructura:** Identificar vulnerabilidades técnicas en servidores, redes y bases de datos.
- **-Gestión de Accesos:** Administrar las identidades y privilegios de usuario, asegurando que cada persona acceda solo a lo necesario para su función.

**E. Líderes de Proceso (Decanos, directores y jefes de Oficina)**
Cada líder es el "dueño" de la información de su área:

- **Identificación de Activos:** Mantener actualizado el inventario de activos de información de su dependencia (bases de datos de estudiantes, registros contables, etc.).
- **Ejecución de Controles:** Asegurar que los funcionarios y contratistas bajo su mando cumplan con las políticas de escritorio limpio, cambio de contraseñas y manejo de documentos.
- **Reporte Proactivo:** Informar de manera inmediata cualquier sospecha de fuga de información o anomalía en sus procesos.

**F. Oficina de Control Interno**
Responsable de la tercera línea de defensa:

- **Auditoría y Verificación:** Evaluar de manera independiente si los controles definidos en el plan se están aplicando realmente.
- **Validación de Cumplimiento:** Verificar la alineación con la Ley 1581 de 2012 y los estándares de MINTIC.
- **-Recomendaciones de Mejora:** Sugerir ajustes al plan basados en los hallazgos de las auditorías de gestión.

**G. Servidores Públicos, Docentes y Contratistas**
Es la responsabilidad transversal de toda la comunidad:

- **Cumplimiento Normativo:** Acatar las políticas de tratamiento de datos personales y seguridad digital.
- **Reserva de Información:** Mantener la confidencialidad de la información a la que tengan acceso por razón de sus funciones.
- **Uso Responsable de Activos:** Cuidar los equipos de cómputo y herramientas digitales suministradas por la Institución.

## 5. MARCO REGULATORIO ACTUAL

El presente Plan de Tratamiento de Riesgos se rige por una jerarquía normativa que abarca desde la Constitución Nacional hasta los actos administrativos internos de la Institución:

| Nivel Normativo | Referencia | Nombre / Tema | Aplicación Específica al Plan |
|---|---|---|---|
| **Constitucional** | **Artículo 15** | Derecho al Habeas Data | Protege el derecho de la comunidad universitaria a conocer, actualizar y rectificar su información en bases de datos. |
| **Constitucional** | **Artículo 74** | Acceso a Documentos Públicos | Define que la información es pública salvo reserva legal (seguridad nacional o datos sensibles). |
| **Ley Nacional** | **Ley 1581 de 2012** | Ley General de Protección de Datos Personales | Establece las obligaciones de la Institución como "responsable del Tratamiento" de datos de estudiantes y docentes. |
| **Ley Nacional** | **Ley 1712 de 2014** | Ley de Transparencia y Acceso a la Información | Obliga a proteger la información reservada y clasificada frente a riesgos de fuga. |
| **Ley Nacional** | **Ley 1273 de 2009** | Ley de Delitos Informáticos | Define las conductas punibles como el acceso abusivo a sistemas o la interceptación de datos. |
| **Decreto Único** | **Decreto 1078 de 2015** | Decreto Único Reglamentario del Sector TIC | Reglamenta el sector y establece las bases para la gestión de activos de información en entidades públicas. |
| **Decreto Nacional** | **Decreto 767 de 2022** | Política de Gobierno Digital | Define los lineamientos para la seguridad digital y el aprovechamiento de datos en la administración pública. |
| **Resolución MINTIC** | **Resolución 500 de 2021** | Estándares del MSPI | Dicta los lineamientos técnicos que el Colmayor debe seguir para el Modelo de Seguridad y Privacidad de la Información. |
| **Estándar Técnico** | **ISO/IEC 27001:2022** | Sistemas de Gestión de Seguridad de la Información | Norma internacional utilizada como referencia para la selección de controles de este plan. |

| | | | |
|---|---|---|---|
| **Estándar Técnico** | **ISO 31000:2018** | Gestión del Riesgo – Directrices | Marco metodológico para la identificación y valoración de riesgos institucionales. |
| **Institucional** | **Resolución 087 de 2018** | Comité de Gestión y Desempeño | Asigna la autoridad para la aprobación y seguimiento de este plan de riesgos. |
| **Institucional** | **Acuerdo 014 de 2023** | Política de Gestión Integrada | Declara el compromiso de la rectoría con la protección de la información institucional. |

## 6. METODOLOGÍA DE GESTIÓN DEL RIESGO

La Institución adopta el ciclo de mejora continua para la seguridad digital, estructurado en las siguientes fases técnicas:

### 6.1. Establecimiento del Contexto

Antes de identificar riesgos, se deben definir los parámetros:

- **Contexto Externo:** Amenazas cibernéticas globales, requisitos legales (MINTIC, Ley 1581) y entorno social.
- **Contexto Interno:** Infraestructura tecnológica del Colmayor (servidores, redes Wifi, plataformas académicas), cultura organizacional y procesos administrativos.

### 6.2. Identificación de Riesgos (El Inventario de Amenazas)

No se puede proteger lo que no se conoce. En esta fase se identifican:

1. **Activos de Información:** Datos de estudiantes, registros financieros, propiedad intelectual docente, etc.
2. **Amenazas:** Eventos que pueden causar daño (ej. ataques de phishing, fallos de hardware, incendios, errores humanos).
3. **Vulnerabilidades:** Debilidades que la amenaza puede explotar (ej. software sin actualizar, falta de backups, ausencia de capacitación).

### 6.3. Análisis de Riesgos (Cálculo del Nivel de Exposición)

Se utiliza la escala institucional para determinar la magnitud del riesgo.

**A. Evaluación de la Probabilidad:**

- **Rara vez (1):** El evento podría ocurrir solo en circunstancias excepcionales.
- **Improbable (2):** El evento puede ocurrir en algún momento.
- **Posible (3):** El evento podría ocurrir en cualquier momento.
- **Probable (4):** El evento ocurrirá en la mayoría de las circunstancias.
- **Casi seguro (5):** Se espera que el evento ocurra en la mayoría de las circunstancias.

**B. Evaluación del Impacto:** Se mide en tres dimensiones de la información:

- **Confidencialidad:** ¿Quién puede ver los datos?
- **Integridad:** ¿Se pueden alterar los datos sin autorización?
- **Disponibilidad:** ¿Podemos acceder a los datos cuando los necesitemos?
- **Fórmula de Nivel de Riesgo:** $Riesgo (Inherente) = Probabilidad \times Impacto$


### 6.4. Evaluación de Controles Existentes

Una vez identificado el riesgo, se verifica qué está haciendo la Institución actualmente para mitigarlo. Los controles se califican según:

- **Tipo de Control:** Preventivo (antes), Detectivo (durante) o Correctivo (después).
- **Naturaleza:** Manual o Automático.
- **Documentación:** ¿Está el control formalizado en un manual o resolución?

### 6.5. Cálculo del Riesgo Residual

Es el nivel de riesgo que permanece después de aplicar los controles actuales. Si el riesgo residual sigue siendo Alto o Extremo, se deben proponer nuevas acciones en el Plan de Tratamiento.

### 6.6. Tratamiento de Riesgos (Opciones de Respuesta)

Según el resultado del riesgo residual, la Institución decide:

- **Reducir (Mitigar):** Implementar nuevos controles técnicos (ej. doble factor de autenticación).
- **Compartir (Transferir):** Contratar pólizas de seguros contra incidentes cibernéticos.
- **Evitar:** Cancelar un proceso o tecnología que represente un peligro inaceptable.
- **Aceptar:** Si el riesgo es bajo, se asume el nivel de exposición con monitoreo periódico.

### 6.7. Comunicación y Monitoreo Reporte:

Los resultados se consolidan en el Mapa de Riesgos Institucional.

- **Revisión:** El Comité Institucional de Gestión y Desempeño revisará la matriz de riesgos semestralmente para ajustar los controles ante nuevas amenazas detectadas por la OTI o Control Interno.

*Estrategias de Tratamiento*:

| Estrategia | Descripción | Aplicación según MINTIC |
|---|---|---|
| **Mitigar** | Reducir el riesgo mediante controles técnicos o administrativos. | Implementación de Firewalls, cifrado y políticas de contraseñas. |
| **Transferir** | Delegar el impacto a un tercero. | Contratación de seguros de ciber riesgo u outsourcing especializado. |
| **Evitar** | Eliminar la actividad que genera el riesgo. | Cese de uso de software obsoletos o procesos inseguros. |
| **Aceptar** | Tolerar el riesgo si es bajo y manejable. | Riesgos cuyo costo de mitigación supera el posible impacto. |

## 7. TRATAMIENTO DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN

De acuerdo con el documento institucional, el tratamiento es el proceso donde se seleccionan e implementan medidas para modificar el riesgo identificado, basándose en la premisa de optimizar la captura, procesamiento y reporte seguro de la información mediante las TIC.

### 7.1. Fases de la Gestión y Tratamiento

El documento establece un ciclo de tres etapas clave antes de definir la acción de tratamiento:

- **Análisis de Riesgos:** Comprensión de las amenazas (eventos que explotan debilidades) y vulnerabilidades.
- **Identificación de Impactos:** Análisis de las consecuencias sobre la Confidencialidad, Integridad y Disponibilidad de los activos de información.
- **-Medición (Fórmula):** Cálculo del nivel mediante Riesgo = Probabilidad × Impacto, utilizando escalas cualitativas (bajo, medio, alto) y cuantitativas (0 a 10)

### 7.1.2. FASES DE GESTIÓN Y TRATAMIENTO

El proceso de gestión en el Colegio Mayor de Antioquia no es lineal, sino un ciclo recurrente que busca la mejora continua de la seguridad digital a través de las siguientes fases:

**FASE 1: Análisis y Evaluación de Riesgos Esta fase es la base del plan y se divide en tres etapas críticas según el manual institucional:**

Identificación de Factores: Se listan las Amenazas (eventos externos o internos como hackeos o errores humanos), las Vulnerabilidades (debilidades técnicas o de procedimiento) y los Impactos (consecuencias financieras, legales o reputacionales).

- **Cuantificación de Probabilidad:** Se determina qué tan posible es que el riesgo se materialice, utilizando escalas que van desde lo "Raro" hasta lo "Casi Seguro".
- **Evaluación del Impacto:** Se analiza el daño potencial sobre los tres pilares: Confidencialidad (acceso no autorizado), Integridad (modificación de datos) y Disponibilidad (caída de sistemas).

**FASE 2: Medición del Nivel de Riesgo (Cálculo Técnico)**

Siguiendo la metodología GT-MA-004, la institución aplica la fórmula:

**Nivel de Riesgo = Probabilidad × Impacto**

La medición se realiza bajo dos enfoques:

- **Cualitativo**: Clasificación mediante términos como Bajo, Medio o Alto.
- **Cuantitativo:** Uso de valores numéricos (ejemplo: escala de 0 a 10) para obtener una precisión estadística que permita priorizar la inversión en seguridad.

**FASE 3: Selección de la Estrategia de Tratamiento**

Una vez medido el riesgo, se decide la acción a tomar. El documento define cuatro caminos posibles:

- **Mitigar:** Es la acción de implementar controles (ej. cifrado, backups) para bajar el nivel del riesgo.
- **Transferir:** Desplazar la responsabilidad o el impacto a un tercero (ej. pólizas de seguros o proveedores de nube).

- **Evitar:** Eliminar la actividad o sistema que genera un riesgo inaceptable.
- **Aceptar**: Tolerar el riesgo cuando su nivel es bajo y el costo de controlarlo es demasiado elevado.

**FASE 4: Implementación y Registro**

(Desarrollo del Plan) Los resultados del tratamiento no se quedan en papel; el documento exige:

- **Registro en el Mapa de Riesgos:** El riesgo debe quedar identificado explícitamente como "Riesgo de Seguridad y Privacidad de la Información".
- **Documento de Control de Avance:** Se debe llevar una bitácora que registre cómo han evolucionado los riesgos tras la aplicación de los controles.

**FASE 5: Seguimiento y Comunicación**

El cierre del ciclo se da a través de:

- **Informes de Plan de Acción:** El seguimiento se realiza conforme a los tiempos establecidos en el Plan de Acción por proceso de la Institución.
- **Reporte de Incidentes:** Comunicación oportuna ante vulneraciones reales para ajustar el plan de manera reactiva y preventiva.
-

### 7.2. Opciones de Tratamiento Institucional

Una vez obtenido el nivel de riesgo, el Colegio Mayor de Antioquia define cuatro estrategias de respuesta:

- **Mitigar (Reducir):** Aplicación de controles preventivos, Detectivos o correctivos para disminuir la probabilidad de ocurrencia o la gravedad del impacto. Es la respuesta estándar para riesgos que superan el umbral de aceptación.
- **Transferir (Compartir):** Acción de trasladar el impacto del riesgo a un tercero, como proveedores de servicios o mediante la contratación de seguros especializados.
- **Evitar:** Eliminar la causa del riesgo, suprimiendo la actividad o el sistema tecnológico que genera la vulnerabilidad inaceptable.
- **Aceptar:** Decisión informada de no tomar medidas adicionales, aplicable cuando el riesgo se encuentra en niveles tolerables y está bajo monitoreo constante.

### 7.3. Selección y Aplicación de Controles

El tratamiento se materializa a través de controles que deben estar debidamente documentados:

- **Controles Técnicos:** Cifrado, copias de seguridad (backups), firewalls y gestión de identidades.
- **Controles Administrativos:** Políticas de seguridad, acuerdos de confidencialidad y planes de capacitación.
- **Seguimiento:** Los controles implementados deben registrarse en el Mapa de Riesgos Institucional con su debida identificación como "Riesgo de Seguridad y Privacidad de la Información".

### 7.4. Monitoreo del Tratamiento

El seguimiento del tratamiento no es estático; el documento GT-MA-004 especifica que:

- Debe alinearse con los tiempos establecidos en el Plan de Acción por proceso.
- Se debe registrar en un documento de control de avance.
- Los resultados deben ser comunicados a los responsables para asegurar que las TIC sigan siendo un soporte seguro y no una fuente de vulneración ante eventuales ataques o errores.

## 8. ACTIVIDADES Y ENTREGABLES DE LAS FASES DE LA METODOLOGÍA DE IMPLEMENTACIÓN

#### 8.1.1. Fase I – Caracterización de los sistemas de gestión y de los procesos de la Entidad

Dentro de esta fase se realizan las siguientes actividades:
- Listado Maestro de Registros en el SIG Actualizado
- Identificación de procedimientos actualizados
- Inventario de activos de información.

#### 8.1.2. Fase II – Identificación de riesgos

Dentro de esta fase se realizan las siguientes actividades:
- Identificación de causas
- Identificación de riesgo.
- Establecer las consecuencias
- Tipificar y valorar el riesgo
- Determinar el impacto
- Determinar la probabilidad
- Determinar el nivel de riesgo inherente y residual

#### 8.1.3. Fase III – Valoración de controles

- Cálculo estimado del riesgo residual
- Selección de la opción de tratamiento
- Determinar las acciones de mitigación del riesgo.

#### 8.1.4. Fase V – Seguimiento y Evaluación.

- Realizar seguimiento a la autoevaluación de la gestión por áreas
- Realizar monitoreo de los riesgos a través de la evaluación independiente que realiza la Entidad y el líder del sistema de gestión de seguridad y privacidad de la información.
- Determinar las alertas que se generen a partir de los resultados de las mediciones anteriores.

- Aplicar acciones de mejora continua. resultado de las auditorías, de los mapas de riesgos y planes de acción.
- Socialización de resultados.

## 9. METODOLOGÍA DE IMPLEMENTACIÓN

Esta metodología ofrece un esquema organizado para la administración de riesgos en organizaciones públicas, con el objetivo de identificar, evaluar y reducir los riesgos de forma eficiente.

**1. Contexto y Alcance**

Esta etapa inicial define los límites y el marco de trabajo para la gestión de riesgos.

- **Actividades:** Se establece el alcance del sistema (activos, procesos y áreas involucradas), se identifican los objetivos estratégicos y se determinan las expectativas de las partes interesadas, como clientes, reguladores y empleados.

**2. Identificación de Riesgos**

Consiste en descubrir qué puede suceder, cómo y por qué, centrándose en los activos de información.

- **Actividades:** Elaborar un inventario completo de activos, detectar sus vulnerabilidades (debilidades técnicas o de proceso) y determinar las amenazas potenciales (eventos externos o internos) que podrían explotarlas.

**3. Análisis y Evaluación de Riesgos**

En esta fase se mide la magnitud de los riesgos para poder priorizarlos.

- **Actividades:** Se estima el impacto (financiero, legal, reputacional u operativo) y se calcula la probabilidad de ocurrencia. Con estos datos, se clasifican los riesgos en niveles: **Bajo, Medio, Alto o Crítico**.

**4. Definición de Estrategias de Tratamiento**

Se decide formalmente la acción a seguir para cada riesgo priorizado.

- Opciones de tratamiento:
  - **Mitigar:** Implementar controles para reducir la probabilidad o el impacto.
  - **Evitar:** Detener la actividad que genera el riesgo.
  - **Transferir:** Compartir el riesgo con terceros (ej. seguros o contratos).
  - **Aceptar:** Tolerar el riesgo si es bajo y su gestión no es costo-efectiva.

**5. Plan de Tratamiento de Riesgos**

Es la hoja de ruta detallada para la ejecución de las estrategias seleccionadas.

- **Actividades:** Selección de controles específicos (basados en **ISO/IEC 27002**), asignación de responsables, definición de recursos (humanos, técnicos, financieros) y establecimiento de cronogramas con plazos claros.

**6. Implementación de Controles**

Es la puesta en marcha de las medidas de seguridad.

- **Actividades:** Establecer políticas y procedimientos documentados, configurar herramientas tecnológicas (firewalls, cifrado, sistemas de autenticación) y realizar jornadas de capacitación y concientización para el personal.

**7. Supervisión y Mejora Continua**

Asegura que los controles sigan siendo efectivos a lo largo del tiempo.

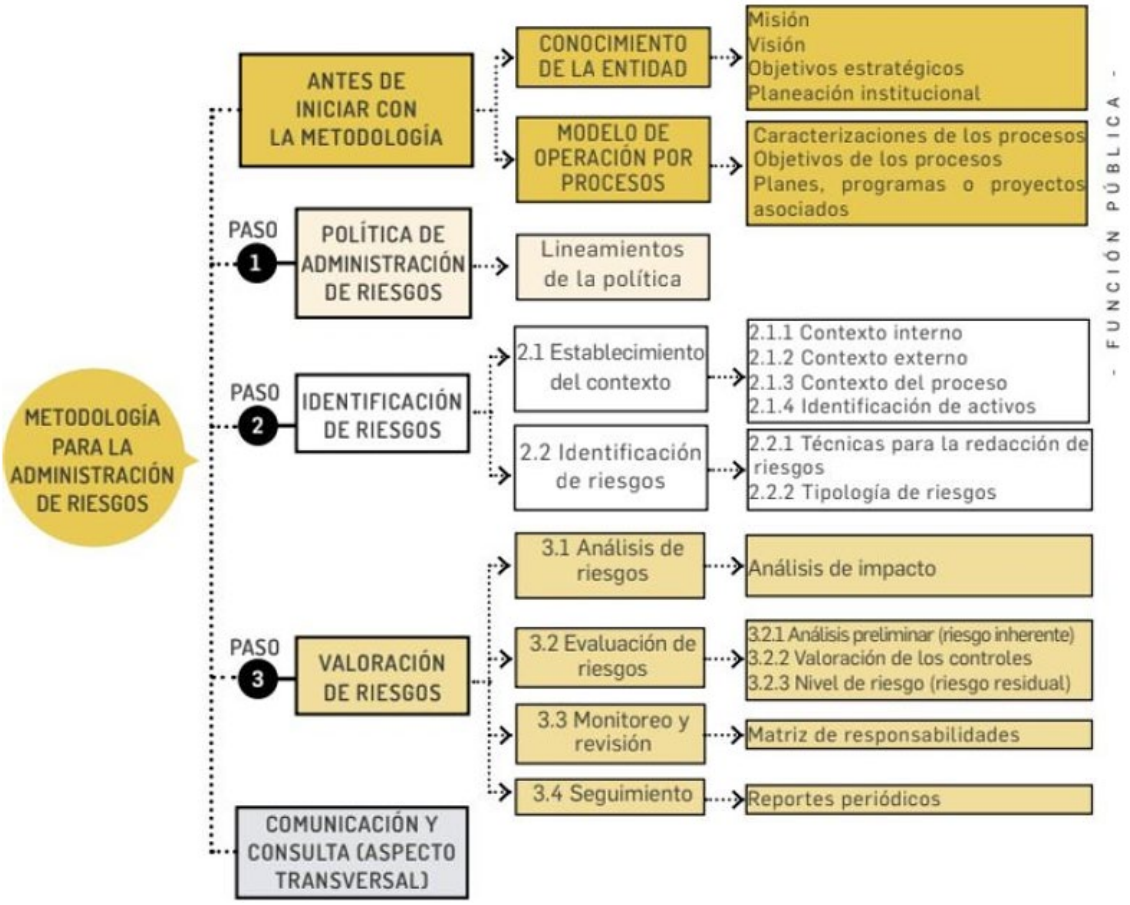
- **Actividades:** Ejecución de auditorías internas, monitoreo constante de riesgos residuales (los que quedan tras aplicar controles) y ajuste del sistema basado en incidentes reales o cambios en el entorno institucional.

**8. Comunicación y Documentación**

Garantiza la transparencia y el soporte probatorio de la gestión.

- **Actividades:** Generar informes periódicos sobre el estado de los riesgos para la alta dirección, documentar cada acción realizada y sus resultados, y asegurar que todos los equipos relevantes estén informados.

**9.1. Metodología para la administración del riesgo.**




**9.2. ENTREGABLES**

**Fase I: Contexto y Alcance**

- **Documento de Alcance y Objetivos de Gestión de Riesgos**: Define formalmente qué activos, procesos y áreas están bajo protección y qué metas se esperan alcanzar con el tratamiento.
- **Identificación de Partes Interesadas**: Registro detallado de los actores (clientes, reguladores, empleados) y sus expectativas legales o contractuales frente a la información.

**Fase II: Identificación de Riesgos**

- **Lista (Inventario) de Activos de Información**: Un catálogo exhaustivo de los activos que tienen valor para la institución (sistemas, bases de datos, soportes físicos, personas).
- **Mapa de Amenazas y Vulnerabilidades**: Documento técnico donde se cruzan las debilidades detectadas en los activos con las posibles amenazas externas o internas que podrían explotarlas.

**Fase III: Análisis y Evaluación de Riesgos**

- **Matriz de Evaluación de Riesgos**: Herramienta donde se visualiza el nivel de riesgo tras cruzar la probabilidad de ocurrencia con el impacto (financiero, legal o reputacional).
- **Registro Priorizado de Riesgos**: Lista de riesgos ordenados de mayor a menor criticidad, lo que permite enfocar recursos en los niveles "Altos" o "Críticos".

**Fase IV: Definición de Estrategias de Tratamiento**

- **Documentación de Decisiones Estratégicas**: Registro formal que justifica por qué se eligió una acción específica para cada riesgo (Mitigar, Evitar, Transferir o Aceptar).

**Fase V: Plan de Tratamiento de Riesgos**

- **Plan de Tratamiento de Riesgos**: Hoja de ruta que detalla los controles a implementar, cronogramas de ejecución, recursos (humanos, técnicos, financieros) y responsables.
- **Lista de Controles de Seguridad Seleccionados**: Catálogo específico de medidas basadas en estándares internacionales (como ISO/IEC 27002) que se aplicarán.

**Fase VI: Implementación de Controles**

- **Controles Operativos**: Configuración real de herramientas técnicas como firewalls, sistemas de cifrado y mecanismos de autenticación.
- **Procedimientos Documentados**: Manuales y guías escritas que establecen el "paso a paso" para mantener la seguridad en las operaciones diarias.
- **Evidencias de Formación del Personal**: Registros de asistencia y evaluaciones de las jornadas de capacitación y concientización en seguridad.

**Fase VII: Supervisión y Mejora Continua**

- **Informes de Auditoría y Monitoreo**: Resultados de las revisiones internas sobre la efectividad de los controles y el estado de los riesgos residuales.
- **Actualizaciones del Registro de Riesgos**: Versiones revisadas de la matriz de riesgos que reflejan cambios en el entorno o nuevos incidentes detectados.

**Fase VIII: Comunicación y Documentación**

- **Informe Final de Gestión de Riesgos**: Documento periódico dirigido a la alta dirección que resume el estado general de la seguridad y la efectividad del plan.
- **Evidencias de Cumplimiento para Auditorías**: Carpeta de soporte documental lista para inspecciones externas que certifica que la institución cumple con las normativas (Ley 1581, ISO 27001, etc.).

## 10. MARCO CONCEPTUAL

- **Activo:** En relación con la seguridad de la información, se refiere a cualquier información o elemento relacionado con el tratamiento de la misma (sistemas, soportes, edificios, personas…) que tenga valor para la organización.
- **Amenazas:** Causa potencial de un incidente no deseado, que puede provocar daños a un sistema o a la organización.
- **Análisis de Riesgo:** Proceso para comprender la naturaleza del riesgo y determinar el nivel de riesgo.
- **Auditoría**: Proceso sistemático, independiente y documentado para obtener evidencias de auditoría y obviamente para determinar el grado en el que se cumplen los criterios de auditoría.
- **Ciberseguridad:** Capacidad del Estado para minimizar el nivel de riesgo al que están expuestos los ciudadanos, ante amenazas o incidentes de naturaleza cibernética.

- **Ciberespacio:** Ámbito o espacio hipotético o imaginario de quienes se encuentran inmersos en la civilización electrónica, la informática y la cibernética. (CONPES 3701, Tomado de la Academia de la lengua española). 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 es también utilizado como sinónimo de salvaguarda o contramedida. En una definición más simple, es una medida que modifica el riesgo.
- **Criticidad:** Ej. Catastrófico, Mayor, Moderado, Menor, Insignificante.
- **Declaración de aplicabilidad**: Documento que enumera los controles aplicados por el Sistema de Gestión de Seguridad de la Información – SGSI, de la organización tras el resultado de los procesos de evaluación y tratamiento de riesgos y su justificación, así como la justificación de las exclusiones de controles del anexo A de ISO 27001.
- **Eficacia:** Grado en el que se realizan las actividades planificadas y se logran los resultados planificados. NTC ISO 9000: 2015.
- **Gestión de incidentes de seguridad de la información:** Procesos para detectar, reportar, evaluar, responder, tratar y aprender de los incidentes de seguridad de la información.
- **Gestión o Administración del riesgo:** Proceso efectuado por la alta dirección de la entidad y por todo el personal para proporcionar a la administración un aseguramiento razonable con respecto al logro de los objetivos.
- **Impacto:** consecuencias que puede ocasionar a la organización la materialización del riesgo.
- **Parte interesada:** Persona u organización que puede afectar a, ser afectada por o percibirse a sí misma como afectada por una decisión o actividad.
- **Plan de continuidad del negocio:** Plan orientado a permitir la continuación de las principales funciones misionales o del negocio en el caso de un evento imprevisto que las ponga en peligro.
- **Plan de tratamiento de riesgos:** Documento que define las acciones para gestionar los riesgos de seguridad de la información inaceptables e implantar los controles necesarios para proteger la misma.
- **Política de administración del riesgo:** Declaración de la Dirección y las intenciones generales de una organización con respecto a la gestión del riesgo.
- **Revisión:** Acción para determinar la idoneidad, conveniencia y eficacia de la gestión del riesgo.
- **Riesgo:** 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.
- **Riesgo inherente:** Es aquel al que se enfrenta una entidad en ausencia de acciones de dirección para modificar su probabilidad o impacto. (primer análisis).
- **Riesgo residual:** Nivel de riesgo que permanece luego de tomar medidas (dirección) de tratamiento del riesgo. (análisis final/permanece).
- **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).
- **Seguimiento:** Asegurar que las acciones establecidas se están llevando a cabo.
- **Seguridad de la información:** Preservación de la confidencialidad, integridad, y disponibilidad de la información.
- **Sistema de Gestión de Seguridad de la Información SGSI:** Conjunto de elementos interrelacionados interactuantes (estructura organizativa, políticas, planificación de actividades, responsabilidades, procesos, procedimientos y recursos) que utiliza una organización para establecer una política y unos objetivos de seguridad de la información y alcanzar dichos objetivos, basándose en un enfoque de gestión y de mejora continua.
- **Trazabilidad:** Cualidad que permite que todas las acciones realizadas sobre la información o un sistema de tratamiento de la información sean asociadas de modo inequívoco a un individuo o entidad.
- **Vulnerabilidad:** Debilidad de un activo o control que puede ser explotada por una o más amenazas.